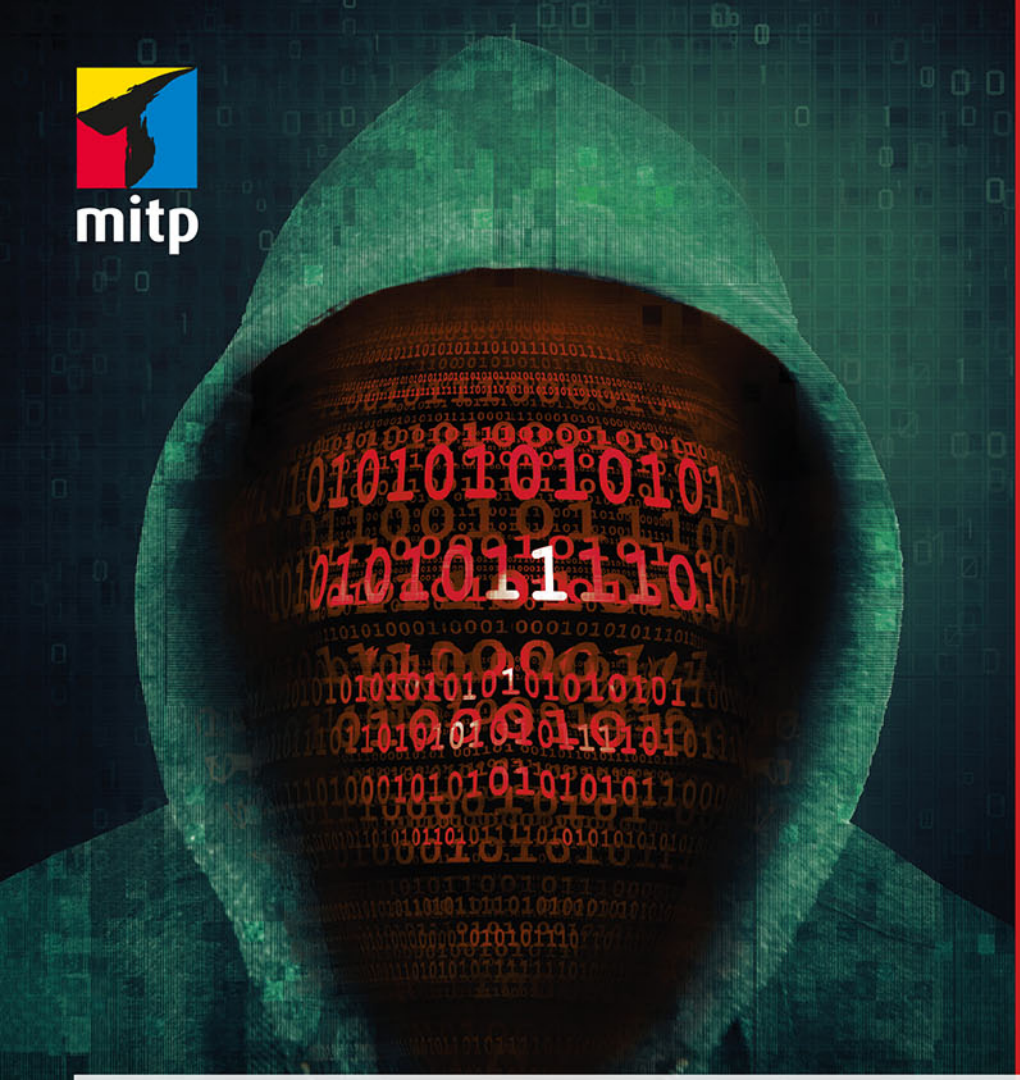

mitp

Eric Amberg

Daniel Schmid

2. Auflage

Hacking

Der umfassende Praxis-Guide

Inkl. Prüfungsvorbereitung zum CEHv11

Eric Amberg, Daniel Schmid

Hacking

Der umfassende Praxis-Guide

Inkl. Prüfungsvorbereitung zum CEHv11

mitp

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

ISBN 978-3-7475-0483-3
2. Auflage 2022

www.mitp.de
E-Mail: mitp-verlag@sigloch.de
Telefon: +49 7953 / 7189 - 079
Telefax: +49 7953 / 7189 - 082

Lektorat: Sabine Schulz
Sprachkorrektorat: Petra Heubach-Erdmann
Covergestaltung: Christian Kalkert
Bildnachweis: © adimas / stock.adobe.com
Satz: III-satz, Husby, www.drei-satz.de

Inhaltsverzeichnis

Einleitung 29

Über die Autoren 35

Danksagung 36

Teil I Grundlagen und Arbeitsumgebung 37

1 Grundlagen Hacking und Penetration Testing 41

1.1 Was ist Hacking? 42

1.2 Die verschiedenen Hacker-Typen 43

1.3 Motive und Absichten eines Hackers 45

1.3.1 Das Motiv 45

1.3.2 Ziel des Angriffs 46

1.4 Ethical Hacking 47

1.5 Der Certified Ethical Hacker (CEHv11) 49

1.5.1 Was steckt dahinter? 49

1.5.2 Die CEHv11-Prüfung im Detail 50

1.6 Die Schutzziele: Was wird angegriffen? 51

1.6.1 Vertraulichkeit 51

1.6.2 Integrität 53

1.6.3 Verfügbarkeit 55

1.6.4 Authentizität und Nicht-Abstreitbarkeit 56

1.6.5 Die Quadratur des Kreises 56

1.7 Systematischer Ablauf eines Hacking-Angriffs 58

1.7.1 Phasen eines echten Angriffs 58

1.7.2 Unterschied zum Penetration Testing 60

1.8 Praktische Hacking-Beispiele 62

1.8.1 Angriff auf den Deutschen Bundestag 62

1.8.2 Stuxnet – der genialste Wurm aller Zeiten 63

1.8.3 Angriff auf heise.de mittels Emotet 63

1.9 Zusammenfassung und Prüfungstipps 64

1.9.1 Zusammenfassung und Weiterführendes 64

1.9.2 CEH-Prüfungstipps 64

1.9.3 Fragen zur CEH-Prüfungsvorbereitung 65

2 Die Arbeitsumgebung einrichten 67

2.1 Virtualisierungssoftware 68

2.1.1 Software-Alternativen 69

2.1.2 Bereitstellung von VirtualBox 70

2.2 Die Laborumgebung in der Übersicht . . . 71
2.3 Kali Linux . . . 72
2.3.1 Einführung . . . 72
2.3.2 Download von Kali Linux als ISO-Image . . . 73
2.3.3 Kali Linux als VirtualBox-Installation . . . 74
2.3.4 Kali Linux optimieren . . . 79
2.4 Windows 10 als Hacking-Plattform . . . 83
2.4.1 Download von Windows 10 . . . 83
2.4.2 Windows-10-Installation in VirtualBox . . . 84
2.4.3 Windows 10 – Spyware inklusive . . . 85
2.4.4 Gasterweiterungen installieren . . . 85
2.5 Übungsumgebung und Zielscheiben einrichten . . . 86
2.5.1 Metasploitable . . . 87
2.5.2 Die Netzwerkumgebung in VirtualBox anpassen . . . 90
2.5.3 Multifunktionsserver unter Linux . . . 92
2.5.4 Windows XP und andere Betriebssysteme . . . 93
2.5.5 Eine Windows-Netzwerkumgebung aufbauen . . . 93
2.6 Zusammenfassung und Weiterführendes . . . 94

3 Einführung in Kali Linux . . . 95
3.1 Ein erster Rundgang . . . 95
3.1.1 Überblick über den Desktop . . . 96
3.1.2 Das Startmenü . . . 99
3.1.3 Der Dateimanager . . . 101
3.1.4 Systemeinstellungen und -Tools . . . 103
3.2 Workshop: Die wichtigsten Linux-Befehle . . . 104
3.2.1 Orientierung und Benutzerwechsel . . . 105
3.2.2 Von Skripts und Dateiberechtigungen . . . 107
3.2.3 Arbeiten mit Root-Rechten . . . 109
3.2.4 Das Dateisystem und die Pfade . . . 112
3.2.5 Dateien und Verzeichnisse erstellen, kopieren, löschen etc. . . . 113
3.2.6 Dateien anzeigen . . . 114
3.2.7 Dateien finden und durchsuchen . . . 115
3.2.8 Die Man-Pages: Hilfe zur Selbsthilfe . . . 118
3.2.9 Dienste starten und überprüfen . . . 119
3.3 Die Netzwerk-Konfiguration anzeigen und anpassen . . . 121
3.4 Software-Installation und -Update . . . 124
3.4.1 Die Paketlisten aktualisieren . . . 124
3.4.2 Installation von Software-Paketen . . . 125
3.4.3 Software suchen . . . 126
3.4.4 Entfernen von Software-Paketen . . . 126
3.5 Zusammenfassung und Prüfungstipps . . . 127
3.5.1 Zusammenfassung und Weiterführendes . . . 127
3.5.2 CEH-Prüfungstipps . . . 127
3.5.3 Fragen zur CEH-Prüfungsvorbereitung . . . 127

