- Official Courseware -

IT-Sicherheit

(Anti-)Hacking für Administratoren und Systembetreuer

Schwachstellen erkennen und Schutzmaßnahmen erhöhen

Version 12

CertPro® PRESS - *Professional Learning*

IT-Sicherheit:

(Anti-)Hacking für Administratoren und Systemverwalter

Angriffe erkennen und Schutzmaßnahmen verstärken

Version 12

CertPro® PRESS
an Imprint of CertPro® it training & services e.K.

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

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

Artikel-Nr.: HK121021

Print-Ausgabe ISBN 978-3-9447-4967-9
ebook-Ausgabe: ISBN 978-3-9447-4968-6

Autor: Carlo F. Westbrook

Einbandgestaltung: CertPro® it training & services e.K.
Bilder und Grafiken: CertPro® it training & services e.K.
Herstellung: CertPro® it training & services e.K.
Druck und Verarbeitung: WIRmachenDRUCK GmbH, 71522 Backnang
Printed in Germany

Auf einen Blick

Modul 00 - Einführung

Modul 01 - Grundlagen der IT-Sicherheit

Modul 02 - Planung und Vorbereitung von Angriffen

Modul 03 - Moderne Angriffstechniken

Modul 04 - Gefahren durch Viren, Würmer, Rootkits, Trojaner, Ransomware & Co.

Modul 05 - Home-Office als „Einfalltor" für Angreifer

Modul 06 - Schutz durch Firewalls, IDS/IPS & Honeypots

Zusatzdokumentation
(im Umfang der Seminarunterlage enthalten)

Modul 07 - Angriffe auf Drahtlosnetzwerke (WLANs)

Modul 08 - Penetrationstests - Einführung und Überblick

Zusatzdokumentation - optional
(im Umfang des Kurs-Downloads als PDF-Dateien enthalten)

Modul 09 - Grundlagen der Kryptografie

Modul 10 - Einführung ins BSI-Grundschutzkompendium

Website zum Buch

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/HK121021.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 19
Teilnahmevoraussetzungen 19
Zielgruppe 19
Lernziele 20
Kursbeschreibung 20
OPTIONALE MODULE: 22
Wichtiger Hinweis 23
Kursrauminstallation 23
Kurze Einführung in Hyper-V 24
Wichtiger Hinweis zu den Kurstools 24
Einrichtungen 25
Modul 01 - Grundlagen der IT-Sicherheit 27
1.1 Aktuelle Trends und Entwicklungen 28
1.2 Aktuelle Trends und Entwicklungen 28
1.3 Trends und Entwicklung rund um die IT-Sicherheit 29
1.3.1 Ständig wachsendes Bedrohungspotential 31
1.3.2 Die Realität – täglich neue „Opfer“… 31
1.3.3 Die Realität – Angriffe gegen „bekannte“ Webseiten 32
DEMO: Aktuelle „Opfer“ im Internet 32
1.4 Online-Monitore - Cyberattacken in „Echtzeit“ 33
DEMO: Aktuelle „Cyberattacken“ im Internet 33
1.5 Die Realität… - der „offene“ Handel im Internet… 34
1.5.1 Die Realität… - völlig neue Geschäftsmodelle… 34
1.6 Ransomware – moderne Erpresser… 35
1.6.1 CryptoLocker, Locky, TeslaCrypt, WannaCry & Co. 35
1.7 Whaling - die Jagd auf die „großen“ Fische… 36
1.8 Drive-by-Download-Attacken 37
1.9 Identitätsdiebstahl - Traue nicht JEDEM…! 37
1.9.1 Identitäten - Offener Handel im Internet 38
1.10 Malware in sozialen Netzwerken 38
1.11 Gefahr: Malware - versteckt im Dateidownload 39
1.12 Gründe für Angriffe 39

