IT-Sicherheit:

(Anti-)Hacking für Administratoren

Angriffe erkennen und Schutzmaßnahmen verstärken

Version 10

CertPro® PRESS
an Imprint of CertPro® Limited

Bibliografische Informationen der Deutschen NationalbibliothekDie Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Datensind im Internet über *http://dnb.d-nb.de* abrufbar.

Kommentare und Fragen können Sie gerne an uns richten unter E-Mail: info@certpro-press.de

Artikel-Nr.: HK-120218

Print-Ausgabe ISBN 978-3-9447-4931-0
ebook-Ausgabe: ISBN 978-3-9447-4932-7

Autor: Carlo Westbrook

Einbandgestaltung: CertPro® Limited
Bilder und Grafiken: CertPro® Limited
Herstellung: CertPro® Limited
Druck und Verarbeitung: WIRmachenDRUCK GmbH, 71522 Backnang
Printed in Germany

Auf einen Blick

Modul 0 - Einführung

Modul 1 - Grundlagen der IT-Sicherheit

Modul 2 - Planung und Vorbereitung von Angriffen

Modul 3 - Moderne Angriffstechniken

Modul 4 - Gefahren durch Viren, Würmer, Trojaner & Rootkits

Modul 5 - Angriffe auf Drahtlosnetzwerke (WLANs)

Modul 6 - Firewalls, IDS & Honeypots

Modul 7 - Überblick zu Penetrationstests

Optionale Module
(im Umfang des Kursteilnehmer-Downloads als PDF-Dateien enthalten)

Modul 8 - Grundlagen der Kryptografie

Modul 9 - Einführung in das BSI-Grundschutzkompendium

Website zum Buch

Liebe Leserin, lieber Leser,

zu dieser Seminarunterlage bieten wir Ihnen zusätzliche Materialien, wie z. B. Zusatzdokumentation, eine Übersicht der darin enthaltenen Weblinks, sowie Beispieldateien, die Sie bei Bedarf gerne direkt aus unserer Verlagswebsite im Internet herunterladen können unter:

https://www.CertPro-Press.de/Courses/9310.html

Konventionen & Symbole

Um bestimmten Textpassagen in der Seminarunterlage etwas hervorzuheben, wurden die folgenden typografischen Konventionen und Symbole verwendet:

Konvention	Bedeutung
`befehl`	Stellt die Befehlssyntax oder auch Befehlsausführung von Kommandozeilenbefehlen dar.
WEITER	Kennzeichnet die Ausführung einer bestimmten Programmfunktion, beispielweise den Mausklick auf eine Schaltfläche.
	Weist auf einen allgemeinen Hinweis zu bestimmten Themenbereichen hin.
	Gibt einen Hinweis auf wichtige Funktionen oder auch Situationen, die unbedingt beachtet werden sollten.
	Kennzeichnet Tipps für die praktische Anwendung bzw. Umsetzung.
	Kennzeichnet Informationen oder auch Situationen, die ein Risiko oder eine Bedrohung darstellen können.
	Weist auf weitere Informationsquellen zu bestimmten Themenbereichen im Internet hin.
	Kennzeichnet Methoden oder Tools, mit denen man Gefahren durch potentielle Angreifer mitunter abwenden kann.

