

Table of Contents

1.0 Wireless Security	1
1.1 Introduction.....	1
1.2 Wired Equivalent Privacy protocol.....	1
1.2.1 Analysis of WEP flaws	3
1.2.2 Key Stream Reuse	3
1.2.3 Message Modification	3
1.2.4 Message Injection.....	4
1.2.5 Authentication Spoofing	6
1.2.6 IP Redirection.....	7
1.2.7 Wireless Frame Generation.....	7
1.2.7.1 AirJack	8
1.2.7.2 Wavesec	9
1.2.7.3 Libwlan	9
1.2.7.4 FakeAP.....	9
1.2.7.5 Wnet	10
1.2.7.7 Scapy	10
1.2.8 Encryption Cracking Tools	11
1.2.8.1 Wepcrack.....	12
1.2.8.2 Dweputils	12
1.2.8.3 Wep_tools.....	13
1.2.8.4 Wep Attack.....	14
1.2.9 Retrieving the WEP keys from Client Host.....	14
1.2.10 Traffic Injection Tools	15
1.2.11 802.1x Cracking Tools	16
1.2.11.1 Asleap-imp and Leap	16
1.2.12 Wireless DoS Attacks	17
1.2.12.1 Physical Layer Attack or Jamming.....	17
1.2.12.1.1 Signal Strength	18
1.2.12.1.2 Carrier Sensing Time.....	18
1.2.12.1.3 Packet Delivery Ratio.....	19
1.2.12.1.4 Signal Strength Consistency check	20
1.2.12.2 Spoofed Dessociation and Deauthentication Frames.....	20
1.2.12.3 Spoofed Malformed Authentication Frames	21
1.2.12.4 Flooding the Access Point Association and Authentication Buffer	21
1.2.12.5 Frame Deletion Attack.....	22
1.2.12.6 DoS attack dependent upon specific Wireless Setting.....	22
1.2.13 Attack against the 802.11i implementations.....	23
1.2.13.1 Authentication Mechanism Attacks	23
1.3 Prevention and Modifications	25
1.3.1 TKIP: temporal Key Integrity Protocol	27

1.3.1.1 TKIP Implementation	27
1.3.1.1.1 Message Integrity	28
1.3.1.1.2 Initialization Vector.....	29
1.3.1.1.3 Prevention against the FMS Attack.....	31
1.3.1.1.4 Per Packet key Mixing.....	31
1.3.1.1.5 Implementation Details of TKIP	32
1.3.1.1.6 Details of Per Packet Key mixing	33
1.3.1.2 Attack on TKIP	38
1.3.2 AES – CCMP	39
1.3.2.1 CCMP Header	40
1.3.2.2 Implementation	40
1.3.2.2.1 Encryption Process in MPDU	41
1.3.2.2.2 Decrypting MPDU.....	42
1.4 Prevention Method using Detection Devices.....	43
1.5 Conclusion	46
2.0 Vulnerability Analysis for Mail Protocols.....	47
2.1 Introduction.....	47
2.2 Format String Specifiers.....	48
2.2.1 Format String Vulnerability	49
2.2.1.1 Format String Denial of Service Attack	49
2.2.1.2 Format String Vulnerability Reading Attack	50
2.2.1.3 Format String Vulnerability Writing Attack	51
2.2.1.4 Preventive Measures for Format String vulnerability	53
2.3 Buffer Overflow Attack.....	54
2.3.1 Buffer Overflow Prevention.....	56
2.4 Directory Traversal Attacks	60
2.4.1 Remote Detection	62
2.5 False Positive in Remote Detection for Mail Traffic.....	63
2.5.1 False Positive in case of SMTP Traffic	64
2.5.2 False Positive in case of IMAP Traffic.....	67
2.6 Conclusion	70
3.0 Vulnerability Analysis for FTP and TFTP.....	71
3.1 Introduction.....	71
3.1.1 Buffer Overflow in FTP.....	72
3.1.2 Directory Traversal Attack in FTP	73
3.2 TFTP Vulnerability Analysis	74
3.2.1 Vulnerability Analysis	75
3.3 Conclusion	77
4.0 Vulnerability Analysis for HTTP.....	79
4.1 Introduction.....	79
4.2 XSS Attack	79
4.2.1 Prevention against Cross Site Scripting Attacks	82
4.2.1.1 Vulnerability Protection.....	82