1.13 Arten von Angreifern ... 40
1.13.1 WER? - „Klassische“ Arten von Angreifern ... 41
1.13.2 WER? - Detaillierte Klassifizierung der „Hacker“ ... 43
1.14 Angriffsziele & häufige Arten von Sicherheitslücken ... 44
1.14.1 Potentielle Angriffesziele ... 44
1.14.2 Die „Top 25-Schwachstellen“ ... 45
1.15 Häufige Methoden bei Netzwerkangriffen ... 46
1.15.1 Klassifizierung von Angriffen ... 47
1.15.2 Angriffe von Innen - „Tür und Tor steht offen…“ ... 47
1.15.3 Mögliche Angriffstypen – einige Beispiele ... 48
1.16 Phasen eines (geplanten) Netzwerkangriffs ... 49
1.17 Phasen einer „Advanced-Persistent-Threat“-Attacke ... 50
1.18 Windows-Sicherheitsfeatures aus Sicht des Angreifers ... 50
1.18.1 Windows-Sicherheitsfeatures aus Sicht der Angreifer ... 51
1.18.2 Kernel Mode & User Mode ... 51
Local Security Authority (LSA) ... 52
Win32-Teilsystem ... 52
1.18.3 Secure boot (UEFI) ... 53
1.18.4 Sicherheitsprinzipale ... 53
1.18.5 Benutzerkonten ... 54
1.18.6 Gruppenverwaltete Dienstkonten (gMSA) ... 55
1.18.7 Gruppen ... 56
1.18.8 Computerkonten ... 58
1.18.9 SAM und Active Directory (AD) ... 59
1.18.10 Gruppenrichtlinien und „Richtlinien für Kennwörter (PSOs)“ ... 60
1.18.11 „Als Administrator ausführen…“ ... 61
1.18.12 Benutzerkontensteuerung (UAC) ... 62
1.18.13 Patches & Service Packs ... 63
1.18.14 Windows-Firewall ... 64
1.18.15 Windows Defender ... 65
1.18.16 Schutz der Datenübertragung mit IPSec ... 66
1.18.17 Dateischutz mit NTFS/ReFS und Encrypting File System (EFS) ... 66
1.18.18 BitLocker & BitLocker-to-Go ... 68
1.18.19 Weitere Sicherheitsfeatures ... 69
1.19 Wichtige Sicherheitsprinzipien ... 69
1.20 Schutz durch mehrstufige Verteidigung ... 70

1.21 Rechtliche Grundlagen 71
1.21.1 Strafbare Handlungen 72
1.21.2 Straftatbestände nach StGB und UWG 74
1.21.3 Strafanzeige und Strafantrag 78
1.21.4 Beweismittel 79
1.22 Zusammenfassung 80
1.23 Lernzielkontrolle 81

Modul 02 - Planung und Vorbereitung von Angriffen 83

2.1 Footprinting - dem Opfer auf der Spur 84
2.2 Ziele des Footprinting 86
2.3 Durchstöbern von Informationsquellen 88
2.3.1 Suche nach Firmeninformationen im Internet 88
2.3.2 „Gelbe Seiten“, Telefonbücher & Co. 89
2.4 Suche nach Webseiten 89
2.5 Google als „Proxy-Server“ missbrauchen 90
DEMO: Aufruf von Cache-Inhalten in Google 90
2.6 Google-Hacking – Opfersuche leicht gemacht 91
2.6.1 Google-Hacking - Erweiterte Suche-Operatoren (Auszug) 91
2.6.2 Google-Suche nach Verzeichnissen 92
2.6.3 Google-Suche nach Servern 93
2.6.4 Suche nach Diensten im Internet 94
DEMO: Verwendung von Such-Operatoren in Google 94
2.7 Die “Google-Hacking Database” 95
2.8 Exploit-DB.com - „aktuelles“ Google-Hacking 96
DEMO: Google-Hacking mithilfe von exploit-db.com 96
2.12 „archive.org“ - Zurück in die Vergangenheit 96
DEMO: Internet-Recherche mithilfe von „archive.org“ 97
2.9 „Internet der Dinge“ - die schöne, neue Welt… 98
2.10 Angriffe - durch Haushaltsgeräte und Kameras 98
2.11 Shodan.io - Kühlschränke, TV-Geräte, SmartHome und mehr… 99
DEMO: Recherche im „Internet der Dinge“ (IoT) 99
2.12 Firmenwebsite und Stellenausschreibungen 100
2.13 Suche in verschiedenen „Job-Börsen“ im Internet 100
DEMO: Internet-Recherche in Online-Jobbörsen 101
2.14 Personensuche im Internet - „Nicknames“ 101
2.15 Suche in „Social Networks“ 102

