

# Hacking

Der umfassende Praxis-Guide

# DAS INHALTS- VERZEICHNIS

» Hier geht's  
direkt  
zum Buch

# Inhaltsverzeichnis

	Einleitung.....	29
	Danksagung.....	36
<b>Teil I</b>	<b>Grundlagen und Arbeitsumgebung.....</b>	<b>37</b>
<b>1</b>	<b>Grundlagen Hacking und Penetration Testing.....</b>	<b>39</b>
1.1	Was ist Hacking?.....	40
1.2	Die verschiedenen Hacker-Typen.....	41
1.3	Motive und Absichten eines Hackers.....	43
1.3.1	Das Motiv.....	43
1.3.2	Ziel des Angriffs.....	44
1.4	Ethical Hacking.....	45
1.5	Der Certified Ethical Hacker (CEHv12).....	46
1.5.1	Was steckt dahinter?.....	47
1.5.2	Die CEHv12-Prüfung im Detail.....	48
1.6	Die Schutzziele: Was wird angegriffen?.....	49
1.6.1	Vertraulichkeit.....	49
1.6.2	Integrität.....	51
1.6.3	Verfügbarkeit.....	53
1.6.4	Authentizität und Nicht-Abstreitbarkeit.....	54
1.6.5	Die Quadratur des Kreises.....	54
1.7	Systematischer Ablauf eines Hacking-Angriffs.....	56
1.7.1	Phasen eines echten Angriffs.....	56
1.7.2	Unterschied zum Penetration Testing.....	58
1.8	Praktische Hacking-Beispiele.....	60
1.8.1	Angriff auf den Deutschen Bundestag.....	60
1.8.2	Stuxnet – der genialste Wurm aller Zeiten.....	61
1.8.3	Angriff auf heise.de mittels Emotet.....	61
1.9	Zusammenfassung und Prüfungstipps.....	62
1.9.1	Zusammenfassung und Weiterführendes.....	62
1.9.2	CEH-Prüfungstipps.....	62
1.9.3	Fragen zur CEH-Prüfungsvorbereitung.....	63
<b>2</b>	<b>Die Arbeitsumgebung einrichten.....</b>	<b>65</b>
2.1	Virtualisierungssoftware.....	66
2.1.1	Software-Alternativen.....	67
2.1.2	Bereitstellung von VirtualBox.....	68
2.2	Die Laborumgebung in der Übersicht.....	70

2.3	Kali Linux	71
2.3.1	Einführung	71
2.3.2	Download von Kali Linux als ISO-Image	72
2.3.3	Kali Linux als VirtualBox-Installation	73
2.3.4	Kali Linux optimieren	77
2.4	Windows 10 als Hacking-Plattform	81
2.4.1	Download von Windows 10	81
2.4.2	Windows-10-Installation in VirtualBox	82
2.4.3	Windows 10 – Spyware inklusive	82
2.4.4	Gasterweiterungen installieren	83
2.5	Übungsumgebung und Zielscheiben einrichten	84
2.5.1	Metasploitable	85
2.5.2	Die Netzwerkumgebung in VirtualBox anpassen	87
2.5.3	Multifunktionsserver unter Linux	90
2.5.4	Windows XP und ältere Windows-Betriebssysteme	90
2.5.5	Eine Windows-Netzwerkumgebung aufbauen	91
2.6	Zusammenfassung und Weiterführendes	91
<b>3</b>	<b>Einführung in Kali Linux</b>	<b>93</b>
3.1	Ein erster Rundgang	93
3.1.1	Überblick über den Desktop	94
3.1.2	Das Startmenü	97
3.1.3	Der Dateimanager	99
3.1.4	Systemeinstellungen und -Tools	101
3.2	Workshop: Die wichtigsten Linux-Befehle	102
3.2.1	Orientierung und Benutzerwechsel	103
3.2.2	Von Skripten und Dateiberechtigungen	105
3.2.3	Arbeiten mit Root-Rechten	107
3.2.4	Das Dateisystem und die Pfade	110
3.2.5	Dateien und Verzeichnisse erstellen, kopieren, löschen etc.	111
3.2.6	Dateien anzeigen	112
3.2.7	Dateien finden und durchsuchen	114
3.2.8	Die Man-Pages: Hilfe zur Selbsthilfe	116
3.2.9	Dienste starten und überprüfen	117
3.3	Die Netzwerk-Konfiguration anzeigen und anpassen	119
3.3.1	IP-Adresse anzeigen	119
3.3.2	Routing-Tabelle anzeigen	120
3.3.3	DNS-Server anzeigen	120
3.3.4	Konfiguration der Schnittstellen	121
3.4	Software-Installation und -Update	123
3.4.1	Die Paketlisten aktualisieren	123
3.4.2	Installation von Software-Paketen	124
3.4.3	Software suchen	124
3.4.4	Entfernen von Software-Paketen	125
3.5	Zusammenfassung und Prüfungstipps	126