4.3 SQL Injection Attacks	88
4.3.1 SQL Injection Case Study	90
4.3.2 Preventive Measures	93
4.3.2.1 Remote Detection	93
4.3.2.2 SQL injection in Oracle Data base	94
4.3.2.2.1 Stored Procedures	94
4.3.2.2.2 Remote Detection for Oracle Database	96
4.3.3 Other Preventive Measures	100
4.3.3.1 Preventive Measures by developers	101
4.4 MS DoS Device Name Vulnerability.....	101
4.4.1 Prevention from DoS Device Name Vulnerability	103
4.5 False Positive in HTTP.....	103
4.6 Evasion of HTTP Signatures.....	105
4.7 Conclusion	109
5.0 Vulnerability Analysis for DNS and DHCP	111
5.1 Introduction of DNS Protocol	111
5.1.1 Vulnerabilities in a DNS Protocol	113
5.1.1.1 DNS Cache Poisoning	113
5.1.1.2 Redirection Attack	116
5.1.1.3 Buffer Overflow Vulnerability	116
5.1.1.4 DNS Man in the Middle Attack or DNS Hijacking	116
5.1.1.5 DNS Amplification Attack	117
5.1.2 False Positives in a DNS Protocol	118
5.2 Introduction of DHCP	120
5.2.1 Vulnerabilities in DHCP	120
5.2.1.1 Client Masquerading.....	120
5.2.1.2 Flooding	121
5.2.1.3 Client Misconfiguration.....	121
5.2.1.4 Theft of Service.....	121
5.2.1.5 Packet Altercation.....	121
5.2.1.6 Key Exposure.....	121
5.2.1.7 Key Distribution.....	122
5.2.1.8 Protocol Agreement Issues	122
5.2.2 False Positive in DHCP	122
5.3 Conclusion	124
6.0 Vulnerability Analysis for LDAP and SNMP	125
6.1 Introduction.....	125
6.2 ASN and BER Encoding	125
6.3 BER implementation for LDAP.....	127
6.3.1 Threat Analysis for Directory Services	129
6.4 SNMP	131
6.4.1 Vulnerability Analysis for SNMP	134
6.5 Conclusion	134

7.0 Vulnerability Analysis for RPC	135
7.1 Introduction.....	135
7.2 RPC Message Protocol	136
7.3 NDR Format	136
7.4 Port Mapper	152
7.5 False Positive for SMB RPC Protocol	153
7.6 Evasion in RPC.....	157
7.6.1 Multiple Binding UUID	157
7.6.2 Fragment Data across many Requests	158
7.6.3 Bind to one UUID then alter Context	159
7.6.4 Prepend an ObjectID	161
7.6.5 Bind with an authentication field.....	161
7.6.6 One packet UDP function call	162
7.6.7 Endianness Selection.....	162
7.6.8 Chaining SMB commands	163
7.6.9 Out of order chaining	164
7.6.10 Chaining with random data in between commands.....	165
7.6.11 Unicode and non-Unicode evasion	165
7.6.12 SMB CreateAndX Path Names.....	166
7.7 Conclusion	167
8.0 Malware	169
8.1 Introduction.....	169
8.2 Malware Naming Convention	169
8.2.1 Worms	170
8.2.2 Trojans	171
8.2.3 Spyware & Adware	172
8.3 Malware Threat Analysis	173
8.3.1 Creating controlled Environment.....	173
8.3.1.1 Confinement with the Hard Virtual Machines	173
8.3.1.2 Confinement with the Soft Virtual Machines.....	174
8.3.1.3 Confinement with Jails and Chroot	176
8.3.1.4 Confinement with System call Sensors	177
8.3.1.5 Confinement with System call Spoofing.....	178
8.3.2 Behavioral Analysis	178
8.3.3 Code Analysis.....	180
8.4 Root Kits	181
8.4.1 User and Kernel Mode Communication	182
8.4.2 I/O Request Packets (IRP)	183
8.4.3 Interrupt Descriptor Table.....	189
8.4.4 Service Descriptor Table.....	190
8.4.5 Direct Kernel Object Manipulation	194
8.4.6 Detection of Rootkits	196
8.5 Spyware	197
8.5.1 Methods of Spyware installation and propagation	199
8.5.1.1 Drive- By- Downloads.....	199
8.5.1.2 Bundling.....	201

8.5.1.3 From Other Spyware	203
8.5.1.4 Security Holes	203
8.5.2 Vulnerability Analysis	203
8.5.2.1 Iframe Exploit	203
8.5.2.2 IE .chm File processing Vulnerability	204
8.5.2.3 Internet Code Download Link	205
8.5.3 Anti Spyware Signature Development	207
8.5.3.1 Vulnerability Signature	207
8.5.3.2 CLSID Data base	208
8.5.3.3 Spyware Specific Signature	208
8.5.3.4 Information Stealing	210
8.5.3.5 Preventing Information from being sent as emails.....	210
8.6 Conclusion	210
9.0 Reverse Engineering.....	213
9.1 Introduction.....	213
9.2 Anti Reversing Technique	213
9.2.1 Anti Disassembly	214
9.2.1.1 Linear Sweep Disassembler.....	214
9.2.1.2 Recursive Traversal Disassembler.....	216
9.2.1.3 Evasion Technique for Disassembler.....	217
9.2.2 Self-Modifying Code	220
9.2.3 Virtual Machine Obfuscation.....	224
9.3 Anti Debugging Technique	225
9.3.1 Break Points	227
9.3.1.1 Software break point	227
9.3.1.2 Hardware break point.....	228
9.3.1.3 Detection of Breakpoint.....	229
9.4 Virtual Machine Detection	229
9.4.1 Checking finger print	230
9.4.2 Checking system tables	230
9.4.3 Checking processor instruction set	231
9.5 Unpacking	232
9.5.1 Manual unpacking of malware.....	233
9.5.1.1 Finding an original entry point of an executable.....	233
9.5.1.2 Taking memory Dump	238
9.5.1.3 Import Table Reconstruction	241
9.5.1.4 Import redirection and code emulation.....	246
9.6 Conclusion	250
Index	253



<http://www.springer.com/978-0-387-74389-9>

Vulnerability Analysis and Defense for the Internet

Singh, A. (Ed.)

2008, XVI, 254 p., Hardcover

ISBN: 978-0-387-74389-9