DEMO: Personensuche im Internet 102
2.16 OSINT-Framework - Suche übersichtlich und leicht gemacht 103
DEMO: Suchoptionen im OSINT-Framework 103
2.17 Suchmaschinen, Usenet & Newsgroups 104
2.18 Maltego - professionelle Recherche 105
2.19 FOCA (Fingerprinting Organizations with Collected Archives) 106
2.20 Footprinting-Tools (Auswahl) 106
2.21 HTTrack Web Site Copier 107
2.21.1 Website-Kopiertools (Auswahl) 108
DEMO: Kopieren einer Webseite mit HTTrack Web Site Copier 108
2.22 Webbasierte Zugänge zu Netzwerkdiensten 109
2.23 Google-Earth, Bing Maps & Co. 110
DEMO: „Vogelperspektive“ von Gebäuden 111
2.24 Read Notify - “Invisible tracking” und mehr… 111
2.24.1 E-Mail-Tracking-Tools (Auswahl) 112
DEMO: „Invisible Tracking“ mittels Readnotify.com 112
2.25 DNS-Abfragen & WHOIS 113
DEMO: Domäneninhaber mittels DeNIC & Internic ermitteln 114
2.26 Ermittlung des Inhabers bestimmter IP-Adressen 115
DEMO: Ermitteln des Inhabers bestimmter IP-Adressen 115
2.26.1 WHOIS-Tools (Auswahl) 116
2.26.2 WhatIsMyIP.com - Wer bin ich überhaupt? 116
2.27 „LSD“-Abfragen an DNS-Server 117
2.27.1 DNS-Eintragstypen (Auswahl) 118
2.27.2 DNS-Informationen abrufen und auswerten 119
DEMO: Ermitteln von DNS-Informationen im Internet 119
2.28 Routenverfolgung mit Traceroute 120
2.28.1 Grafische Traceroute-Tools 121
2.28.2 Traceroute-Tools (Auswahl) 122
DEMO: Einsatz von Traceroute-Tools im Internet 123
2.29 Scanning - die Suche nach der offenen „Tür“ 123
2.30 Rechner orten — am Anfang steht die Suche 125
2.30.1 Ermittlung von Computern mithilfe des Ping-Befehls und ARP 125
DEMO: Ermitteln von Computersystemen mittels Ping und ARP 127
2.30.2 Angry IP (Ping Sweep-Tool) 127
2.30.3 Ping Sweep-Tools (ICMP-Scanner) (Auswahl) 128

DEMO: Rechnersuche mit “Angry IP” 128
2.31 Portscan-Tools 129
2.31.1 SuperScan 129
2.31.2 Network Mapper (nmap) 130
DEMO: Portscans mittels nmap unter Windows 133
2.31.3 Portscan-Tools (ICMP-Scanner) (Auswahl) 137
2.31.4 Portscan-„Light“ mit telnet 137
2.31.5 Portscans erkennen 139
2.32 Enumeration - Server und Betriebssysteme ausspähen 140
2.33 Ausspähen der NetBIOS-Name Services 140
2.33.1 Ausspähen von Arbeitsgruppen und Domänen 141
2.33.2 Auflistung aller Domänencontroller 142
2.33.3 Auflistung der Sicherheitsrichtlinie für Benutzerkennwörter 142
2.33.4 Abfragen von lokalen und Domänen-Benutzerkonten 143
2.33.5 Abfrage der Rollen von Computersystemen 143
2.33.6 Verhindern der NetBIOS-Name Service-Ausspähung 145
2.34 Ausspähen des Administrator-Kontos 145
DEMO: Ermitteln des Administratorkontos 147
2.35 Auflisten vorhandener SMB-Sitzungen mit NetSess.exe 148
DEMO: Auflisten vorhandener SMB-Sitzungen 148
2.36 Unix/Linux ausspähen 149
2.36.1 Verhindern der RPC-Ausspähung unter Unix/Linux 151
2.37 Benutzer unter UNIX/Linux abfragen 151
2.37.1 Abfragemöglichkeiten über rwho und rusers verhindern 152
2.38 Suche nach passenden Exploits 152
2.38.1 Exploit-Kategorien 153
2.38.2 Exploits im Internet 154
DEMO: Ermitteln aktueller Exploits 155
2.38.3 Metasploit-Framework — Exploits für alle 155
2.38.4 MetaSploit Express & Pro - kostenpflichtige Varianten 156
2.38.5 Immunity CANVAS 157
2.39 Schwachstellen vorbeugen: Patch-Management 158
2.39.1 Update-Management mit WSUS 158
DEMO: Manueller Download von Patches 159
2.40 Schwachstellen-Scanner 159
2.40.1 Verfügbare Schwachstellen-Scanner (Auswahl) 160