3.5.1	Zusammenfassung und Weiterführendes .....	126
3.5.2	CEH-Prüfungstipps .....	126
3.5.3	Fragen zur CEH-Prüfungsvorbereitung .....	126
<b>4</b>	<b>Anonym bleiben und sicher kommunizieren .....</b>	<b>129</b>
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 .....	134
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 .....	137
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 .....	147
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
<b>5</b>	<b>Kryptografie und ihre Schwachstellen .....</b>	<b>163</b>
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 .....	176
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 .....	187
5.5.1	Das Prinzip der digitalen Signatur .....	187
5.5.2	Wichtige Verfahren der digitalen Signatur .....	189
5.6	Public-Key-Infrastrukturen (PKI) .....	189
5.6.1	Das Prinzip von PKI .....	190
5.6.2	Digitale Zertifikate .....	190
5.6.3	Zertifikate und PKI in der Praxis .....	191
5.6.4	Zertifikatssperllisten und OCSP .....	195
5.7	Virtual Private Networks (VPN) .....	197
5.7.1	IPsec-VPNs .....	198
5.7.2	SSL-VPNs .....	199
5.8	Angriffe auf kryptografische Systeme .....	201
5.8.1	Methodologie der Kryptoanalyse .....	201
5.8.2	Der Heartbleed-Angriff .....	203
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

<b>6</b>	<b>Informationsbeschaffung – Footprinting &amp; Reconnaissance .....</b>	<b>217</b>
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	250
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	<b>Scanning – das Netzwerk unter der Lupe</b>	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 . . . . .	272
7.3.6	Betriebssystem-Erkennung . . . . .	273
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 . . . . .	278
7.4.1	Was ist Metasploit? . . . . .	278
7.4.2	Erste Schritte mit Metasploit (MSF) . . . . .	278
7.4.3	Nmap in Metasploit nutzen . . . . .	282
7.5	Weitere Tools und Verfahren . . . . .	284
7.5.1	Paketerstellung und Scanning mit hping3 . . . . .	284
7.5.2	Weitere Packet-Crafting-Tools . . . . .	286
7.5.3	Banner Grabbing mit Telnet und Netcat . . . . .	286
7.5.4	Scannen von IPv6-Netzwerken . . . . .	288
7.6	Gegenmaßnahmen gegen Portscanning und Banner Grabbing . . . . .	289
7.7	Zusammenfassung und Prüfungstipps . . . . .	290
7.7.1	Zusammenfassung und Weiterführendes . . . . .	290
7.7.2	CEH-Prüfungstipps . . . . .	290
7.7.3	Fragen zur CEH-Prüfungsvorbereitung . . . . .	291
8	<b>Enumeration – welche Ressourcen sind verfügbar?</b> . . . . .	295
8.1	Was wollen wir mit Enumeration erreichen? . . . . .	295
8.2	NetBIOS- und SMB-Enumeration . . . . .	296
8.2.1	Die Protokolle NetBIOS und SMB . . . . .	296
8.2.2	Der Enumeration-Prozess . . . . .	298
8.3	SNMP-Enumeration . . . . .	303
8.3.1	SNMP-Grundlagen . . . . .	304
8.3.2	SNMP-Agents identifizieren . . . . .	306
8.3.3	Enumeration-Tools nutzen . . . . .	307
8.4	LDAP-Enumeration . . . . .	312
8.4.1	LDAP- und AD-Grundlagen . . . . .	312
8.4.2	Der Enumeration-Prozess . . . . .	314
8.5	SMTP-Enumeration . . . . .	316
8.5.1	SMTP-Grundlagen . . . . .	316
8.5.2	Der Enumeration-Prozess . . . . .	317
8.6	NTP-Enumeration . . . . .	320