4 Anonym bleiben und sicher kommunizieren ... 129
4.1 Von Brotkrumen und Leuchtspuren ... 129
4.2 Proxy-Server – schon mal ein Anfang ... 131
4.2.1 Grundlagen – so arbeiten Proxys ... 131
4.2.2 Einen Proxy-Server nutzen ... 132
4.2.3 Öffentliche Proxys in der Praxis ... 133
4.2.4 Vor- und Nachteile von Proxy-Servern ... 135
4.2.5 Proxy-Verwaltung mit FoxyProxy ... 136
4.3 VPN, SSH und Socks – so bleiben Black Hats anonym ... 136
4.3.1 Virtual Private Networks (VPN) ... 137
4.3.2 SSH-Tunnel ... 139
4.3.3 SOCKS-Proxy ... 141
4.3.4 Kaskadierung für höchste Anonymität und Vertraulichkeit ... 145
4.3.5 Proxifier – Für unwillige Programme ... 146
4.4 Deep Web und Darknet – im Untergrund unterwegs ... 146
4.4.1 Wo geht es bitte zum Untergrund? ... 146
4.4.2 Das Tor-Netzwerk ... 148
4.4.3 Das Freenet Project ... 153
4.4.4 Die Linux-Distribution Tails ... 154
4.5 Anonym mobil unterwegs ... 156
4.5.1 Mobile Proxy-Tools und Anonymizer ... 156
4.6 Sonstige Sicherheitsmaßnahmen ... 157
4.6.1 System säubern mit dem CCleaner ... 158
4.6.2 G-Zapper: Cookies unter Kontrolle ... 159
4.7 Zusammenfassung und Prüfungstipps ... 159
4.7.1 Zusammenfassung und Weiterführendes ... 159
4.7.2 CEH-Prüfungstipps ... 160
4.7.3 Fragen zur CEH-Prüfungsvorbereitung ... 161

5 Kryptografie und ihre Schwachstellen ... 163
5.1 Einführung in die Krypto-Algorithmen ... 164
5.1.1 Alice und Bob ... und Mallory ... 164
5.1.2 Algorithmen und Schlüssel ... 165
5.1.3 Das CrypTool – Kryptografie praktisch erfahren ... 166
5.2 Die symmetrische Verschlüsselung ... 167
5.2.1 Grundlagen der symmetrischen Verfahren ... 167
5.2.2 Verschlüsselung im alten Rom: Die Cäsar-Chiffre ... 168
5.2.3 Strom- und Blockchiffre ... 168
5.2.4 Vor- und Nachteile von symmetrischen Algorithmen ... 169
5.2.5 Wichtige symmetrische Algorithmen ... 169
5.2.6 Symmetrische Verschlüsselung in der Praxis ... 172
5.3 Die asymmetrische Verschlüsselung ... 175
5.3.1 Wo liegt das Problem? ... 175
5.3.2 Der private und der öffentliche Schlüssel ... 175
5.3.3 Der Schlüsselaustausch ... 176

5.3.4 Authentizitätsprüfung . . . 178
5.3.5 Wichtige asymmetrische Algorithmen . . . 179
5.4 Hash-Algorithmen . . . 181
5.4.1 Ein digitaler Fingerabdruck . . . 181
5.4.2 Integritätsprüfung mit Hashwerten . . . 182
5.4.3 Wichtige Hash-Algorithmen . . . 185
5.5 Digitale Signaturen . . . 188
5.5.1 Das Prinzip der digitalen Signatur . . . 188
5.5.2 Wichtige Verfahren der digitalen Signatur . . . 189
5.6 Public-Key-Infrastrukturen (PKI) . . . 190
5.6.1 Das Prinzip von PKI . . . 190
5.6.2 Digitale Zertifikate . . . 191
5.6.3 Zertifikate und PKI in der Praxis . . . 192
5.6.4 Zertifikatssperrlisten und OCSP . . . 195
5.7 Virtual Private Networks (VPN) . . . 197
5.7.1 IPsec-VPNs . . . 198
5.7.2 SSL-VPNs . . . 200
5.8 Angriffe auf kryptografische Systeme . . . 201
5.8.1 Methodologie der Kryptoanalyse . . . 201
5.8.2 Der Heartbleed-Angriff . . . 204
5.8.3 Des Poodles Kern – der Poodle-Angriff . . . 205
5.9 Kryptotrojaner und Ransomware . . . 206
5.9.1 WannaCry . . . 206
5.9.2 Petya . . . 207
5.9.3 Locky . . . 208
5.9.4 Schutz- und Gegenmaßnahmen . . . 208
5.10 Zusammenfassung und Prüfungstipps . . . 209
5.10.1 Zusammenfassung und Weiterführendes . . . 209
5.10.2 CEH-Prüfungstipps . . . 209
5.10.3 Fragen zur CEH-Prüfungsvorbereitung . . . 209

Teil II Informationsbeschaffung . . . 213

6 Informationsbeschaffung – Footprinting & Reconnaissance . . . 217
6.1 Ich will hacken, wozu die langweilige Informationssuche? . . . 218
6.1.1 Worum geht es bei der Informationsbeschaffung? . . . 219
6.1.2 Welche Informationen sind relevant? . . . 219
6.2 Suchmaschinen und Informationsportale nutzen . . . 221
6.2.1 Reguläre Suchmaschinen . . . 221
6.2.2 Netcraft: Nach öffentlichen und zugriffsbeschränkten Seiten suchen . . . 222
6.2.3 WayBack Machine – das Internet-Archiv . . . 223
6.2.4 Shodan . . . 224
6.2.5 Map-Anbieter: Mal von oben betrachtet . . . 225
6.2.6 Personen-Suchmaschinen . . . 226

6.2.7 Jobsuchmaschinen als Informationsquelle . . . 226
6.2.8 Arbeitgeber-Bewertungsportale . . . 227
6.3 Google-Hacking . . . 227
6.3.1 Was steckt dahinter? . . . 227
6.3.2 Wichtige Suchoperatoren . . . 228
6.3.3 Die Google Hacking Database (GHDB) . . . 228
6.4 Social-Media-Footprinting . . . 229
6.4.1 Wo suchen wir? . . . 230
6.4.2 Was suchen wir? . . . 230
6.4.3 Wie suchen wir? . . . 230
6.5 Technische Analysen . . . 231
6.5.1 Whois . . . 231
6.5.2 DNS – Das Domain Name System . . . 233
6.5.3 E-Mail-Footprinting . . . 237
6.5.4 Website-Footprinting . . . 239
6.5.5 Dokumente analysieren mit Metagoofil . . . 240
6.6 Recon-ng – das Web-Reconnaissance-Framework . . . 241
6.6.1 Die ersten Schritte mit Recon-ng . . . 241
6.6.2 Ein Modul installieren und laden . . . 243
6.6.3 Wie geht es weiter? . . . 245
6.7 Maltego – Zusammenhänge visualisieren . . . 245
6.7.1 Einführung in Maltego . . . 245
6.7.2 Maltego starten . . . 246
6.7.3 Mit Maltego arbeiten . . . 247
6.7.4 Der Transform Hub . . . 250
6.8 Gegenmaßnahmen gegen Footprinting . . . 251
6.9 Zusammenfassung und Prüfungstipps . . . 251
6.9.1 Zusammenfassung und Weiterführendes . . . 251
6.9.2 CEH-Prüfungstipps . . . 252
6.9.3 Fragen zur CEH-Prüfungsvorbereitung . . . 252