Inhaltsverzeichnis

Kurzvorstellung 18
Teilnahmevoraussetzungen 18
Zielgruppe 18
Lernziele 19
Kursbeschreibung 19
OPTIONALE MODULE: 21
Wichtiger Hinweis 22
Kursrauminstallation 22
Kurze Einführung in Hyper-V 23
Wichtiger Hinweis zu den Kurstools 23
Einrichtungen 24
Modul 1 - Grundlagen der IT-Sicherheit 25
1.1 Aktuelle Trends und Entwicklungen 26
1.2 Aktuelle Trends und Entwicklungen 26
1.3 Aktuelle Entwicklung der IT-Sicherheit 27
1.3.1 Anforderungen an die IT-Sicherheit 28
1.4 Bedrohungspotential 29
1.4.1 Aktuelle Gefahren für Computersysteme und -netzwerke 29
1.4.2 Spear Phising – Opfer beim Namen genannt 31
1.4.3 Die Realität – täglich neue „Opfer“… 32
1.4.4 „Ranglisten“ der besten Hacker… 32
1.4.5 Die Realität – Angriffe gegen „bekannte“ Webseiten 33
DEMO: Aktuelle „Opfer“ im Internet 33
1.5 Online-Monitore - Cyberattacken in „Echtzeit“ 34
DEMO: Aktuelle „Cyberattacken“ im Internet 35
1.6 Ransomware – moderne Erpresser 35
1.6.1 CryptoLocker, Locky, TeslaCrypt, WannaCry & Co. 36
1.6.2 Beispiele für Ransomware-Angriffe 36
1.7 Die Realität… - und noch ein erschreckender Trend… 37
1.8 Die Realität… - der „offene“ Handel mit Kreditkartendaten 37
1.9 Angriffe auf bekannte Sicherheitstechnologien 38
1.10 Whaling - die Jagt auf die „großen“ Fische… 39

1.11 Drive-by-Download-Attacken 39
1.12 Identitätsdiebstahl - Traue nicht JEDEM…! 40
1.13 Identitäten - Offener Handel im Internet 40
1.14 Malware in sozialen Netzwerken 41
1.14.1 Gefahr: Malware - versteckt im Dateidownload 41
1.15 Gründe für Angriffe 42
1.16 Arten von Angreifern 43
1.16.1 WER? - „Klassische“ Arten von Angreifern 43
1.16.2 WER? - Detaillierte Klassifizierung der „Hacker“ 45
1.17 Hacker vs. Penetration Tester - der Vergleich 46
1.18 Angriffsziele & häufige Arten von Sicherheitslücken 46
1.18.1 Potentielle Angriffesziele 47
1.18.2 Die „Top 25-Schwachstellen“ 47
1.19 Häufige Methoden bei Netzwerkangriffen 49
1.19.1 Klassifizierung von Angriffen 49
1.19.2 Mögliche Angriffstypen – einige Beispiele 50
1.20 Phasen eines (geplanten) Netzwerkangriffs 51
1.21 Windows-Sicherheitsfeatures aus Sicht des Angreifers 52
1.21.1 Windows-Sicherheitsfeatures aus Sicht der Angreifer 52
1.21.2 Kernel Mode & User Mode 53
Local Security Authority (LSA) 54
Win32-Teilsystem 54
1.21.3 Secure boot (UEFI) 54
1.21.4 Sicherheitsprinzipale 55
1.21.5 Benutzerkonten 56
1.21.6 Gruppenverwaltete Dienstkonten (gMSA) 57
1.21.7 Gruppen 58
1.21.8 Computerkonten 60
1.21.9 SAM und Active Directory (AD) 61
1.21.10 Gruppenrichtlinien und „Richtlinien für Kennwörter (PSOs)“ 62
1.21.11 „Als Administrator ausführen…“ 63
1.21.12 Benutzerkontensteuerung (UAC) 64
1.21.13 Patches & Service Packs 65
1.21.14 Windows-Firewall 66
1.21.15 Windows Defender 67
1.21.16 Schutz der Datenübertragung mit IPSec 67