8.6.1	Funktionsweise von NTP .....	320
8.6.2	Der Enumeration-Prozess .....	320
8.7	DNS-Enumeration .....	322
8.7.1	NFS-Enumeration .....	327
8.7.2	Weitere Enumeration-Techniken .....	328
8.8	Schutzmaßnahmen gegen Enumeration .....	328
8.9	Zusammenfassung und Prüfungstipps .....	331
8.9.1	Zusammenfassung und Weiterführendes .....	331
8.9.2	CEH-Prüfungstipps .....	331
8.9.3	Fragen zur CEH-Prüfungsvorbereitung .....	332
<b>9</b>	<b>Vulnerability-Scanning und Schwachstellenanalyse .....</b>	<b>335</b>
9.1	Was steckt hinter Vulnerability-Scanning? .....	335
9.1.1	Vulnerabilities und Exploits .....	336
9.1.2	Common Vulnerabilities and Exposures (CVE) .....	336
9.1.3	CVE- und Exploit-Datenbanken .....	338
9.1.4	Vulnerability-Scanner .....	339
9.2	Vulnerability-Scanning mit Nmap .....	341
9.2.1	Die Kategorie »vuln« .....	341
9.2.2	Die passenden Skripts einsetzen .....	341
9.3	Nessus .....	344
9.3.1	Installation von Nessus .....	344
9.3.2	Vulnerability-Scanning mit Nessus .....	345
9.3.3	Nessus versus OpenVAS .....	349
9.4	Rapid 7 Nexpose .....	350
9.5	Vulnerability-Scanning in der Praxis .....	351
9.5.1	Vulnerability-Assessments .....	351
9.5.2	Einsatz von Vulnerability-Scannern im Ethical Hacking .....	352
9.5.3	Credentialed Scan vs. Remote Scan .....	353
9.5.4	Verifizieren der Schwachstelle .....	354
9.5.5	Exploits zum Testen von Schwachstellen .....	354
9.5.6	Spezialisierte Scanner .....	355
9.6	Zusammenfassung und Prüfungstipps .....	355
9.6.1	Zusammenfassung und Weiterführendes .....	355
9.6.2	CEH-Prüfungstipps .....	356
9.6.3	Fragen zur CEH-Prüfungsvorbereitung .....	356
<b>Teil III</b>	<b>Systeme angreifen .....</b>	<b>359</b>
<b>10</b>	<b>Password Hacking .....</b>	<b>365</b>
10.1	Zugriffsschutz mit Passwörtern und anderen Methoden .....	365
10.2	Angriffsvektoren auf Passwörter .....	367
10.2.1	Nicht elektronische Angriffe .....	367
10.2.2	Aktive Online-Angriffe .....	367