7 Scanning – das Netzwerk unter der Lupe . . . 255
7.1 Scanning – Überblick und Methoden . . . 255
7.1.1 Die Scanning-Phase . . . 256
7.1.2 Ziel des Scanning-Prozesses . . . 256
7.1.3 Scanning-Methoden . . . 256
7.2 TCP/IP-Essentials . . . 257
7.2.1 Das OSI-Netzwerk-Referenzmodell . . . 257
7.2.2 ARP, Switch & Co. – Layer-2-Technologien . . . 259
7.2.3 Das Internet Protocol (IPv4) . . . 259
7.2.4 Das Internet Control Message Protocol (ICMP) . . . 260
7.2.5 Das User Datagram Protocol (UDP) . . . 261
7.2.6 Das Transmission Control Protocol (TCP) . . . 262
7.3 Nmap – DER Portscanner . . . 263
7.3.1 Host Discovery . . . 264

7.3.2 Normale Portscans . . . 267
7.3.3 Zu scannende Ports festlegen . . . 269
7.3.4 Besondere Portscans . . . 270
7.3.5 Dienst- und Versionserkennung . . . 271
7.3.6 Betriebssystem-Erkennung . . . 272
7.3.7 Firewall/IDS-Vermeidung (Evasion) . . . 273
7.3.8 Ausgabe-Optionen . . . 274
7.3.9 Die Nmap Scripting Engine (NSE) . . . 275
7.3.10 Weitere wichtige Optionen . . . 276
7.3.11 Zenmap . . . 277
7.4 Scannen mit Metasploit . . . 277
7.4.1 Was ist Metasploit? . . . 277
7.4.2 Erste Schritte mit Metasploit (MSF) . . . 278
7.4.3 Nmap in Metasploit nutzen . . . 281
7.5 Weitere Tools und Verfahren . . . 283
7.5.1 Paketerstellung und Scanning mit hping3 . . . 283
7.5.2 Weitere Packet-Crafting-Tools . . . 285
7.5.3 Banner Grabbing mit Telnet und Netcat . . . 285
7.5.4 Scannen von IPv6-Netzwerken . . . 287
7.6 Gegenmaßnahmen gegen Portscanning und Banner Grabbing . . . 288
7.7 Zusammenfassung und Prüfungstipps . . . 289
7.7.1 Zusammenfassung und Weiterführendes . . . 289
7.7.2 CEH-Prüfungstipps . . . 290
7.7.3 Fragen zur CEH-Prüfungsvorbereitung . . . 290

8 Enumeration – welche Ressourcen sind verfügbar? . . . 293
8.1 Was wollen wir mit Enumeration erreichen? . . . 293
8.2 NetBIOS- und SMB-Enumeration . . . 294
8.2.1 Die Protokolle NetBIOS und SMB . . . 294
8.2.2 Der Enumeration-Prozess . . . 296
8.3 SNMP-Enumeration . . . 301
8.3.1 SNMP-Grundlagen . . . 302
8.3.2 SNMP-Agents identifizieren . . . 304
8.3.3 Enumeration-Tools nutzen . . . 305
8.4 LDAP-Enumeration . . . 310
8.4.1 LDAP- und AD-Grundlagen . . . 310
8.4.2 Der Enumeration-Prozess . . . 312
8.5 SMTP-Enumeration . . . 314
8.5.1 SMTP-Grundlagen . . . 314
8.5.2 Der Enumeration-Prozess . . . 315
8.6 NTP-Enumeration . . . 317
8.6.1 Funktionsweise von NTP . . . 317
8.6.2 Der Enumeration-Prozess . . . 318
8.7 DNS-Enumeration . . . 319
8.7.1 NFS-Enumeration . . . 324

8.7.2 Weitere Enumeration-Techniken . . . 326
8.8 Schutzmaßnahmen gegen Enumeration . . . 326
8.9 Zusammenfassung und Prüfungstipps . . . 328
8.9.1 Zusammenfassung und Weiterführendes . . . 328
8.9.2 CEH-Prüfungstipps . . . 329
8.9.3 Fragen zur CEH-Prüfungsvorbereitung . . . 329

9 Vulnerability-Scanning und Schwachstellenanalyse . . . 331
9.1 Was steckt hinter Vulnerability-Scanning? . . . 331
9.1.1 Vulnerabilities und Exploits . . . 332
9.1.2 Common Vulnerabilities and Exposures (CVE) . . . 332
9.1.3 CVE- und Exploit-Datenbanken . . . 333
9.1.4 Vulnerability-Scanner . . . 335
9.2 Vulnerability-Scanning mit Nmap . . . 336
9.2.1 Die Kategorie »vuln« . . . 336
9.2.2 Die passenden Skripts einsetzen . . . 337
9.3 Nessus . . . 339
9.3.1 Installation von Nessus . . . 339
9.3.2 Vulnerability-Scanning mit Nessus . . . 341
9.3.3 Nessus versus OpenVAS . . . 345
9.4 Rapid 7 Nexpose . . . 345
9.5 Vulnerability-Scanning in der Praxis . . . 346
9.5.1 Vulnerability-Assessments . . . 346
9.5.2 Einsatz von Vulnerability-Scannern im Ethical Hacking . . . 348
9.5.3 Credential Scan vs. Remote Scan . . . 349
9.5.4 Verifizieren der Schwachstelle . . . 349
9.5.5 Exploits zum Testen von Schwachstellen . . . 350
9.5.6 Spezialisierte Scanner . . . 350
9.6 Zusammenfassung und Prüfungstipps . . . 351
9.6.1 Zusammenfassung und Weiterführendes . . . 351
9.6.2 CEH-Prüfungstipps . . . 351
9.6.3 Fragen zur CEH-Prüfungsvorbereitung . . . 352

Teil III Systeme angreifen . . . 355

10 Password Hacking . . . 361
10.1 Zugriffsschutz mit Passwörtern und anderen Methoden . . . 362
10.2 Angriffsvektoren auf Passwörter . . . 363
10.3 Password Guessing und Password Recovery . . . 364
10.3.1 Grundlagen des Password Guessings . . . 365
10.3.2 Default-Passwörter . . . 366
10.3.3 Password Recovery unter Windows . . . 369
10.3.4 Password Recovery für Linux . . . 374
10.3.5 Password Recovery auf Cisco-Routern . . . 375

10.4 Die Windows-Authentifizierung . . . 377
10.4.1 Die SAM-Datenbank . . . 377
10.4.2 LM und NTLM . . . 378
10.4.3 Kerberos . . . 379
10.4.4 NTLM-Hashes auslesen mit FGdump . . . 383
10.5 Die Linux-Authentifizierung . . . 385
10.5.1 Speicherorte der Login-Daten . . . 385
10.5.2 Passwort-Hashes unter Linux . . . 386
10.5.3 Der Salt – Passwort-Hashes »salzen« . . . 386
10.5.4 Wie gelangen wir an die Passwort-Hashes? . . . 387
10.6 Passwort-Hashes angreifen . . . 389
10.6.1 Angriffsvektoren auf Passwort-Hashes . . . 389
10.6.2 Pass the Hash (PTH) . . . 392
10.6.3 Wortlisten erstellen . . . 394
10.6.4 L0phtcrack . . . 398
10.6.5 John the Ripper . . . 400
10.6.6 Cain & Abel . . . 402
10.7 Online-Angriffe auf Passwörter . . . 402
10.7.1 Grundlegende Problematik . . . 402
10.7.2 Medusa . . . 403
10.7.3 Hydra . . . 405
10.7.4 Ncrack . . . 406
10.8 Distributed Network Attack (DNA) . . . 408
10.8.1 Funktionsweise . . . 408
10.8.2 ElcomSoft Distributed Password Recovery . . . 409
10.9 Schutzmaßnahmen gegen Password Hacking . . . 409
10.10 Zusammenfassung und Prüfungstipps . . . 410
10.10.1 Zusammenfassung und Weiterführendes . . . 410
10.10.2 CEH-Prüfungstipps . . . 411
10.10.3 Fragen zur CEH-Prüfungsvorbereitung . . . 412

11 Shells und Post-Exploitation . . . 413
11.1 Remote-Zugriff mit Shell und Backdoor . . . 413
11.1.1 Einführung in Shells und Backdoors . . . 414
11.1.2 Netcat und Ncat – Einführung . . . 416
11.1.3 Grundlegende Funktionsweise von Netcat und Ncat . . . 417
11.1.4 Eine Bind-Shell bereitstellen . . . 421
11.1.5 Eine Reverse-Shell bereitstellen . . . 422
11.1.6 Wo stehen wir jetzt? . . . 424
11.2 Grundlagen Privilegien-Eskalation . . . 424
11.2.1 Vertikale Rechteerweiterung . . . 424
11.2.2 Horizontale Rechteerweiterung . . . 425
11.2.3 Rechte von Programmen . . . 425
11.3 Mit Privilegien-Eskalation zur Root-Shell . . . 426
11.3.1 Reverse-Shell durch DistCC-Exploit . . . 426