1.21.17 Dateischutz mit NTFS/ReFS und Encrypting File System (EFS) 68
1.21.18 BitLocker & BitLocker-to-Go 69
1.22 Weitere Sicherheitsfeatures 70
1.22 Wichtige Sicherheitsprinzipien 71
1.23 Schutz durch mehrstufige Verteidigung 72
1.24 Rechtliche Grundlagen 73
1.24.1 Strafbare Handlungen 74
1.24.2 Straftatbestände nach StGB und UWG 76
1.24.3 Strafanzeige und Strafantrag 80
1.24.4 Beweismittel 81
1.25 Zusammenfassung 82
1.26 Lernzielkontrolle 83
Modul 2 - Planung und Vorbereitung von Angriffen 85
2.1 Footprinting - dem Opfer auf der Spur 86
2.2 Ziele des Footprinting 88
2.3 Durchstöbern von Informationsquellen 90
2.3.1 Suche nach Firmeninformationen im Internet 90
2.3.2 „Gelbe Seiten“, Telefonbücher & Co. 91
2.3.3 Personensuche im Internet 91
DEMO: Personensuche im Internet 92
2.3.4 Personensuche im Internet - „Nicknames“… 92
2.3.5 Suche in „Social Networks“ 93
2.4 Suche nach Webseiten 94
2.5 Google als „Proxy-Server“ missbrauchen 94
DEMO: Aufruf von Cache-Inhalten in Google 95
2.6 Google-Hacking – Opfersuche leicht gemacht 95
2.6.1 Google-Hacking - Erweiterte Suche-Operatoren (Auszug) 96
2.6.2 Suche nach VNC-Servern 97
2.6.3 Google-Suche nach Verzeichnissen 97
2.6.4 Google-Suche nach Servern 98
2.6.5 Suche nach Diensten im Internet 99
DEMO: Verwendung von Such-Operatoren in Google 99
2.7 Die “Google-Hacking Database” 100
DEMO: Suche nach Kennwörtern in der GHDB 101
2.8 Exploit-DB.com - „aktuelles“ Google-Hacking 101
DEMO: Google-Hacking mithilfe von exploit-db.com 102

2.9 Shodan.io - Kühlschränke, TV-Geräte, SmartHome und mehr… 102
DEMO: Recherche im „Internet der Dinge“ (IoT) 103
2.10 Firmenwebsite und Stellenausschreibungen 103
2.11 Suche in verschiedenen „Job-Börsen“ im Internet 104
DEMO: Internet-Recherche in Online-Jobbörsen 104
2.12 „archive.org“ - Zurück in die Vergangenheit 105
DEMO: Internet-Recherche mithilfe von „archive.org“ 105
2.13 Suchmaschinen, Usenet & Newsgroups 106
2.14 Copernic Desktop Search und Search Server 107
DEMO: Internet-Recherche mit Copernic Desktop Search 108
2.15 Maltego - professionelle Recherche 108
2.16 FOCA (Fingerprinting Organizations with Collected Archives) 109
2.17 Footprinting-Tools (Auswahl) 109
2.18 HTTrack Web Site Copier 110
2.18.1 Website-Kopiertools (Auswahl) 111
DEMO: Kopieren einer Webseite mit HTTrack Web Site Copier 111
2.20 Google-Earth, Bing Maps & Co. 113
DEMO: „Vogelperspektive“ von Gebäuden 114
2.21 Read Notify - “Invisible tracking” und mehr… 114
2.21.1 E-Mail-Tracking-Tools (Auswahl) 115
DEMO: „Invisible Tracking“ mittels Readnotify.com 115
2.22 DNS-Abfragen & WHOIS 116
DEMO: Domäneninhaber mittels DeNIC & Internic ermitteln 117
2.23 Ermittlung des Inhabers bestimmter IP-Adressen 118
DEMO: Ermitteln des Inhabers bestimmter IP-Adressen 118
2.23.1 WHOIS-Tools (Auswahl) 119
2.23.2 WhatIsMyIP.com - Wer bin ich überhaupt? 119
2.24 SamSpade - detaillierte Informationssuche 120
2.25 „LSD“-Abfragen an DNS-Server 120
2.25.1 DNS-Eintragstypen (Auswahl) 121
2.25.2 DNS-Informationen abrufen und auswerten 122
DEMO: Ermitteln von DNS-Informationen im Internet 123
2.26 Routenverfolgung mit Traceroute 123
2.26.1 Grafische Traceroute-Tools 125
DEMO: Einsatz von Traceroute-Tools im Internet 126
2.27 Scanning - die Suche nach der offenen „Tür“ 126