10.2.3	Passive Online-Angriffe . . . . .	368
10.2.4	Offline-Angriffe . . . . .	368
10.3	Password Guessing und Password Recovery . . . . .	368
10.3.1	Grundlagen des Password Guessings . . . . .	369
10.3.2	Default-Passwörter . . . . .	370
10.3.3	Password Recovery unter Windows . . . . .	372
10.3.4	Password Recovery für Linux . . . . .	378
10.3.5	Password Recovery auf Cisco-Routern . . . . .	379
10.4	Die Windows-Authentifizierung . . . . .	381
10.4.1	Die SAM-Datenbank . . . . .	381
10.4.2	LM und NTLM . . . . .	381
10.4.3	Kerberos . . . . .	382
10.4.4	NTLM-Hashes auslesen mit FGDump . . . . .	386
10.5	Die Linux-Authentifizierung . . . . .	388
10.5.1	Speicherorte der Login-Daten . . . . .	388
10.5.2	Passwort-Hashes unter Linux . . . . .	389
10.5.3	Der Salt – Passwort-Hashes »salzen« . . . . .	390
10.5.4	Wie gelangen wir an die Passwort-Hashes? . . . . .	391
10.6	Passwort-Hashes angreifen . . . . .	392
10.6.1	Angriffsvektoren auf Passwort-Hashes . . . . .	392
10.6.2	Pass the Hash (PTH) . . . . .	396
10.6.3	Wortlisten erstellen . . . . .	397
10.6.4	L0phtcrack . . . . .	402
10.6.5	John the Ripper . . . . .	404
10.6.6	Hashcat . . . . .	406
10.6.7	Cain & Abel . . . . .	406
10.7	Online-Angriffe auf Passwörter . . . . .	407
10.7.1	Grundlegende Problematik . . . . .	407
10.7.2	Medusa . . . . .	407
10.7.3	Hydra . . . . .	409
10.7.4	Ncrack . . . . .	410
10.8	Distributed Network Attack (DNA) . . . . .	412
10.8.1	Funktionsweise . . . . .	412
10.8.2	ElcomSoft Distributed Password Recovery . . . . .	413
10.9	Schutzmaßnahmen gegen Password Hacking . . . . .	413
10.10	Zusammenfassung und Prüfungstipps . . . . .	415
10.10.1	Zusammenfassung und Weiterführendes . . . . .	415
10.10.2	CEH-Prüfungstipps . . . . .	415
10.10.3	Fragen zur CEH-Prüfungsvorbereitung . . . . .	416
<b>11</b>	<b>Shells und Post-Exploitation . . . . .</b>	<b>417</b>
11.1	Remote-Zugriff mit Shell und Backdoor . . . . .	417
11.1.1	Einführung in Shells und Backdoors . . . . .	418
11.1.2	Netcat und Ncat – Einführung . . . . .	420
11.1.3	Grundlegende Funktionsweise von Netcat und Ncat . . . . .	421

11.1.4	Eine Bind-Shell bereitstellen . . . . .	424
11.1.5	Eine Reverse-Shell bereitstellen . . . . .	426
11.1.6	Wo stehen wir jetzt? . . . . .	427
11.2	Grundlagen Privilegien-Eskalation . . . . .	427
11.2.1	Vertikale Rechteerweiterung . . . . .	428
11.2.2	Horizontale Rechteerweiterung . . . . .	428
11.2.3	Rechte von Programmen . . . . .	428
11.3	Mit Privilegien-Eskalation zur Root-Shell . . . . .	429
11.3.1	Reverse-Shell durch DistCC-Exploit . . . . .	429
11.3.2	Bereitstellung eines Post-Exploits . . . . .	430
11.3.3	Mit Metasploit-Multi-Handler zur Root-Shell . . . . .	434
11.4	Meterpreter – die Luxus-Shell für Hacker . . . . .	435
11.4.1	Exploits und Payload . . . . .	435
11.4.2	Einführung in Meterpreter . . . . .	436
11.4.3	Meterpreter-Shell in der Praxis . . . . .	438
11.4.4	Eine Meterpreter-Shell für Windows erstellen . . . . .	440
11.4.5	Externe Module in Meterpreter laden . . . . .	443
11.5	Privilegien-Eskalation in einer Windows Domäne . . . . .	444
11.5.1	Das Szenario . . . . .	445
11.5.2	Ermittlung des Domain-Controllers . . . . .	445
11.5.3	Privilegien-Eskalation durchführen . . . . .	446
11.6	Verteidigungsmaßnahmen gegen Privilegien-Eskalation . . . . .	447
11.7	Zusammenfassung und Prüfungstipps . . . . .	448
11.7.1	Zusammenfassung und Weiterführendes . . . . .	448
11.7.2	CEH-Prüfungstipps . . . . .	449
11.7.3	Fragen zur CEH-Prüfungsvorbereitung . . . . .	449
<b>12</b>	<b>Mit Malware das System übernehmen . . . . .</b>	<b>451</b>
12.1	Malware-Grundlagen . . . . .	452
12.1.1	Typische Malware-Kategorien . . . . .	452
12.1.2	Wie gelangt Malware auf das Opfer-System? . . . . .	455
12.1.3	Eine selbst erstellte Malware . . . . .	456
12.2	Viren und Würmer . . . . .	457
12.2.1	Was ist ein Computervirus? . . . . .	457
12.2.2	Was ist ein Computerwurm? . . . . .	459
12.2.3	Einen Makro-Virus erstellen . . . . .	460
12.3	Trojanische Pferde in der Praxis . . . . .	465
12.3.1	Trojaner-Typen . . . . .	465
12.3.2	Einen Trojaner selbst bauen . . . . .	467
12.3.3	Viren- und Trojaner-Baukästen . . . . .	470
12.4	Malware tarnen und vor Entdeckung schützen . . . . .	472
12.4.1	Grundlagen der Tarnung von Payload . . . . .	473
12.4.2	Encoder einsetzen . . . . .	475
12.4.3	Payload mit Hyperion verschlüsseln . . . . .	478
12.4.4	Das Veil-Framework . . . . .	479