DEMO: Einsatz von Schwachstellen-Scannern 160
2.41 Angriffsplan erstellen 161
2.42 „Domain Dominance“ - Macht über alles… 161
2.43 Angriffe verschleiern mittels offener Proxyserver 162
2.43.1 Proxy Chaining - effektiv verstecken 162
2.43.2 Verschleiern leicht gemacht - Proxy Switcher 163
2.43.3 Verschleiern leicht gemacht - Proxy Workbench 163
2.43.4 Proxy-Tools (Auswahl) 164
DEMO: Open Proxy-Server im Internet 164
2.43.5 TOR und CyberGhost 165
2.44 Botnets - alle für einen… 166
2.45 Zusammenfassung 167
2.46 Lernzielkontrolle 168
Modul 03 - Moderne Angriffstechniken 169
3.1 Gefahrenpotential: Physikalische Angriffe 169
3.1.1 Gefahren für Gebäude, Serverräume und Rechenzentren 170
3.1.2 Gefahren für Netzwerkgeräte und -verbindungen 171
3.2 Schutz gegen Angriffe auf Gebäude, Serverräume, Netzwerkgeräte & -verbindungen 172
3.2.1 Schutzmaßnahmen: JA, aber bitte nicht so… 173
3.3 Gefahren für Computersysteme 173
3.3.1 BIOS-Kennwörter „knacken“ 174
3.4 Benutzerkennwörter zurücksetzen 175
3.4.1 NTCrack & Co. - Passwort-Reset leichtgemacht 175
3.4.2 Kommerzielle Tools zum Passwort-Zurücksetzen 176
3.4.3 Ophcrack Live-CD - Passwort-Crack für „Jedermann“ 177
3.5 Installations-DVD - Windows aushebeln leicht gemacht 178
DEMO: Angriff mithilfe der Installations-DVD 178
3.6 Physikalischer Angriffe mit Keyloggern 179
3.6.1 Hardware-Keylogger - eine Auswahl 180
DEMO: Einsatz von Hardware-Keyloggern 180
3.7 Schutz gegen physikalische Angriffe auf Computersysteme 181
3.8 Software-Keylogger - die unsichtbare Gefahr 181
3.8.1 Software-Keylogger - eine Auswahl 182
3.9 USB-Spyware & Co. - die oft „verkannte“ Gefahr 182
3.10 Schutz gegen Software-Keylogger & Spyware 183
3.11 Gefahren für mobile Computersysteme 183

3.12 Social Engineering - „Feinde unter uns…“ 184
3.12.1 Social Engineering - in Kinofilmen vorgemacht 185
3.12.2 Typischer Social Engineering-Angriff - per „Vishing“ 185
3.12.3 Caller ID Spoofing - (Ver-)kenne Deinen Anrufer… 186
DEMO: Caller ID-Spoofing-Anbieter im Internet 186
3.12.4 Eavesdropping - in der Regel völlig unbemerkt… 187
3.12.5 „Shoulder Surfing“ — ohne großen Aufwand 187
3.12.6 „Shoulder Surfing“ — auch mit Hilfsmitteln möglich 188
DEMO: Einsatz von Spycams 189
3.12.7 Impersonation Attack - Frechheit siegt… 189
3.12.8 „Piggy Backing“ und „Tail Gating“ 189
3.12.9 „Dumpster Diving“ — die Mühe lohnt sich oft 190
3.12.10 „Dumpster Diving“ - im Home-Office 190
3.12.11 Smishing - Phishing-Angriff mittels SMS-Nachricht 191
3.12.12 USB-Sticks & Co. - die oft unerkannten Gefahren… 191
3.12.13 Alternativ: Parkplatz 192
3.12.14 USB-Stick - Malware einfach in den Briefkasten… 193
3.13 Schutz gegen Social Engineering-Attacken 193
3.14 Electronic Social Engineering 194
3.14.1 Phishing 194
3.14.2 Phishing - Typisches Beispiel für Phishing-E-Mails 195
3.14.3 Professionelles Phishing 195
3.14.4 Phishing - aufs Home-Office angepasst… 196
3.14.5 Spear-Phishing - Opfer beim Namen genannt 196
3.14.6 „Dynamit Phising“ - mittels Emotet & Co. 197
3.14.7 Vorbereitende Schritte der Phisher 197
3.15 Spam-Attacken - auch ein Mittel der Phisher… 198
DEMO: „Gesichter“ der Spammer 198
3.15.1 PhishTank - Anti-Phishing-Webseite 198
DEMO: Überblick über Phishing-Webseiten 199
3.15.2 Selbsttest - Online jederzeit machbar… 199
3.16 Klicken - oder besser nicht…? 200
3.17 Pharming - die Unterstützung für den Phisher 201
DEMO: Pharming-Versuch unter Windows 201
3.18 Phishing/Pharming - ein Paradebeispiel aus der Praxis… 202
3.19 Phishing-Tricks - Basis 10-Adressen… 202