2.28 Rechner orten — am Anfang steht die Suche 128
2.28.1 Angry IP (Ping Sweep-Tool) 128
2.28.2 Ping Sweep-Tools (ICMP-Scanner) (Auswahl) 129
DEMO: Rechnersuche mit “Angry IP” 129
2.29 Portscan-Tools 130
2.29.1 SuperScan 130
DEMO: Portscans mit SuperScan 131
2.29.2 Network Mapper (nmap) 131
DEMO: Portscans mittels nmap unter Windows 134
2.29.3 Portscan-Tools (ICMP-Scanner) (Auswahl) 138
2.29.4 Portscan-„Light“ mit telnet 139
2.29.5 Portscans erkennen 140
2.30 Firewalk - ab durch die Feuerwand 141
2.30.1 Firewalk - Gegenmaßnahmen 142
2.31 Enumeration - Server und Betriebssysteme ausspähen 142
2.31.1 Ausspähen von Webservern 143
2.31.2 Banner-Grabbing 144
2.31.3 Banner-Grabbing verhindern 146
2.31.4 Ausspähen weiterer Netzwerkdienste 147
2.32 Ausspähen der NetBIOS-Name Services 149
2.32.1 Ausspähen von Arbeitsgruppen und Domänen 149
2.32.2 Auflistung aller Domänencontroller 150
2.32.3 Auflistung der Sicherheitsrichtlinie für Benutzerkennwörter 151
2.32.4 Abfragen von lokalen und Domänen-Benutzerkonten 151
2.32.5 Abfrage der Rollen von Computersystemen 152
2.32.6 Verhindern der NetBIOS-Name Service-Ausspähung 153
2.33 Ermittlung von Computern mithilfe des Ping-Befehls und ARP 154
DEMO: Ermitteln von Computersystemen mittels Ping und ARP 155
2.34 Ausspähen des Administrator-Kontos 156
DEMO: Ermitteln des Administratorkontos 158
2.35 Ausspähen von NetBIOS-Sitzungen 158
DEMO: Informationsgewinnung mit enum & Co 161
2.35.1 Schutz gegen Missbrauch der IPC$-Freigabe 161
2.36 Auflisten vorhandener SMB-Sitzungen mit NetSess.exe 164
DEMO: Auflisten vorhandener SMB-Sitzungen 165
2.37 Active Directory ausspähen 165

2.37.1 Ausspähen mittels LDP.exe (LDAP-Tool) 166
2.37.2 Ausspähen von Active Directory verhindern 168
2.38 Unix/Linux ausspähen 169
2.38.1 Verhindern der RPC-Ausspähung unter Unix/Linux 171
2.39 Benutzer unter UNIX/Linux abfragen 171
2.39.1 Abfragemöglichkeiten über rwho und rusers verhindern 172
2.40 Suche nach passenden Exploits 172
2.40.1 Exploit-Kategorien 173
2.40.2 Exploits im Internet 174
DEMO: Ermitteln aktueller Exploits 175
2.40.3 Metasploit-Framework — Exploits für alle 175
2.40.4 MetaSploit Express & Pro - kostenpflichtige Varianten 177
2.40.5 Immunity CANVAS 177
2.41 Schwachstellen vorbeugen: Patch-Management 178
2.41.1 Update-Management mit WSUS 178
DEMO: Manueller Download von Patches 179
2.41.2 Flexera: Secunia CSI + SCCM / WSUS 180
2.42 Schwachstellen-Scanner 181
2.42.1 Verfügbare Schwachstellen-Scanner (Auswahl) 181
DEMO: Einsatz von Schwachstellen-Scannern 182
2.43 Angriffsplan erstellen 182
2.44 Botnets - alle für einen… 183
2.45 Angriffe verschleiern mittels offener Proxyserver 184
2.45.1 Proxy Chaining - effektiv verstecken 184
2.45.2 Verschleiern leicht gemacht - Proxy Switcher 185
2.45.3 Verschleiern leicht gemacht - Proxy Workbench 185
2.45.4 Proxy-Tools (Auswahl) 186
DEMO: Open Proxy-Server im Internet 186
2.45.5 TOR und CyberGhost 187
2.46 Zusammenfassung 187
2.47 Lernzielkontrolle 188