12.4.5	Shellter AV Evasion	480
12.4.6	Fileless Malware	481
12.5	Rootkits	482
12.5.1	Grundlagen der Rootkits	483
12.5.2	Kernel-Rootkits	484
12.5.3	Userland-Rootkits	484
12.5.4	Rootkit-Beispiele	484
12.5.5	Rootkits entdecken und entfernen	485
12.6	Covert Channel	486
12.6.1	ICMP-Tunneling	486
12.6.2	NTFS Alternate Data Stream (ADS)	489
12.7	Keylogger und Spyware	491
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
<b>13</b>	<b>Malware-Erkennung und -Analyse</b>	<b>503</b>
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	532
13.3	Sheep-Dip-Systeme	533
13.3.1	Einführung	533
13.3.2	Aufbau eines Sheep-Dip-Systems	534
13.4	Schutz durch Sandbox	535
13.4.1	Sandboxie	535
13.4.2	Cuckoo	537

13.5	Allgemeine Schutzmaßnahmen vor Malware-Infektion .....	538
13.6	Zusammenfassung und Prüfungstipps .....	539
13.6.1	Zusammenfassung und Weiterführendes .....	539
13.6.2	CEH-Prüfungstipps .....	540
13.6.3	Fragen zur CEH-Prüfungsvorbereitung .....	540
<b>14</b>	<b>Steganografie</b> .....	<b>543</b>
14.1	Grundlagen der Steganografie .....	543
14.1.1	Wozu Steganografie? .....	543
14.1.2	Ein paar einfache Beispiele .....	544
14.1.3	Klassifikation der Steganografie .....	545
14.2	Computergestützte Steganografie .....	549
14.2.1	Daten in Bildern verstecken .....	549
14.2.2	Daten in Dokumenten verstecken .....	554
14.2.3	Weitere Cover-Datenformate .....	555
14.3	Steganalyse und Schutz vor Steganografie .....	556
14.3.1	Methoden der Steganalyse .....	556
14.3.2	Steganalyse-Tools .....	557
14.3.3	Schutz vor Steganografie .....	557
14.4	Zusammenfassung und Prüfungstipps .....	558
14.4.1	Zusammenfassung und Weiterführendes .....	558
14.4.2	CEH-Prüfungstipps .....	559
14.4.3	Fragen zur CEH-Prüfungsvorbereitung .....	559
<b>15</b>	<b>Spuren verwischen</b> .....	<b>561</b>
15.1	Auditing und Logging .....	561
15.1.1	Die Windows-Protokollierung .....	562
15.1.2	Die klassische Linux-Protokollierung .....	564
15.2	Spuren verwischen auf einem Windows-System .....	567
15.2.1	Das Windows-Auditing deaktivieren .....	567
15.2.2	Windows-Ereignisprotokolle löschen .....	569
15.2.3	Most Recently Used (MRU) löschen .....	571
15.2.4	Zeitstempel manipulieren .....	573
15.2.5	Clearing-Tools .....	576
15.3	Spuren verwischen auf einem Linux-System .....	578
15.3.1	Logfiles manipulieren und löschen .....	578
15.3.2	Systemd-Logging in Journald. ....	580
15.3.3	Zeitstempel manipulieren .....	581
15.3.4	Die Befehlszeilen-Historie löschen .....	583
15.4	Schutz vor dem Spuren-Verwischen .....	584
15.5	Zusammenfassung und Prüfungstipps .....	585
15.5.1	Zusammenfassung und Weiterführendes .....	585
15.5.2	CEH-Prüfungstipps .....	586
15.5.3	Fragen zur CEH-Prüfungsvorbereitung .....	587