11.3.2 Bereitstellung eines Post-Exploits 428
11.3.3 Mit Metasploit-Multi-Handler zur Root-Shell. 431
11.4 Meterpreter – die Luxus-Shell für Hacker 432
11.4.1 Exploits und Payload. 433
11.4.2 Einführung in Meterpreter. 433
11.4.3 Meterpreter-Shell in der Praxis 435
11.4.4 Eine Meterpreter-Shell für Windows erstellen 437
11.4.5 Externe Module in Meterpreter laden 440
11.5 Empire – Das Powershell-Post-Exploitation-Framework 442
11.5.1 Das Szenario 442
11.5.2 Bereitstellung von Empire 443
11.5.3 Grundlagen: Listener, Stager, Agents 444
11.5.4 Empire in Aktion: Module nutzen. 447
11.6 Verteidigungsmaßnahmen gegen Privilegien-Eskalation 449
11.7 Zusammenfassung und Prüfungstipps. 450
11.7.1 Zusammenfassung und Weiterführendes 450
11.7.2 CEH-Prüfungstipps 451
11.7.3 Fragen zur CEH-Prüfungsvorbereitung 451

12 Mit Malware das System übernehmen 453
12.1 Malware-Grundlagen 454
12.1.1 Typische Malware-Kategorien 454
12.1.2 Wie gelangt Malware auf das Opfer-System? 456
12.1.3 Eine selbst erstellte Malware 458
12.2 Viren und Würmer 459
12.2.1 Was ist ein Computervirus? 459
12.2.2 Was ist ein Computerwurm? 461
12.2.3 Einen Makro-Virus erstellen 462
12.3 Trojanische Pferde in der Praxis 466
12.3.1 Trojaner-Typen 466
12.3.2 Einen Trojaner selbst bauen 468
12.3.3 Viren- und Trojaner-Baukästen 471
12.4 Malware tarnen und vor Entdeckung schützen. 473
12.4.1 Grundlagen der Tarnung von Payload 473
12.4.2 Encoder einsetzen. 476
12.4.3 Payload mit Hyperion verschlüsseln 479
12.4.4 Das Veil-Framework 480
12.4.5 Shellter AV Evasion 480
12.4.6 Fileless Malware 481
12.5 Rootkits 483
12.5.1 Grundlagen der Rootkits 483
12.5.2 Kernel-Rootkits 484
12.5.3 Userland-Rootkits 484
12.5.4 Rootkit-Beispiele 485
12.5.5 Rootkits entdecken und entfernen 485

12.6 Covert Channel . . . 486
12.6.1 ICMP-Tunneling . . . 487
12.6.2 NTFS Alternate Data Stream (ADS) . . . 490
12.7 Keylogger und Spyware . . . 492
12.7.1 Grundlagen . . . 492
12.7.2 Keylogger und Spyware in der Praxis . . . 492
12.8 Advanced Persistent Threat (APT) . . . 497
12.8.1 Wie funktioniert ein APT? . . . 497
12.8.2 Ablauf eines APT-Angriffs . . . 498
12.8.3 Zielgruppen von APT-Angriffen . . . 498
12.9 Schutzmaßnahmen gegen Malware . . . 499
12.10 Zusammenfassung und Prüfungstipps . . . 499
12.10.1 Zusammenfassung und Weiterführendes . . . 499
12.10.2 CEH-Prüfungstipps . . . 500
12.10.3 Fragen zur CEH-Prüfungsvorbereitung . . . 500

13 Malware-Erkennung und -Analyse . . . 503
13.1 Grundlagen der Malware-Analyse . . . 503
13.1.1 Statische Malware-Analyse . . . 504
13.1.2 Dynamische Malware-Analyse . . . 507
13.2 Verdächtiges Verhalten analysieren . . . 507
13.2.1 Virencheck durchführen . . . 508
13.2.2 Prozesse überprüfen . . . 512
13.2.3 Netzwerkaktivitäten prüfen . . . 515
13.2.4 Die Windows-Registrierung checken . . . 520
13.2.5 Autostart-Einträge unter Kontrolle . . . 524
13.2.6 Windows-Dienste checken . . . 526
13.2.7 Treiber überprüfen . . . 528
13.2.8 Integrität der Systemdateien prüfen . . . 530
13.2.9 Datei-Integrität durch Prüfsummen-Check . . . 531
13.2.10 System-Integrität mit Tripwire sichern . . . 533
13.3 Sheep-Dip-Systeme . . . 534
13.3.1 Einführung . . . 534
13.3.2 Aufbau eines Sheep-Dip-Systems . . . 535
13.4 Schutz durch Sandbox . . . 536
13.4.1 Sandboxie . . . 536
13.4.2 Cuckoo . . . 538
13.5 Aufbau einer modernen Anti-Malware-Infrastruktur . . . 539
13.5.1 Relevante Komponenten . . . 540
13.5.2 Komponenten der Anti-Malware-Infrastruktur . . . 540
13.6 Allgemeine Schutzmaßnahmen vor Malware-Infektion . . . 542
13.7 Zusammenfassung und Prüfungstipps . . . 543
13.7.1 Zusammenfassung und Weiterführendes . . . 543
13.7.2 CEH-Prüfungsgstipps . . . 544
13.7.3 Fragen zur CEH-Prüfungsvorbereitung . . . 545

14 Steganografie ... 547
14.1 Grundlagen der Steganografie ... 547
14.1.1 Wozu Steganografie? ... 547
14.1.2 Ein paar einfache Beispiele ... 548
14.1.3 Klassifikation der Steganografie ... 549
14.2 Computergestützte Steganografie ... 553
14.2.1 Daten in Bildern verstecken ... 553
14.2.2 Daten in Dokumenten verstecken ... 558
14.2.3 Weitere Cover-Datenformate ... 559
14.3 Steganalyse und Schutz vor Steganografie ... 560
14.3.1 Methoden der Steganalyse ... 560
14.3.2 Steganalyse-Tools ... 561
14.3.3 Schutz vor Steganografie ... 561
14.4 Zusammenfassung und Prüfungstipps ... 562
14.4.1 Zusammenfassung und Weiterführendes ... 562
14.4.2 CEH-Prüfungstipps ... 563
14.4.3 Fragen zur CEH-Prüfungsvorbereitung ... 563

15 Spuren verwischen ... 565
15.1 Auditing und Logging ... 565
15.1.1 Die Windows-Protokollierung ... 566
15.1.2 Die klassische Linux-Protokollierung ... 568
15.2 Spuren verwischen auf einem Windows-System ... 571
15.2.1 Das Windows-Auditing deaktivieren ... 571
15.2.2 Windows-Ereignisprotokolle löschen ... 573
15.2.3 Most Recently Used (MRU) löschen ... 575
15.2.4 Zeitstempel manipulieren ... 578
15.2.5 Clearing-Tools ... 582
15.3 Spuren verwischen auf einem Linux-System ... 583
15.3.1 Logfiles manipulieren und löschen ... 583
15.3.2 Systemd-Logging in Journald ... 586
15.3.3 Zeitstempel manipulieren ... 586
15.3.4 Die Befehlszeilen-Historie löschen ... 588
15.4 Schutz vor dem Spuren-Verwischen ... 589
15.5 Zusammenfassung und Prüfungstipps ... 590
15.5.1 Zusammenfassung und Weiterführendes ... 590
15.5.2 CEH-Prüfungstipps ... 591
15.5.3 Fragen zur CEH-Prüfungsvorbereitung ... 591

Teil IV Netzwerk- und sonstige Angriffe ... 595

16 Network Sniffing mit Wireshark & Co. ... 599
16.1 Grundlagen von Netzwerk-Sniffern ... 599
16.1.1 Technik der Netzwerk-Sniffer ... 599