Modul 3 - Moderne Angriffstechniken 191

3.1 Gefahren für Gebäude, Serverräume und Netzwerkverbindungen 191
3.1.1 Gefahren für Gebäude, Serverräume und Rechenzentren 192
3.1.2 Gefahren für Netzwerkgeräte und -verbindungen 193
3.2 Schutz gegen Angriffe auf Gebäude, Serverräume, Netzwerkgeräte & -verbindungen 194

3.2.1 Schutzmaßnahmen: JA, aber bitte nicht so… 195
3.3 Gefahren für Computersysteme 195
3.3.1 BIOS-Kennwörter „knacken“ 196
3.4 Benutzerkennwörter zurücksetzen 197
3.4.1 NTCrack & Co. - Passwort-Reset leichtgemacht 198
3.4.2 Kommerzielle Tools zum Passwort-Zurücksetzen 199
3.4.3 Ophcrack Live-CD - Passwort-Crack für „Jedermann“ 199
3.5 Installations-DVD - Windows aushebeln leicht gemacht 200
DEMO: Angriff mithilfe der Installations-DVD 201
3.6 Physikalischer Angriffe mit Keyloggern 201
3.6.1 Hardware-Keylogger - eine Auswahl 202
DEMO: Einsatz von Hardware-Keyloggern 202
3.7 Schutz gegen physikalische Angriffe auf Computersysteme 203
3.8 Software-Keylogger - die unsichtbare Gefahr 203
3.8.1 Software-Keylogger - eine Auswahl 204
3.9 USB-Spyware & Co. - die oft „verkannte“ Gefahr 204
3.10 Schutz gegen Software-Keylogger & Spyware 206
3.11 Gefahren für mobile Computersysteme 207
3.12 Social Engineering - „Feinde unter uns…“ 207
3.12.1 Typische Social Engineering-Angriffe 208
3.12.2 „Shoulder Surfing“ — ohne großen Aufwand 209
3.12.3 „Shoulder Surfing“ — auch mit Hilfsmitteln möglich 209
DEMO: Einsatz von Spycams 210
3.12.4 „Dumpster Diving“ — die Mühe lohnt sich oft 210
3.12.5 USB-Sticks & Co. - die oft unerkannten Gefahren… 211
3.13 Schutz gegen Social Engineering-Attacken 212
3.14 Electronic Social Engineering 212
3.14.1 Phishing 213
3.14.2 Phishing - Typisches Beispiel für Phishing-E-Mails 213
3.14.3 Professionelles Phishing 214
3.14.4 Vorbereitende Schritte der Phisher 214
3.15 Spam-Attacken - auch ein Mittel der Phisher… 215
3.15.1 PhishTank - Anti-Phishing-Webseite 215
DEMO: Überblick über Phishing-Webseiten 216
3.16 Spear Phishing - das Opfer beim Namen genannt 216
DEMO: Fake-Webseite im Internet Explorer 217