<b>Teil IV</b>	<b>Netzwerk- und sonstige Angriffe</b>	<b>589</b>
<b>16</b>	<b>Network Sniffing mit Wireshark &amp; Co.</b>	<b>593</b>
16.1	Grundlagen von Netzwerk-Sniffern	593
16.1.1	Technik der Netzwerk-Sniffer	593
16.1.2	Wireshark und die Pcap-Bibliotheken	595
16.2	Wireshark installieren und starten	595
16.2.1	Installation unter Linux	595
16.2.2	Installation unter Windows	596
16.2.3	Der erste Start	597
16.3	Die ersten Schritte mit Wireshark	598
16.3.1	Grundeinstellungen	598
16.3.2	Ein erster Mitschnitt	600
16.4	Mitschnitt-Filter einsetzen	601
16.4.1	Analyse eines TCP-Handshakes	602
16.4.2	Der Ping in Wireshark	603
16.4.3	Weitere Mitschnittfilter	604
16.5	Anzeigefilter einsetzen	605
16.5.1	Eine HTTP-Sitzung im Detail	606
16.5.2	Weitere Anzeigefilter	608
16.6	Passwörter und andere Daten ausspähen	609
16.6.1	FTP-Zugangsdaten ermitteln	610
16.6.2	Telnet-Zugangsdaten identifizieren	611
16.6.3	SSH – sicherer Schutz gegen Mitlesen	613
16.6.4	Andere Daten ausspähen	615
16.7	Auswertungsfunktionen von Wireshark nutzen	616
16.8	Tcpdump und TShark einsetzen	618
16.8.1	Tcpdump – der Standard-Sniffer für die Konsole	618
16.8.2	TShark – Wireshark auf der Konsole	621
16.9	Zusammenfassung und Prüfungstipps	623
16.9.1	Zusammenfassung und Weiterführendes	623
16.9.2	CEH-Prüfungstipps	623
16.9.3	Fragen zur CEH-Prüfungsvorbereitung	624
<b>17</b>	<b>Lauschangriffe &amp; Man-in-the-Middle</b>	<b>627</b>
17.1	Eavesdropping und Sniffing für Hacker	627
17.1.1	Eavesdropping und Wiretapping	628
17.1.2	Sniffing als Angriffsvektor	628
17.2	Man-in-the-Middle (MITM)	629
17.2.1	Was bedeutet Man-in-the-Middle?	630
17.2.2	Was erreichen wir durch einen MITM-Angriff?	631
17.3	Active Sniffing	631
17.3.1	Mirror-Ports: Ein Kabel mit drei Enden	632
17.3.2	Aus Switch mach Hub – MAC-Flooding	632
17.3.3	Auf dem Silbertablett: WLAN-Sniffing	634