3.20 Phishing-Tricks - Kurz-URL-Dienste… 203
3.21 Überprüfung unbekannter URLs in E-Mails 204
DEMO: Untersuchen unbekannter URLs 204
3.22 Schutz gegen Phishing- und Pharming 205
3.23 Informationssammlung in Social Networks 206
3.24 „Reverse“-Bildersuche im Internet 206
3.25 Twitter-Scams & Co. - Trau, Schau, Wem… 207
3.26 Phising - in sozialen Netzwerken 207
3.26.1 Schutzmöglichkeiten gegen Angriffe in Social Networks 208
3.27 Angriffe mit Sniffer-Tools 208
3.27.1 WireShark 209
3.27.2 Nach Kennwort-Hashes “sniffen“ 210
3.27.3 Sniffer-Attacken vorbereiten 210
3.27.4 Aktive Sniffing-Attacke 212
3.27.5 Passive Sniffing-Attacke 213
DEMO: Sniffing von Kennwörtern mit Cain & Abel 214
3.28 ARP-Spoofing aufspüren mit XArp 214
3.28.1 Sniffer-Angriffen vorbeugen 215
3.29 Angriffe auf Kennwörter 216
3.29.1 Kennwörter — und sichere Kennwörter 217
3.29.2 (Un-)Sichere Kennwörter 218
3.29.3 Das „Problem“ mit den GPUs 219
3.30 Angriffe auf Passwörter in Windows-Netzwerken 220
3.30.1 Windows und Passwörter 221
3.30.2 Verbesserungen mit NTLMv2 222
3.31 Speicherung von Kennwörtern in Windows SAM 223
3.32 Kerberos V5-Protokoll 223
3.33 Methoden für den Angriff auf Kennwörter 225
3.33.1 Kennwörter erraten 226
3.33.2 Erraten von Kennwörtern automatisieren 226
3.34 Schutz gegen das Erraten von Kennwörtern 227
3.34.1 Kontosperrungsschwelle konfigurieren 228
3.35 CrackStation - Online-Entschlüsselung von Kennwort-Hashes 229
DEMO: Online-Angriff auf Kennwort-Hashes mit CrackStation 230
3.36 Absichern der Authentifizierung 230
3.37 Nach Kennwörtern „sniffen“ 233

3.38 (Remote-)Kennwörter „knacken“ 234
3.38.1 L0phtCrack 235
3.38.2 Elcomsoft Distributed Password Recovery 236
3.38.3 Weitere Passwort-Cracker 236
DEMO: Angriffe auf Kennwörter 237
3.39 Schutz gegen Passwort-Cracker 237
3.39.1 Sicherheitsgruppe „Protected Users“ 238
3.39.2 KeePass & Co. - praktische Helfer 239
3.40 Pass-the-Hash und Pass-the-Ticket - Entschlüsseln nicht nötig 239
DEMO: Angriffe auf Kennwörter mit Mimikatz, WCE & Co. 240
3.41 Windows Defender Credential Guard & ATA 249
3.42 Tricks der Hacker - Dateien verstecken 250
3.42.1 Alternative Datenströme (ADS) 250
DEMO: Daten in alternativen Datenströmen (ADS) verstecken inkl. Hardlink 252
3.42.2 In NTFS versteckte Dateien aufspüren 252
3.42.3 Steganografie - vielfältige Möglichkeiten zum Verstecken 253
DEMO: Übersicht über Steganografie-Tools 255
3.43 Zusammenfassung 255
3.44 Lernzielkontrolle 256