3.17 Klicken - oder besser nicht…? 217
3.18 Pharming - die Unterstützung für den Phisher 218
DEMO: Pharming-Versuch unter Windows 219
3.19 Phishing/Pharming - ein Paradebeispiel aus der Praxis… 219
3.20 Phishing-Tricks - Basis 10-Adressen… 220
3.21 Phishing-Tricks - Kurz-URL-Dienste… 220
3.22 Überprüfung unbekannter URLs in E-Mails 221
DEMO: Untersuchen unbekannter URLs 222
3.23 Schutz gegen Phishing- und Pharming 222
3.24 Informationssammlung in Social Networks 223
3.25 „Reverse“-Bildersuche im Internet 224
3.26 Twitter-Scams & Co. - Trau, Schau, Wem… 224
3.27 Phising - in sozialen Netzwerken 225
3.27.1 Schutzmöglichkeiten gegen Angriffe in Social Networks 225
3.28 Angriffe mit Sniffer-Tools 226
3.28.1 WireShark (ehemals Ethereal) 227
3.28.2 Nach Kennwort-Hashes “sniffen“ 228
3.28.3 Sniffer-Attacken vorbereiten 228
DEMO: Sniffing von Kennwörtern mit Cain & Abel 230
3.28.4 Sniffer-Angriffen vorbeugen 230
3.29 Angriffe auf Kennwörter 231
3.29.1 Kennwörter — und sichere Kennwörter 232
3.29.2 (Un-)Sichere Kennwörter 234
3.29.3 Das „Problem“ mit den GPUs 235
3.30 Angriffe auf Passwörter in Windows-Netzwerken 236
3.30.1 Windows und Passwörter 237
3.30.2 Verbesserungen mit NTLMv2 238
3.31 Speicherung von Kennwörtern in Windows SAM 239
3.32 Kerberos V5-Protokoll 239
3.33 Absichern der Authentifizierung 241
3.34 Methoden für den Angriff auf Kennwörter 245
3.34.1 Kennwörter erraten 245
3.34.2 Erraten von Kennwörtern automatisieren 246
3.34.3 Schutz gegen das Erraten von Kennwörtern 247
3.34.4 Kontosperrungsschwelle konfigurieren 247
3.35 Nach Kennwörtern „sniffen“ 248

3.36 (Remote-)Kennwörter „knacken“ 249
3.36.1 Cain and Abel 250
3.36.2 L0phtCrack 251
3.36.3 Elcomsoft Distributed Password Recovery 252
3.36.4 Brutus AET2 252
3.36.5 Weitere Passwort-Cracker 253
DEMO: Angriffe auf Kennwörter mit L0phtcrack 253
3.37 Auslesen von Kennwortfeldern 254
DEMO: Auslesen von Kennwortfeldern 254
3.38 Kennwortschutz von Dateien cracken 255
DEMO: Kennwortschutz von Dateien cracken 255
3.39 Sicherheitsgruppe „Protected Users“ 256
3.40 CrackStation - Online-Entschlüsselung von Kennwort-Hashes 257
DEMO: Online-Angriff auf Kennwort-Hashes mit CrackStation 258
3.41 Pass-the-Hash und Pass-the-Ticket - Entschlüsseln nicht nötig 258
DEMO: Angriffe auf Kennwörter mit Mimikatz, WCE & Co. 259
3.42 Credential Guard - Schutz gegen Pass-the-Hash & Co. 268
3.43 Tricks der Hacker - Dateien verstecken 269
3.43.1 Alternative Datenströme (ADS) 269
DEMO: Daten in alternativen Datenströmen (ADS) verstecken inkl. Hardlink 271
3.43.2 In NTFS versteckte Dateien aufspüren 271
3.44 Zusammenfassung 272
3.45 Lernzielkontrolle 273

Modul 4 - Gefahren durch Viren, Würmer, Trojaner & Rootkits..... 275

4.1 Computerviren - die „betagte“ Gefahr 275
4.1.1 Virusdefinition 276
4.1.2 Virus-Kategorien 276
DEMO: Analysieren von Virendateien 279
4.1.3 Virenbaukästen aus dem Internet 279
4.1.4 Computerviren und -würmer - Infektionswege 280
4.2 Computerwürmer - Fortpflanzung ist alles… 280
4.3 Schutz vor Viren und Würmern 281
4.3.1 Antivirus-Software - vielfältiges Angebot 282
4.3.2 Testviren & Co. 283
DEMO: Verwendung von Antivirus-Software 283
4.4 Online-Tests für Dateien 284