16.1.2 Wireshark und die Pcap-Bibliotheken . . . 601
16.2 Wireshark installieren und starten . . . 601
16.2.1 Installation unter Linux . . . 601
16.2.2 Installation unter Windows . . . 602
16.2.3 Der erste Start . . . 603
16.3 Die ersten Schritte mit Wireshark . . . 604
16.3.1 Grundeinstellungen . . . 604
16.3.2 Ein erster Mitschnitt . . . 606
16.4 Mitschnitt-Filter einsetzen . . . 607
16.4.1 Analyse eines TCP-Handshakes . . . 608
16.4.2 Der Ping in Wireshark . . . 609
16.4.3 Weitere Mitschnittfilter . . . 610
16.5 Anzeigefilter einsetzen . . . 611
16.5.1 Eine HTTP-Sitzung im Detail . . . 612
16.5.2 Weitere Anzeigefilter . . . 614
16.6 Passwörter und andere Daten ausspähen . . . 615
16.6.1 FTP-Zugangsdaten ermitteln . . . 616
16.6.2 Telnet-Zugangsdaten identifizieren . . . 617
16.6.3 SSH – sicherer Schutz gegen Mitlesen . . . 619
16.6.4 Andere Daten ausspähen . . . 621
16.7 Auswertungsfunktionen von Wireshark nutzen . . . 622
16.8 Tcpdump und TShark einsetzen . . . 624
16.8.1 Tcpdump – der Standard-Sniffer für die Konsole . . . 624
16.8.2 TShark – Wireshark auf der Konsole . . . 627
16.9 Zusammenfassung und Prüfungstipps . . . 629
16.9.1 Zusammenfassung und Weiterführendes . . . 629
16.9.2 CEH-Prüfungstipps . . . 629
16.9.3 Fragen zur CEH-Prüfungsvorbereitung . . . 630

17 Lauschangriffe & Man-in-the-Middle . . . 633
17.1 Eavesdropping und Sniffing für Hacker . . . 633
17.1.1 Eavesdropping und Wiretapping . . . 634
17.1.2 Sniffing als Angriffsvektor . . . 634
17.2 Man-in-the-Middle (MITM) . . . 635
17.2.1 Was bedeutet Man-in-the-Middle? . . . 636
17.2.2 Was erreichen wir durch einen MITM-Angriff? . . . 637
17.3 Active Sniffing . . . 637
17.3.1 Mirror-Ports: Ein Kabel mit drei Enden . . . 638
17.3.2 Aus Switch mach Hub – MAC-Flooding . . . 638
17.3.3 Auf dem Silbertablett: WLAN-Sniffing . . . 640
17.3.4 Weitere physische Abhörmöglichkeiten . . . 641
17.4 Die Kommunikation für MITM umleiten . . . 641
17.4.1 Physische Umleitung . . . 641
17.4.2 Umleitung über aktive Netzwerk-Komponenten . . . 642
17.4.3 Umleiten mit ARP-Spoofing . . . 643

17.4.4 ICMP-Typ 5 Redirect 643
17.4.5 DNS-Spoofing oder DNS-Cache-Poisoning 644
17.4.6 Manipulation der hosts-Datei 646
17.4.7 Umleiten via DHCP-Spoofing 647
17.5 Die Dsniff-Toolsammlung 648
17.5.1 Programme der Dsniff-Suite 648
17.5.2 Abhören des Netzwerk-Traffics 649
17.5.3 MITM mit arpspoof 650
17.5.4 Die ARP-Tabelle des Switches mit macof überfluten 653
17.5.5 DNS-Spoofing mit dnspoof 653
17.5.6 Dsniff 656
17.6 Man-in-the-Middle-Angriffe mit Ettercap 657
17.6.1 Einführung in Ettercap 657
17.6.2 DNS-Spoofing mit Ettercap 659
17.7 Schutz vor Lauschangriffen & MITM 667
17.8 Zusammenfassung und Prüfungstipps 669
17.8.1 Zusammenfassung und Weiterführendes 669
17.8.2 CEH-Prüfungstipps 670
17.8.3 Fragen zur CEH-Prüfungsvorbereitung 670

18 Session Hijacking 673
18.1 Grundlagen des Session Hijackings 673
18.1.1 Wie funktioniert Session Hijacking grundsätzlich? 674
18.1.2 Session-Hijacking-Varianten 674
18.2 Network Level Session Hijacking 675
18.2.1 Die TCP-Session im Detail 676
18.2.2 Entführen von TCP-Sessions 678
18.2.3 Eine Telnet-Session entführen 680
18.2.4 Weitere Hijacking-Varianten auf Netzwerk-Ebene 685
18.3 Application Level Session Hijacking 686
18.3.1 Die Session-IDs 686
18.3.2 Die Session-ID ermitteln 687
18.3.3 Sniffing/Man-in-the-Middle 688
18.3.4 Die Session-ID erraten – das Prinzip 688
18.3.5 WebGoat bereitstellen 689
18.3.6 Die Burp Suite – Grundlagen und Installation 692
18.3.7 Burp Suite als Intercepting Proxy 693
18.3.8 Der Burp Sequencer – Session-IDs analysieren 697
18.3.9 Entführen der Session mithilfe der Session-ID 700
18.3.10 Man-in-the-Browser-Angriff 707
18.3.11 Weitere Angriffsformen 709
18.4 Gegenmaßnahmen gegen Session Hijacking 711
18.4.1 Session Hijacking entdecken 711
18.4.2 Schutzmaßnahmen 712

18.5 Zusammenfassung und Prüfungstipps ... 714
18.5.1 Zusammenfassung und Weiterführendes ... 714
18.5.2 CEH-Prüfungstipps ... 715
18.5.3 Fragen zur CEH-Prüfungsvorbereitung ... 715

19 Firewalls, IDS/IPS und Honeypots einsetzen und umgehen ... 717
19.1 Firewall-Technologien ... 717
19.1.1 Netzwerk- und Personal-Firewalls ... 718
19.1.2 Filtertechniken und Kategorisierung der Netzwerk-Firewalls ... 719
19.2 Firewall-Szenarien ... 723
19.2.1 DMZ-Szenarien ... 723
19.2.2 Failover-Szenarien ... 725
19.3 Firewalls umgehen ... 726
19.3.1 Identifikation von Firewalls ... 726
19.3.2 IP-Adress-Spoofing ... 727
19.3.3 Was wirklich funktioniert ... 728
19.4 Intrusion-Detection- und -Prevention-Systeme ... 729
19.4.1 Einführung in Snort ... 732
19.5 Intrusion-Detection-Systeme umgehen ... 736
19.5.1 Injection/Insertion ... 736
19.5.2 Evasion ... 737
19.5.3 Denial-of-Service-Angriff (DoS) ... 738
19.5.4 Obfuscation ... 738
19.5.5 Generieren von False Positives ... 738
19.5.6 Fragmentation ... 739
19.5.7 TCP Session Splicing ... 740
19.5.8 Weitere Evasion-Techniken ... 740
19.6 Honeypots ... 741
19.6.1 Grundlagen und Begriffsklärung ... 741
19.6.2 Kategorisierung der Honeypots ... 742
19.6.3 KFSensor – ein Honeypot in der Praxis ... 745
19.6.4 Honeypots identifizieren und umgehen ... 749
19.6.5 Rechtliche Aspekte beim Einsatz von Honeypots ... 750
19.7 Zusammenfassung und Prüfungstipps ... 751
19.7.1 Zusammenfassung und Weiterführendes ... 751
19.7.2 CEH-Prüfungstipps ... 752
19.7.3 Fragen zur CEH-Prüfungsvorbereitung ... 752

20 Social Engineering ... 755
20.1 Einführung in das Social Engineering ... 755
20.1.1 Welche Gefahren birgt Social Engineering? ... 756
20.1.2 Verlustangst, Neugier, Eitelkeit – die Schwachstellen des Systems Mensch ... 756
20.1.3 Varianten des Social Engineerings ... 759
20.1.4 Allgemeine Vorgehensweise beim Social Engineering ... 761