17.3.4	Weitere physische Abhörmöglichkeiten .....	635
17.4	Die Kommunikation für MITM umleiten .....	635
17.4.1	Physische Umleitung .....	635
17.4.2	Umleitung über aktive Netzwerk-Komponenten .....	636
17.4.3	Umleiten mit ARP-Spoofing .....	637
17.4.4	ICMP-Typ 5 Redirect .....	637
17.4.5	DNS-Spoofing oder DNS-Cache-Poisoning .....	638
17.4.6	Manipulation der hosts-Datei. ....	640
17.4.7	Umleiten via DHCP-Spoofing .....	641
17.5	Die Dsniff-Toolsammlung .....	642
17.5.1	Programme der Dsniff-Suite .....	642
17.5.2	Abhören des Netzwerk-Traffics .....	643
17.5.3	MITM mit arpspoof .....	644
17.5.4	Die ARP-Tabelle des Switches mit macof überfluten .....	647
17.5.5	DNS-Spoofing mit dnsnoop .....	647
17.5.6	Dsniff .....	650
17.6	Man-in-the-Middle-Angriffe mit Ettercap .....	651
17.6.1	Einführung in Ettercap .....	651
17.6.2	DNS-Spoofing mit Ettercap .....	653
17.7	Schutz vor Lauschangriffen & MITM .....	661
17.8	Zusammenfassung und Prüfungstipps .....	663
17.8.1	Zusammenfassung und Weiterführendes .....	663
17.8.2	CEH-Prüfungstipps .....	664
17.8.3	Fragen zur CEH-Prüfungsvorbereitung .....	664
<b>18</b>	<b>Session Hijacking</b> .....	<b>667</b>
18.1	Grundlagen des Session Hijackings .....	667
18.1.1	Wie funktioniert Session Hijacking grundsätzlich? .....	668
18.1.2	Session-Hijacking-Varianten .....	668
18.2	Network Level Session Hijacking .....	669
18.2.1	Die TCP-Session im Detail .....	670
18.2.2	Entführen von TCP-Sessions .....	672
18.2.3	Weitere Hijacking-Varianten auf Netzwerk-Ebene .....	674
18.3	Application Level Session Hijacking .....	675
18.3.1	Die Session-IDs .....	676
18.3.2	Die Session-ID ermitteln .....	677
18.3.3	Sniffing/Man-in-the-Middle .....	677
18.3.4	Die Session-ID erraten – das Prinzip .....	678
18.3.5	WebGoat bereitstellen .....	678
18.3.6	Die Burp Suite – Grundlagen und Installation .....	681
18.3.7	Burp Suite als Intercepting Proxy .....	683
18.3.8	Der Burp Sequencer – Session-IDs analysieren .....	686
18.3.9	Entführen der Session mithilfe der Session-ID .....	690
18.3.10	Man-in-the-Browser-Angriff .....	696

18.3.11	Weitere Angriffsformen . . . . .	698
18.4	Gegenmaßnahmen gegen Session Hijacking . . . . .	700
18.4.1	Session Hijacking entdecken . . . . .	700
18.4.2	Schutzmaßnahmen . . . . .	701
18.5	Zusammenfassung und Prüfungstipps . . . . .	703
18.5.1	Zusammenfassung und Weiterführendes . . . . .	703
18.5.2	CEH-Prüfungstipps . . . . .	704
18.5.3	Fragen zur CEH-Prüfungsvorbereitung . . . . .	704
<b>19</b>	<b>Firewalls, IDS/IPS und Honeypots einsetzen und umgehen . . . . .</b>	<b>707</b>
19.1	Firewall-Technologien . . . . .	707
19.1.1	Netzwerk- und Personal-Firewalls . . . . .	708
19.1.2	Filtertechniken und Kategorisierung der Netzwerk-Firewalls . . . . .	709
19.2	Firewall-Szenarien . . . . .	713
19.2.1	DMZ-Szenarien . . . . .	713
19.2.2	Failover-Szenarien . . . . .	715
19.3	Firewalls umgehen . . . . .	716
19.3.1	Identifikation von Firewalls . . . . .	716
19.3.2	IP-Adress-Spoofing . . . . .	717
19.3.3	Was wirklich funktioniert . . . . .	718
19.4	Intrusion-Detection- und -Prevention-Systeme . . . . .	719
19.4.1	Grundlagen und Unterschiede zwischen IDS und IPS . . . . .	719
19.4.2	Einführung in Snort . . . . .	722
19.5	Intrusion-Detection-Systeme umgehen . . . . .	726
19.5.1	Injection/Insertion . . . . .	726
19.5.2	Evasion . . . . .	727
19.5.3	Denial-of-Service-Angriff (DoS) . . . . .	728
19.5.4	Obfuscation . . . . .	728
19.5.5	Generieren von False Positives . . . . .	728
19.5.6	Fragmentation . . . . .	729
19.5.7	TCP Session Splicing . . . . .	730
19.5.8	Weitere Evasion-Techniken . . . . .	730
19.6	Network Access Control (NAC) . . . . .	731
19.6.1	NAC-Lösungen - Grundlagen . . . . .	731
19.6.2	Angriffsvektoren auf NAC-Lösungen . . . . .	732
19.7	Honeypots . . . . .	733
19.7.1	Grundlagen und Begriffsklärung . . . . .	734
19.7.2	Kategorisierung der Honeypots . . . . .	734
19.7.3	Valhala – ein Honeypot in der Praxis . . . . .	737
19.7.4	Honeypots identifizieren und umgehen . . . . .	740
19.7.5	Rechtliche Aspekte beim Einsatz von Honeypots . . . . .	742
19.8	Zusammenfassung und Prüfungstipps . . . . .	742
19.8.1	Zusammenfassung und Weiterführendes . . . . .	742
19.8.2	CEH-Prüfungstipps . . . . .	744
19.8.3	Fragen zur CEH-Prüfungsvorbereitung . . . . .	744