Modul 04 - Gefahren durch Viren, Würmer, Rootkits, Trojaner, Ransomware & Co. 257

4.1 Computerviren - die „betagte“ Gefahr 257
4.1.1 Virusdefinition 258
4.1.2 Virus-Kategorien 258
DEMO: Analysieren von Virendateien (optional) 261
4.1.3 Virenbaukästen aus dem Internet 261
4.1.4 Computerviren und -würmer - Infektionswege 262
4.2 Computerwürmer - Fortpflanzung ist alles… 262
4.3 Schutz vor Viren und Würmern 263
4.3.1 Antivirus-Software - vielfältiges Angebot 264
4.3.2 Testviren & Co. 265
DEMO: Verwendung von Antivirus-Software (optional) 265
4.4 Online-Tests für Dateien 266
DEMO: Online-Überprüfung von Dateien 266
4.5 Spyware - die oft „verkannte“ Gefahr 267
4.6 Schutz vor Spyware 267

4.7 Trojaner - die Macht der Angreifer… 268
4.7.1 Trojaner-Arten 268
4.7.2 Trojaner-Ports 269
4.7.3 Bekannte Trojaner-Programme 270
4.7.4 OptixPro 271
4.7.5 Weitere Backdoor-Tools & Trojaner 272
4.7.6 DarkComet-RAT, BlackShades & Co. - aktuelle Gefahren 273
DEMO: Einsatz von Trojanern 273
4.7.7 Infektionsmöglichkeiten mit Trojanern 274
4.8 Vortäuschen bestimmter Dateitypen 274
4.9 Verstecken von Trojanern mit Wrappern 276
4.9.1 Verstecken von Trojanern mit EliteWrap 276
DEMO: Verstecken von Trojanern mit EliteWrap (optional) 277
4.10 Verstecken von Trojanern mit Crypter-Tools 278
DEMO: Verstecken von Trojanern mit Crypter-Tools 278
4.11 Infektion mit Trojanern vermeiden 279
4.12 Trojaner und Backdoors aufspüren 280
4.13 Rootkits - die unsichtbare Gefahr… 282
4.13.1 Arten von Rootkits 282
4.13.2 Beispiel: Nuclear Rootkit 283
DEMO: Einsatz von Rootkits unter Windows (optional) 284
4.13.3 Rootkits aufspüren 284
4.13.4 Anti-Rootkit-Software - eine Auswahl… 285
DEMO: Aufspüren von Rootkits unter Windows (optional) 285
4.14 Ransomware - moderne Erpresser… 285
4.14.1 Bekannte Ransomware 286
4.15 Schutz vor Ransomware mittels FSRM, Ordner-Schutz & Co. 286
4.16 malpedia - detailreiche Infos zu Malware & Co. 287
4.17 Zusammenfassung 287

Modul 05 - Home-Office als „Einfalltor“ für Angreifer 289

5.1 Computerviren - die „betagte“ Gefahr 289
5.2 Online-Monitore - Cyberattacken in „Echtzeit“ 290
DEMO: Aktuelle „Cyberattacken“ im Internet 291
5.3 Opfer-Suche leicht gemacht… 291
5.3.1 Suche in „Social Networks“ 292
DEMO: Mitarbeitersuche mittels Google, Xing & Co. 292