20.2 Human Based Social Engineering . . . 761
20.2.1 Vortäuschen einer anderen Identität . . . 762
20.2.2 Shoulder Surfing & Co. . . . 764
20.2.3 Piggybacking und Tailgaiting . . . 765
20.3 Computer Based Social Engineering . . . 766
20.3.1 Phishing . . . 766
20.3.2 Pharming . . . 766
20.3.3 Spear Phishing . . . 767
20.3.4 Drive-by-Downloads . . . 768
20.3.5 Gefälschte Viren-Warnungen . . . 769
20.4 Das Social-Engineer Toolkit (SET) . . . 770
20.4.1 Einführung in SET . . . 770
20.4.2 Praxisdemonstration: Credential Harvester . . . 772
20.4.3 Weitere Angriffe mit SET . . . 775
20.5 So schützen Sie sich gegen Social-Engineering-Angriffe . . . 776
20.6 Zusammenfassung und Prüfungstipps . . . 778
20.6.1 Zusammenfassung und Weiterführendes . . . 778
20.6.2 CEH-Prüfungstipps . . . 779
20.6.3 Fragen zur CEH-Prüfungsvorbereitung . . . 779

21 Hacking-Hardware . . . 781
21.1 Allgemeines und rechtliche Hinweise zu Spionage-Hardware . . . 782
21.2 Angriffsvektor USB-Schnittstelle . . . 782
21.2.1 Hardware Keylogger . . . 783
21.2.2 USB Rubber Ducky . . . 784
21.2.3 Bash Bunny . . . 786
21.2.4 Digispark . . . 788
21.2.5 USBNinja . . . 789
21.2.6 Mouse Jiggler . . . 790
21.3 Weitere Hacking-Gadgets . . . 790
21.3.1 VideoGhost . . . 790
21.3.2 Packet Squirrel . . . 791
21.3.3 LAN Turtle . . . 792
21.3.4 Throwing Star LAN Tap . . . 792
21.3.5 Software Defined Radio . . . 793
21.3.6 Crazyradio PA . . . 793
21.3.7 WiFi Pinapple . . . 794
21.3.8 Proxmark 3 . . . 795
21.3.9 ChameleonMini . . . 795
21.4 Raspberry Pi als Hacking-Kit . . . 795
21.5 Gegenmaßnahmen . . . 797
21.6 Zusammenfassung und Prüfungstipps . . . 799
21.6.1 Zusammenfassung und Weiterführendes . . . 799
21.6.2 CEH-Prüfungstipps . . . 800
21.6.3 Fragen zur CEH-Prüfungsvorbereitung . . . 800

22 DoS- und DDoS-Angriffe ... 803
22.1 DoS- und DDoS-Grundlagen ... 803
22.1.1 Was ist ein Denial-of-Service-Angriff? ... 804
22.1.2 Warum werden DoS- und DDoS-Angriffe durchgeführt? ... 804
22.1.3 Kategorien der DoS/DDoS-Angriffe ... 805
22.2 DoS- und DDoS-Angriffstechniken ... 805
22.2.1 UDP-Flood-Angriff ... 806
22.2.2 ICMP-Flood-Angriff ... 806
22.2.3 Smurf-Angriff ... 807
22.2.4 Syn-Flood-Angriff ... 808
22.2.5 Fragmentation-Angriff ... 811
22.2.6 Slowloris-Angriff ... 812
22.2.7 Permanenter Denial-of-Service (PDoS) ... 813
22.2.8 Distributed-Reflected-Denial-of-Service-Angriff (DRDoS) ... 814
22.3 Botnetze – Funktionsweise und Betrieb ... 815
22.3.1 Bots und deren Einsatzmöglichkeiten ... 816
22.3.2 Aufbau eines Botnetzes ... 816
22.3.3 Wie gelangen Bots auf die Opfer-Systeme? ... 818
22.3.4 Mobile Systeme und IoT ... 819
22.3.5 Botnetze in der Praxis ... 819
22.3.6 Verteidigung gegen Botnetze und DDoS-Angriffe ... 820
22.4 DoS-Angriffe in der Praxis ... 822
22.4.1 SYN- und ICMP-Flood-Angriff mit hping3 ... 823
22.4.2 DoS-Angriff mit Metasploit ... 825
22.4.3 DoS-Angriff mit SlowHTTPTest ... 827
22.4.4 Low Orbit Ion Cannon (LOIC) ... 828
22.5 Verteidigung gegen DoS- und DDoS-Angriffe ... 830
22.5.1 Allgemeiner Grundschutz ... 830
22.5.2 Schutz vor volumetrischen DDoS-Angriffen ... 831
22.6 Zusammenfassung und Prüfungstipps ... 832
22.6.1 Zusammenfassung und Weiterführendes ... 832
22.6.2 CEH-Prüfungstipps ... 833
22.6.3 Fragen zur CEH-Prüfungsvorbereitung ... 833

Teil V Web-Hacking ... 835

23 Web-Hacking – Grundlagen ... 839
23.1 Was ist Web-Hacking? ... 839
23.2 Architektur von Webanwendungen ... 840
23.2.1 Die Schichten-Architektur ... 840
23.2.2 Die URL-Codierung ... 841
23.2.3 Das Hypertext Transfer Protocol (HTTP) ... 842
23.2.4 Cookies ... 845

23.2.5 HTTP vs. HTTPS ... 845
23.2.6 Webservices und -technologien ... 846
23.3 Die gängigsten Webserver: Apache, IIS, nginx ... 851
23.3.1 Apache HTTP Server ... 851
23.3.2 Internet Information Services (IIS) ... 853
23.3.3 nginx ... 855
23.4 Typische Schwachstellen von Webservern und -anwendungen ... 856
23.4.1 Schwachstellen in Webserver-Plattformen ... 856
23.4.2 Schwachstellen in der Webanwendung ... 857
23.5 Reconnaissance für Web-Hacking-Angriffe ... 858
23.5.1 Footprinting und Scanning ... 858
23.5.2 Web-Firewalls und Proxys entlarven ... 860
23.5.3 Hidden Content Discovery ... 860
23.5.4 Website-Mirroring ... 863
23.5.5 Security-Scanner ... 863
23.6 Praxis-Szenario: Einen Apache-Webserver mit Shellshock hacken ... 866
23.6.1 Die Laborumgebung präparieren ... 866
23.6.2 Den Angriff durchführen ... 868
23.7 Praxis-Szenario 2: Angriff auf WordPress ... 869
23.7.1 WordPress-VM bereitstellen ... 870
23.7.2 WordPress scannen und Enumeration ... 874
23.7.3 User-Hacking ... 876
23.8 Zusammenfassung und Prüfungstipps ... 876
23.8.1 Zusammenfassung und Weiterführendes ... 876
23.8.2 CEH-Prüfungstipps ... 877
23.8.3 Fragen zur CEH-Prüfungsvorbereitung ... 877

24 Web-Hacking – OWASP Top 10 ... 879
24.1 Einführung in die OWASP-Projekte ... 879
24.2 WebGoat & Co – virtuelle Sandsäcke für das Web-Hacking-Training ... 883
24.2.1 WebGoat ... 883
24.2.2 Mutillidae II ... 884
24.2.3 bWAPP ... 885
24.2.4 DVWA ... 886
24.2.5 OWASP Broken Web Application ... 887
24.2.6 Web Security Dojo ... 887
24.2.7 Vulnhub und Pentesterlab ... 888
24.3 Die OWASP Top 10 in der Übersicht ... 888
24.4 A1 – Injection ... 889
24.4.1 Kategorien von Injection-Angriffen ... 889
24.4.2 Beispiel für einen Injection-Angriff ... 890
24.5 A2 – Fehler in der Authentifizierung ... 892
24.5.1 Grundlagen ... 892
24.5.2 Identitätsdiebstahl durch Token-Manipulation ... 893
24.5.3 Schutzmaßnahmen ... 896