DEMO: Online-Überprüfung von Dateien 284
4.5 Spyware - die oft „verkannte“ Gefahr 285
4.6 Schutz vor Spyware 286
4.7 Ransomware - moderne Erpresser 286
4.7.1 Bekannte Ransomware 287
4.8 Trojaner - die Macht der Angreifer 287
4.8.1 Trojaner-Arten 288
4.8.2 Trojaner-Ports 288
4.8.3 Bekannte Trojaner-Programme 289
4.8.4 OptixPro 291
4.8.5 Weitere Backdoor-Tools & Trojaner 292
4.8.6 DarkComet-RAT, BlackShades & Co. - aktuelle Gefahren 292
DEMO: Einsatz von Trojanern 293
4.8.7 Infektionsmöglichkeiten mit Trojanern 293
4.9 Vortäuschen bestimmter Dateitypen 294
4.10 Verstecken von Trojanern mit Wrappern 295
4.10.1 Verstecken von Trojanern mit EliteWrap 296
DEMO: Verstecken von Trojanern mit EliteWrap 297
4.11 Verstecken von Trojanern mit Crypter-Tools 298
DEMO: Verstecken von Trojanern mit Crypter-Tools 298
4.12 Infektion mit Trojanern vermeiden 299
4.13 Trojaner und Backdoors aufspüren 300
4.14 Rootkits - die unsichtbare Gefahr 302
4.14.1 Arten von Rootkits 302
4.14.2 Beispiel: Nuclear Rootkit 303
DEMO: Einsatz von Rootkits unter Windows 304
4.14.3 Rootkits aufspüren 304
4.14.4 Anti-Rootkit-Software - eine Auswahl 305
DEMO: Aufspüren von Rootkits unter Windows 305
4.14.5 Malware-Analyse mit IDA Pro 306
4.15 malpedia - detailreiche Infos zu Malware & Co. 306
4.16 Zusammenfassung 307

Modul 5 - Angriffe auf Drahtlosnetzwerke (WLANs) 309

5.1 Wireless LAN (WLAN)-Grundlagen 310
5.1.2 Nachteile von WLANs 312
5.1.3 Wireless LAN (WLAN)-Typen 314

5.1.4 WLAN-Standards und -Frequenzen 315
5.1.5 IEEE 802.11-Standard und das ISO/OSI-Modell 319
5.1.6 WLAN-Antennentypen 320
5.2 WLAN-Sicherheit 324
5.2.1 Verschlüsselung 325
5.2.2 WEP (Wireless Equivalent Privacy) 325
5.2.3 Verschlüsselung mit WPA und WPA2 326
5.2.4 WLAN-Verschlüsselung 327
5.2.5 Zugriffskontrolle (Access Control) 327
5.2.6 Closed Network 328
5.2.7 IEEE 802.1x/EAP 329
5.2.8 Virtual Private Network (VPN) 330
5.2.9 Open User Authentication (OUA) 331
5.2.10 Traffic Lock - Schutz „innerhalb“ des WLANs 331
5.3 Gefahren für Drahtlosnetzwerke (WLANs) 332
5.3.1 WarChalking-Symbole 333
5.3.2 GPS-Mapping - WLANs finden leicht gemacht… 334
5.3.3 GPS-Mapping - mit WiGLE ganz global und einfach… 334
DEMO: WLANs mit WiGLE.net ermitteln 335
5.3.4 GPS-Mapping - Skyhook 335
5.3.5 Hotspot-Finder-Apps 336
5.4 Footprinting - dem WLAN auf der Spur 336
5.4.1 WiFi-Finder-Tool - inSSIDer 337
5.4.2 Weitere WiFi-Finder-Tools (Auswahl) 337
5.4.3 Weitere WiFi-Finder-Apps (Auswahl) 338
DEMO: Aufspüren von WLANs 339
5.5 „Open System“-Konfiguration 339
5.6 „Gefährliche“ Access Points 340
5.7 Man-In-The-Middle-Attacken 340
5.7.1 Passive Angriffe 341
5.7.2 WLAN Sniffer-Tools (Auswahl) 342
5.7.3 Aktive Angriffe - Umgehen der Access Control-Liste 342
5.7.4 Aktive Angriffe - AirCrack-NG Tools-Suite 343
5.7.5 Aktive Angriffe - Aufdecken versteckter SSIDs 344
DEMO: Ermitteln der BSSID von „versteckten“ WLANs 345
5.8 Aktive Angriffe - Kennwort-Attacken 346