5.3.2 Personensuche im Internet - „Nicknames“… 292
DEMO: Suche nach „Nicknames“ im internet 293
5.3.3 „Internet der Dinge“ (IoT) - die schöne neue Welt… 293
5.3.4 Missbrauch von Haushaltsgräten und Kameras für Angriffe 294
5.3.5 Aufspürbar: Remote-Zugriffe mittels RDP, VPN & Co. 294
DEMO: Suche nach Haushaltsgeräten, RDP & Co. 295
5.4 Social Engineering - mögliche Angriffe im Home-Office 295
5.4.1 Typischer „Social Engineering“-Angriff per Telefon 296
5.4.2 Caller ID Spoofing - (Ver-)kenne Deinen Anrufer… 296
5.4.3 Impersonation Attack - teils auch im Home-Office… 297
5.4.4 Dumpster Diving - im Home-Office, es lohnt sich meist 297
5.5 Phishing & Co. im Home-Office 298
5.5.1 Angepasste und oft echt wirkende Phishing-Mails 298
5.5.2 Makroviren - oft als Word-Doku im Mail-Anhang 299
5.5.3 Der Einstieg - im Home-Office 299
5.6 USB-Stick - Alternative zur „klassischen“ E-Mail 300
5.7 Exploit-Kategorien - Futter für den USB-Stick 300
5.8 Trojaner - die Macht der Angreifer… 301
5.8.1 Trojaner-Arten 301
DEMO: Einsatz von Trojanern 302
5.8.2 Infektionsmöglichkeiten mit Trojanern 302
5.9 Bots - als Teil eines Angriffs… 303
5.9.1 Denial-of-Service (DoS)-Attacken mittels „Bots“ 304
5.10 Verstecken von Trojanern mit Crypter-Tools 304
5.10.1 Verschlüsselung mit WPA oder besser: WPA2 305
5.10.2 Zugriffskontrolle (Access Control) 305
5.10.3 Closed Network 306
5.10.4 Gefahren für Drahtlosnetzwerke (WLANs) 306
5.10.5 GPS-Mapping - WLANs finden leicht gemacht… 307
DEMO: WLANs mit Wigle.net ermitteln 307
5.10.6 Man-in-the-Middle-Angriff auf Home-Office-WLANs 308
5.10.7 Passive Angriffe 308
5.10.8 Aktive Angriffe - Umgehen der Access Control-Liste 309
5.10.9 Aktive Angriffe - AirCrack-NG Tools-Suite 309
5.10.10 Aktive Angriffe - Denial of Service-Atttacke 310
5.11 WLAN-Hack ganz ohne Tools? 310

5.12 Weitere Gefahren im Home-Office 311
5.13 Die 5 wichtigsten Schritte für sicheres Arbeiten von Zuhause 311
5.14 Sichere Teilnahme an Video-Konferenzen 314
5.15 Sicherer Umgang mit Passwörtern 315
5.15.1 KeePass & Co. - praktsiche Helfer auch für Zuhause 315
5.16 Tipps für den „sicheren Arbeitsplatz“ 316
5.16.1 Datenverschlüsselung mittels BitLocker 316
5.17 Sicherer Internet-Zugang vom Home-Office 317
5.18 Ausstattung im Home-Office zur Absicherung 317
5.19 KeePass & Co. - praktsiche Helfer auch für Zuhause 318
5.20 Motto: Gib Hackern keine Chance! 319
5.21 Zusammenfassung 319

Modul 06 - Schutz durch Firewalls, IDS/IPS & Honeypots 321

6.1 Einführung in Firewalls 322
6.2 Filtertechnologien 322
6.3 Next Generation Firewalls (NGFWs) 323
6.4 Einsatzkonzepte für Firewalls 324
6.4.1 Bastion Host 324
6.4.2 Dreifach vernetzte Firewall / DMZ 325
6.4.3 Back-to-Back-Firewall 325
6.5 Unternehmens-Firewalls 327
DEMO: Konfiguration einer Netzwerk-Firewall 327
6.6 Personal Firewalls 328
DEMO: Konfiguration der Windows-Firewall 328
6.7 HTTPTunnel - Firewalls umgehen 329
6.7.1 TeamViewer, AnyDesk & Co. 329
6.8 Intrusion Detection Systeme (IDS) 330
6.8.1 Arten von Intrusion Detection Systemen (IDS) 330
6.8.2 Platzierung von Intrusion Detection Systemen (IDS) 331
6.8.3 Eindringversuche erkennen 331
6.8.4 Snort - der „Rüssel“ im Netzwerk 332
DEMO: Bereitstellung von Snort als IDS unter Windows 334
6.8.5 Microsoft Advanced Threat Analytics (ATA) 334
DEMO: (optional) Bereitstellen von Microsoft ATA 335
6.8.6 Microsoft Advanced Threat Protection (ATP) 335
6.8.7 Weitere IDS/IPS-Systeme 336