24.6 A3 – Verlust der Vertraulichkeit sensibler Daten ... 896
24.6.1 Welche Daten sind betroffen? ... 896
24.6.2 Angriffsszenarien ... 897
24.6.3 Schutzmaßnahmen ... 898
24.7 A4 – XML External Entities (XXE) ... 899
24.7.1 XML-Entities ... 899
24.7.2 Ein Beispiel für einen XXE-Angriff ... 900
24.7.3 Schutzmaßnahmen ... 901
24.8 A5 – Fehler in der Zugriffskontrolle ... 902
24.8.1 Unsichere direkte Objektreferenzen ... 902
24.8.2 Fehlerhafte Autorisierung auf Anwendungsebene ... 904
24.8.3 Schutzmaßnahmen ... 907
24.9 A6 – Sicherheitsrelevante Fehlkonfiguration ... 907
24.9.1 Typische Fehlkonfigurationen ... 907
24.9.2 Directory Browsing ... 908
24.9.3 Schutzmaßnahmen ... 910
24.10 A7 – Cross-Site-Scripting (XSS) ... 910
24.10.1 Wie funktioniert XSS? ... 911
24.10.2 Ein einfaches XSS-Beispiel ... 911
24.10.3 XSS-Varianten ... 913
24.10.4 Ein Beispiel für Stored XSS ... 915
24.10.5 Exkurs: Cross-Site-Request-Forgery (CSRF) ... 917
24.10.6 Schutzmaßnahmen ... 918
24.11 A8 – Unsichere Deserialisierung ... 919
24.11.1 Was bedeutet Serialisierung von Daten? ... 919
24.11.2 Wie wird die Deserialisierung zum Problem? ... 920
24.11.3 Schutzmaßnahmen ... 920
24.12 A9 – Nutzung von Komponenten mit bekannten Schwachstellen ... 921
24.12.1 Wo liegt die Gefahr und wer ist gefährdet? ... 921
24.12.2 Verwundbare JavaScript-Bibliotheken aufdecken mit Retire.js ... 921
24.12.3 Schutzmaßnahmen ... 922
24.13 A10 – Unzureichendes Logging & Monitoring ... 923
24.13.1 Herausforderungen beim Logging & Monitoring ... 923
24.13.2 Sind unserer Systeme gefährdet? ... 924
24.14 Zusammenfassung und Prüfungstipps ... 925
24.14.1 Zusammenfassung und Weiterführendes ... 925
24.14.2 CEH-Prüfungstipps ... 925
24.14.3 Fragen zur CEH-Prüfungsvorbereitung ... 926

25 SQL-Injection ... 929
25.1 Mit SQL-Injection das Login austricksen ... 930
25.1.1 Der grundlegende Ansatz ... 930
25.1.2 Anmeldung als gewünschter Benutzer ... 933
25.1.3 Clientseitige Sicherheit ... 934

25.2 Daten auslesen mit SQL-Injection ... 936
25.2.1 Manipulation eines GET-Requests ... 937
25.2.2 Informationen über die Datenbank auslesen ... 938
25.2.3 Die Datenbank-Tabellen identifizieren ... 940
25.2.4 Spalten und Passwörter auslesen ... 942
25.3 Fortgeschrittene SQL-Injection-Techniken ... 943
25.3.1 Einführung in Blind SQL-Injection ... 944
25.3.2 Codieren des Injection-Strings ... 946
25.3.3 Blind SQLi: Eins oder null? ... 949
25.3.4 Time based SQL-Injection ... 950
25.4 SQLMap – automatische Schwachstellensuche ... 952
25.4.1 SQLi-CheatSheets ... 952
25.4.2 Einführung in SQLMap ... 953
25.4.3 Weitere Analysen mit SQLMap ... 958
25.5 Schutzmaßnahmen vor SQLi-Angriffen ... 960
25.6 Zusammenfassung und Prüfungstipps ... 961
25.6.1 Zusammenfassung und Weiterführendes ... 961
25.6.2 CEH-Prüfungstipps ... 961
25.6.3 Fragen zur CEH-Prüfungsvorbereitung ... 962

26 Web-Hacking – sonstige Injection-Angriffe ... 965
26.1 Command-Injection ... 965
26.1.1 Einführung in Command-Injection-Angriffe ... 966
26.1.2 Command-Injection in der Praxis ... 966
26.1.3 Schutzmaßnahmen vor Command-Injection-Angriffen ... 968
26.2 LDAP-Injection ... 969
26.2.1 Die LDAP-Infrastruktur bereitstellen ... 969
26.2.2 Ein erster Injection-Angriff ... 973
26.2.3 LDAP-Injection mit der BurpSuite vereinfachen ... 975
26.2.4 LDAP-Injection-Discovery ... 976
26.2.5 Discovery-Automatisierung mit Hilfe der BurpSuite ... 977
26.2.6 Flexibilität und Geduld sind gefragt ... 981
26.2.7 Schutz vor LDAP-Injection-Angriffen ... 982
26.3 File-Injection ... 982
26.3.1 Directory-Traversal-Angriffe ... 983
26.3.2 File-Upload-Angriffe ... 985
26.3.3 Local File Inclusion versus Remote File Inclusion ... 987
26.4 Zusammenfassung und Prüfungstipps ... 991
26.4.1 Zusammenfassung und Weiterführendes ... 991
26.4.2 CEH-Prüfungstipps ... 991
26.4.3 Fragen zur CEH-Prüfungsvorbereitung ... 991

27 Buffer-Overflow-Angriffe ... 993
27.1 Wie funktioniert ein Buffer-Overflow-Angriff? ... 993
27.1.1 Das Grundprinzip ... 994

27.1.2 Welche Anwendungen sind verwundbar? ... 994
27.1.3 Funktionsweise des Stacks ... 995
27.1.4 Register ... 995
27.2 Ein Buffer-Overflow-Angriff in der Praxis ... 997
27.2.1 SLmail-Exploit ... 997
27.2.2 Die Laborumgebung ... 997
27.2.3 Der Immunity Debugger ... 999
27.2.4 Fuzzing ... 1002
27.2.5 Einen eindeutigen String erstellen ... 1006
27.2.6 Den EIP lokalisieren ... 1008
27.2.7 Den Shellcode platzieren ... 1008
27.2.8 Bad Characters identifizieren ... 1010
27.2.9 Grundüberlegung: Wohin soll der EIP zeigen? ... 1012
27.2.10 Mona und die Module ... 1012
27.2.11 Die Anweisung JMP ESP auffinden ... 1013
27.2.12 Den Programmablauf über den EIP steuern ... 1015
27.2.13 Den Shellcode erstellen und ausführen ... 1017
27.3 Heap-Overflow-Angriffe ... 1021
27.3.1 Der Heap ... 1021
27.3.2 Heap Overflow versus Stack Overflow ... 1022
27.3.3 Use-after-free ... 1022
27.3.4 Heap Spraying ... 1022
27.4 Schutzmaßnahmen gegen Buffer-Overflow-Angriffe ... 1023
27.4.1 Address Space Layout Randomization (ASLR) ... 1023
27.4.2 Data Execution Prevention (DEP) ... 1024
27.4.3 SEHOP und SafeSEH ... 1024
27.4.4 Stack Canary ... 1024
27.4.5 Wie sicher sind die Schutzmaßnahmen? ... 1025
27.5 Zusammenfassung und Prüfungstipps ... 1026
27.5.1 Zusammenfassung und Weiterführendes ... 1026
27.5.2 CEH-Prüfungstipps ... 1027
27.5.3 Fragen zur CEH-Prüfungsvorbereitung ... 1027

Teil VI Angriffe auf WLAN und Next-Gen-Technologien ... 1029

28 WLAN-Hacking ... 1033
28.1 WLAN-Grundlagen ... 1033
28.1.1 Frequenzen und Kanäle ... 1034
28.1.2 Der IEEE-802.11-Standard ... 1035
28.1.3 Infrastruktur ... 1036
28.1.4 Verbindungsaufbau ... 1039
28.1.5 Verschlüsselungsmethoden ... 1042
28.2 Setup für das WLAN-Hacking ... 1045
28.2.1 Die WLAN-Hacking-Plattform ... 1045

28.2.2 Der richtige WLAN-Adapter . . . 1046
28.2.3 Den Monitor Mode aktivieren . . . 1046
28.3 WLAN-Scanning und -Sniffing . . . 1048
28.3.1 Scanning . . . 1049
28.3.2 WLAN-Sniffing . . . 1049
28.3.3 Hidden SSIDs aufspüren . . . 1051
28.4 Angriffe auf WLAN . . . 1053
28.4.1 Denial of Service durch Störsender . . . 1053
28.4.2 Deauthentication-Angriff . . . 1053
28.4.3 Angriff auf WEP . . . 1055
28.4.4 Angriff auf WPA/WPA2 . . . 1058
28.4.5 Angriff auf WPA3 . . . 1060
28.4.6 Angriff auf WPS . . . 1061
28.4.7 MAC-Filter umgehen . . . 1064
28.4.8 WLAN-Passwörter auslesen . . . 1066
28.4.9 Standard-Passwörter . . . 1068
28.4.10 Captive Portals umgehen . . . 1069
28.5 Rogue Access Points . . . 1071
28.5.1 Fake-Access-Point bereitstellen . . . 1072
28.5.2 WLAN-Phishing . . . 1074
28.6 Schutzmaßnahmen . . . 1076
28.6.1 Allgemeine Maßnahmen . . . 1077
28.6.2 Fortgeschrittene Sicherheitsmechanismen . . . 1078
28.7 Zusammenfassung und Prüfungstipps . . . 1079
28.7.1 Zusammenfassung und Weiterführendes . . . 1079
28.7.2 CEH-Prüfungstipps . . . 1080
28.7.3 Fragen zur CEH-Prüfungsvorbereitung . . . 1080