5.8.1 Aktive Angriffe - Kennwort-Attacken mit Aircrack-NG 346
DEMO: WPA und WPA2-Crack mit AirCrack-NG 348
5.8.2 Weitere Passwort-Cracker-Tools (Auswahl) 348
5.9 Aktive Angriffe - Denial of Service-Attacken 349
5.9.1 Aktive Angriffe - WLAN-Störsender (Auswahl) 350
5.10 WLAN-Hack ganz ohne Tools? 350
5.11 Tipps für das Betreiben sicherer WLANs 351
DEMO: (optional) Konfiguration eines WLAN-AccessPoints 352
5.12 Zusammenfassung 353
5.13 Lernzielkontrolle 353
Modul 6 - Firewalls, IDS & Honeypots 355
6.1 Einführung in Firewalls 356
6.2 De-Militarisierte Zone (DMZ) 356
6.3 Filtertechnologien 357
6.4 Einsatzkonzepte für Firewalls 358
6.4.1 Bastion Host 358
6.4.2 Dreifach vernetzte Firewall 359
6.4.3 Back-to-Back-Firewall 359
6.5 Unternehmens-Firewalls 360
6.6 Personal Firewalls 361
DEMO: Konfiguration der Windows-Firewall 361
6.7 Beispiel für das Umgehen einer einfachen Firewall-Lösung 362
6.7.1 Portumleitung mit FPipe 364
DEMO: Verwendung von fpipe.exe für die Portumleitung 366
6.7.2 firewalk - ab durch die Feuerwand 366
6.7.3 HTTPTunnel - Firewalls umgehen 367
6.8 Intrusion Detection Systeme (IDS) 368
6.8.1 Arten von Intrusion Detection Systemen (IDS) 369
6.8.2 Platzierung von Intrusion Detection Systemen (IDS) 370
6.8.3 Eindringversuche erkennen 370
6.8.4 Snort - der „Rüssel“ im Netzwerk 371
DEMO: Bereitstellung von Snort als IDS unter Windows 373
6.8.5 Microsoft Advanced Threat Analytics (ATA) 373
DEMO: (optional) Bereitstellen von Microsoft ATA 374
6.8.6 Microsoft Advanced Threat Protection (ATP) 374
6.8.7 Weitere IDS-Systeme 375

6.9 Honeypots — die Honigtöpfe 375
6.9.1 Honeypots - Verwendungszwecke 376
6.9.2 Honeypots - Einsatzorte 377
6.9.3 Honeypots - Typen 377
6.9.5 KeyFocus KFSensor 378
DEMO: Einsatz von KFSensor als Honeypot 379
6.9.6 SPECTER 379
6.9.7 Weitere Honeypot-Lösungen 381
6.9.8 Honeypots aufspüren 381
6.10 Zusammenfassung 382
Modul 7 - Einführung in Penetrationstests 383
7.1 Zweck eines Penetrationstests 384
7.2 IT-Sicherheit und Penetrationstests 385
7.3 Arten von Penetrationstests 386
7.4 Phasen eines Penetrationstests 386
7.5 Zusammenfassung 389
Anhang A: Portnummern 390
Anhang B: ASCII-Tabelle 396
Anhang C: Wichtige Weblinks 397
Anhang D: Auflösungen zur Lernzielkontrolle 398
Stichwortverzeichnis 400