6.9 Honeypots — die Honigtöpfe 337
6.9.1 Honeypots - Verwendungszwecke 338
6.9.2 Honeypots - Einsatzorte 338
6.9.3 Honeypots - Typen 339
6.9.4 KeyFocus KFSensor 339
DEMO: Einsatz von KFSensor als Honeypot 341
6.9.5 Honeypots (Auswahl) 341
6.10 Zusammenfassung 342
- Zusatzdokumentation - 343
Modul 07 - Angriffe auf Drahtlosnetzwerke (WLANs) 343
7.1 Wireless LAN (WLAN)-Grundlagen 344
7.1.2 Nachteile von WLANs 346
7.1.3 Wireless LAN (WLAN)-Typen 347
7.1.4 WLAN-Standards und -Frequenzen 348
7.1.5 IEEE 802.11-Standard und das ISO/OSI-Modell 351
7.1.6 WLAN-Antennentypen 353
7.2 WLAN-Sicherheit 356
7.2.1 Verschlüsselung 356
7.2.2 WEP (Wireless Equivalent Privacy) 357
7.2.3 Verschlüsselung mit WPA und WPA2 357
7.2.4 WLAN-Verschlüsselung 358
7.2.5 Zugriffskontrolle (Access Control) 358
7.2.6 Closed Network 359
7.2.7 IEEE 802.1x/EAP 359
7.2.8 Virtual Private Network (VPN) 360
7.2.9 Open User Authentication (OUA) 361
7.2.10 Traffic Lock - Schutz „innerhalb“ des WLANs 361
7.3 Gefahren für Drahtlosnetzwerke (WLANs) 361
7.3.1 WarChalking-Symbole 362
7.3.2 GPS-Mapping - WLANs finden leicht gemacht… 362
7.3.3 GPS-Mapping - mit WiGLE ganz global und einfach… 362
DEMO: WLANs mit WiGLE.net ermitteln 363
7.3.4 GPS-Mapping - Skyhook 363
7.3.5 Hotspot-Finder-Apps 363
7.4 Footprinting - dem WLAN auf der Spur 363

7.4.1 WiFi-Finder-Tool - inSSIDer ... 364
7.4.2 Weitere WiFi-Finder-Tools (Auswahl) ... 364
7.4.3 Weitere WiFi-Finder-Apps (Auswahl) ... 365
DEMO: Aufspüren von WLANs ... 365
7.5 „Open System“-Konfiguration ... 365
7.6 „Gefährliche“ Access Points ... 365
7.7 Man-In-The-Middle-Attacken ... 366
7.7.1 Passive Angriffe ... 366
7.7.2 WLAN Sniffer-Tools (Auswahl) ... 366
7.7.3 Aktive Angriffe - Umgehen der Access Control-Liste ... 367
7.7.4 Aktive Angriffe - AirCrack-NG Tools-Suite ... 367
7.7.5 Aktive Angriffe - Aufdecken versteckter SSIDs ... 368
DEMO: Ermitteln der BSSID von „versteckten“ WLANs ... 369
7.8 Aktive Angriffe - Kennwort-Attacken ... 369
7.8.1 Aktive Angriffe - Kennwort-Attacken mit Aircrack-NG ... 370
DEMO: WPA und WPA2-Crack mit AirCrack-NG ... 371
7.8.2 Weitere Passwort-Cracker-Tools (Auswahl) ... 371
7.9 Aktive Angriffe - Denial of Service-Attacken ... 371
7.9.1 Aktive Angriffe - WLAN-Störsender (Auswahl) ... 372
7.10 WLAN-Hack ganz ohne Tools? ... 372
7.11 Tipps für das Betreiben sicherer WLANs ... 373
DEMO: (optional) Konfiguration eines WLAN-AccessPoints ... 374
7.12 Zusammenfassung ... 374
Modul 08 - Einführung in Penetrationstests ... 375
8.1 Zweck eines Penetrationstests ... 375
8.2 IT-Sicherheit und Penetrationstests ... 376
8.3 Arten von Penetrationstests ... 377
8.4 Phasen eines Penetrationstests ... 377
8.5 Zusammenfassung ... 379
Anhang A: Portnummern ... 381
Anhang B: ASCII-Tabelle ... 387
Anhang C: Wichtige Weblinks ... 389
Anhang D: Auflösungen zur Lernzielkontrolle ... 391
Stichwortverzeichnis ... 393