29 Mobile Hacking . . . 1083
29.1 Grundlagen . . . 1083
29.1.1 Mobile Betriebssysteme . . . 1083
29.1.2 Apps und App-Stores . . . 1085
29.2 Angriffe auf mobile Geräte . . . 1087
29.2.1 Schutzziele . . . 1087
29.2.2 Angriffsvektoren . . . 1088
29.2.3 OWASP Mobile Top 10 . . . 1090
29.3 Mobile Hacking in der Praxis . . . 1091
29.3.1 Android über den PC . . . 1091
29.3.2 Android-Rooting . . . 1095
29.3.3 Jailbreaking iOS . . . 1101
29.3.4 SIM-Unlock . . . 1103
29.3.5 Hacking-Tools für Android . . . 1103
29.3.6 Android-Tojaner erstellen . . . 1106
29.3.7 Angriffe auf iOS . . . 1112
29.3.8 Spyware für mobile Geräte . . . 1112

29.4 Bring Your Own Device (BYOD) ... 1113
29.4.1 BYOD-Vorteile ... 1113
29.4.2 BYOD-Risiken ... 1114
29.4.3 BYOD-Sicherheit ... 1115
29.5 Mobile Device Management (MDM) ... 1115
29.6 Schutzmaßnahmen ... 1117
29.7 Zusammenfassung und Prüfungstipps ... 1119
29.7.1 Zusammenfassung und Weiterführendes ... 1119
29.7.2 CEH-Prüfungstipps ... 1120
29.7.3 Fragen zur CEH-Prüfungsvorbereitung ... 1120

30 IoT- und OT-Hacking und -Security ... 1123
30.1 Das Internet of Things ... 1123
30.1.1 Was ist das Internet of Things? ... 1124
30.1.2 Was umfasst das Internet of Things? ... 1124
30.1.3 Die grundlegende Sicherheitsproblematik von IoT-Geräten ... 1125
30.2 IoT-Technik – Konzepte und Protokolle ... 1125
30.2.1 IoT-Betriebssysteme ... 1126
30.2.2 IoT-Kommunikationsmodelle ... 1126
30.2.3 IoT-Übertragungstechnologien ... 1128
30.2.4 IoT-Kommunikationsprotokolle ... 1130
30.3 Schwachstellen von IoT-Systemen ... 1131
30.3.1 OWASP Top 10 IoT 2018 ... 1131
30.3.2 Angriffsvektoren auf IoT-Systeme ... 1133
30.4 IoT-Angriffszenarien ... 1136
30.4.1 Rolling-Code-Angriff ... 1136
30.4.2 Mirai – Botnet und DDoS-Angriffe ... 1138
30.4.3 Lokale Angriffe über die UART-Schnittstelle ... 1139
30.4.4 Command-Injection via Web-Frontend ... 1140
30.4.5 Der BlueBorne-Angriff ... 1141
30.4.6 Angriffe auf ZigBee-Geräte mit Killerbee ... 1142
30.4.7 Angriffe auf Firmware ... 1143
30.5 Weitere Angriffsformen auf IoT-Ökosysteme ... 1144
30.5.1 Exploit Kits ... 1144
30.5.2 IoT-Suchmaschinen ... 1144
30.6 OT-Hacking ... 1146
30.6.1 OT-Grundlagen und -Konzepte ... 1146
30.6.2 Konvergenz von IT und OT ... 1147
30.6.3 Das Purdue-Modell ... 1148
30.6.4 OT-Sicherheitsherausforderungen ... 1149
30.6.5 OT-Schwachstellen und Bedrohungen ... 1150
30.6.6 OT-Malware ... 1151
30.6.7 OT-Hackingtools und -Enumeration ... 1152
30.6.8 Schutzmaßnahmen vor OT-Angriffen ... 1153
30.7 Schutzmaßnahmen vor IoT-Angriffen ... 1154

30.8 Zusammenfassung und Prüfungstipps 1156
30.8.1 Zusammenfassung und Weiterführendes 1156
30.8.2 CEH-Prüfungstipps 1156
30.8.3 Fragen zur CEH-Prüfungsvorbereitung 1156

31 Angriffe auf die Cloud 1159
31.1 Grundlagen des Cloud Computings 1159
31.1.1 Was ist eigentlich »die Cloud?« 1160
31.1.2 Cloud-Service-Modelle 1161
31.1.3 Deployment-Modelle für die Cloud 1162
31.1.4 Große Cloud-Anbieter 1164
31.2 Wichtige Cloud-Technologien 1165
31.2.1 Virtualisierung 1165
31.2.2 Container-Technologien 1166
31.2.3 Docker 1168
31.2.4 Kubernetes 1171
31.2.5 Schwachstellen von Container-Technologien 1172
31.2.6 Serverless Computing 1173
31.2.7 Schwachstellen von Serverless Computing 1174
31.2.8 Weitere Cloud-Dienstleistungen 1174
31.3 Bedrohungen der Sicherheit und Integrität in der Cloud 1174
31.3.1 Kontrollverlust 1175
31.3.2 Unsichere Cloud-Infrastruktur 1175
31.3.3 Missbrauchs-Risiken beim Cloud-Anbieter 1177
31.3.4 Unsichere Kommunikation mit der Cloud 1177
31.3.5 Unzureichende Zugangskontrolle 1179
31.3.6 Cloud Computing für Hacker 1180
31.3.7 Übersicht und Zusammenfassung 1180
31.4 Angriffe auf Cloud-Infrastrukturen 1181
31.4.1 Zugangsdaten ermitteln 1181
31.4.2 Persistenten Zugang sichern 1182
31.4.3 Malware einschleusen 1182
31.4.4 Unsichere Voreinstellungen ausnutzen 1183
31.4.5 Cryptojacking 1183
31.4.6 Zugang über Federation Services 1184
31.4.7 Angriffsvektor Webanwendung 1185
31.5 Cloud-Security-Tools 1185
31.5.1 Security-Tools des Cloud-Anbieters 1185
31.5.2 Drittanbieter-Security-Software 1185
31.5.3 Pentest-Simulation mit CloudGoat und Pacu 1186
31.6 Zusammenfassung und Prüfungstipps 1187
31.6.1 Zusammenfassung und Weiterführendes 1187
31.6.2 CEH-Prüfungstipps 1189
31.6.3 Fragen zur CEH-Prüfungsvorbereitung 1189

32 Durchführen von Penetrationstests ... 1191
32.1 Begriffsbestimmung Penetrationstest ... 1191
32.1.1 Was bedeutet »Penetrationstest« eigentlich? ... 1192
32.1.2 Wozu einen Penetrationstest durchführen? ... 1192
32.1.3 Penetrationstest vs. Security Audit vs. Vulnerability Assessment ... 1193
32.1.4 Arten des Penetrationstests ... 1194
32.2 Rechtliche Bestimmungen ... 1195
32.2.1 In Deutschland geltendes Recht ... 1196
32.2.2 US-amerikanisches und internationales Recht ... 1197
32.3 Vorbereitung und praktische Durchführung des Penetrationstests ... 1199
32.3.1 Die Beauftragung ... 1199
32.3.2 Methodik der Durchführung ... 1201
32.3.3 Praxistipps ... 1203
32.4 Der Pentest-Report ... 1206
32.4.1 Dokumentation während des Pentests ... 1206
32.4.2 Was umfasst der Pentest-Report? ... 1207
32.4.3 Aufbau des Pentest-Reports ... 1208
32.5 Abschluss und Weiterführendes ... 1210
32.5.1 Das Abschluss-Meeting ... 1211
32.5.2 Weiterführende Tätigkeiten ... 1211
32.6 Zusammenfassung und Prüfungstipps ... 1211
32.6.1 Zusammenfassung und Weiterführendes ... 1211
32.6.2 CEH-Prüfungstipps ... 1212
32.6.3 Fragen zur CEH-Prüfungsvorbereitung ... 1213

A Lösungen ... 1215

Stichwortverzeichnis ... 1229