<b>20</b>	<b>Social Engineering</b> .....	747
20.1	Einführung in das Social Engineering .....	747
20.1.1	Welche Gefahren birgt Social Engineering? .....	748
20.1.2	Verlustangst, Neugier, Eitelkeit – die Schwachstellen des Systems Mensch .....	748
20.1.3	Varianten des Social Engineerings .....	751
20.1.4	Allgemeine Vorgehensweise beim Social Engineering .....	753
20.2	Human Based Social Engineering .....	754
20.2.1	Vortäuschen einer anderen Identität .....	754
20.2.2	Shoulder Surfing & Co. ....	756
20.2.3	Piggybacking und Tailgaiting .....	757
20.3	Computer Based Social Engineering .....	758
20.3.1	Phishing .....	758
20.3.2	Pharming .....	758
20.3.3	Spear Phishing .....	759
20.3.4	Drive-by-Downloads .....	760
20.3.5	Gefälschte Viren-Warnungen .....	761
20.4	Das Social-Engineer Toolkit (SET) .....	762
20.4.1	Einführung in SET .....	762
20.4.2	Praxisdemonstration: Credential Harvester .....	764
20.4.3	Weitere Angriffe mit SET .....	767
20.5	So schützen Sie sich gegen Social-Engineering-Angriffe .....	768
20.6	Zusammenfassung und Prüfungstipps .....	770
20.6.1	Zusammenfassung und Weiterführendes .....	770
20.6.2	CEH-Prüfungstipps .....	771
20.6.3	Fragen zur CEH-Prüfungsvorbereitung .....	771
<b>21</b>	<b>Hacking-Hardware</b> .....	773
21.1	Allgemeines und rechtliche Hinweise zu Spionage-Hardware .....	774
21.2	Angriffsvektor USB-Schnittstelle .....	774
21.2.1	Hardware Keylogger .....	775
21.2.2	USB Rubber Ducky .....	776
21.2.3	Bash Bunny .....	779
21.2.4	Digispark .....	781
21.2.5	USBNinja .....	782
21.2.6	Mouse Jiggler .....	783
21.3	Weitere Hacking-Gadgets .....	783
21.3.1	VideoGhost .....	783
21.3.2	Packet Squirrel .....	784
21.3.3	LAN Turtle .....	785
21.3.4	Throwing Star LAN Tap .....	785
21.3.5	Software Defined Radio .....	786
21.3.6	Crazyradio PA .....	786
21.3.7	WiFi Pinapple .....	787



21.3.8	Proxmark 3 . . . . .	788
21.3.9	ChameleonMini . . . . .	788
21.4	Raspberry Pi als Hacking-Kit . . . . .	788
21.5	Gegenmaßnahmen . . . . .	790
21.6	Zusammenfassung und Prüfungstipps . . . . .	792
21.6.1	Zusammenfassung und Weiterführendes . . . . .	792
21.6.2	CEH-Prüfungstipps . . . . .	793
21.6.3	Fragen zur CEH-Prüfungsvorbereitung . . . . .	793
<b>22</b>	<b>DoS- und DDoS-Angriffe . . . . .</b>	<b>795</b>
22.1	DoS- und DDoS-Grundlagen . . . . .	795
22.1.1	Was ist ein Denial-of-Service-Angriff? . . . . .	796
22.1.2	Warum werden DoS- und DDoS-Angriffe durchgeführt? . . . . .	796
22.1.3	Kategorien der DoS/DDoS-Angriffe . . . . .	797
22.2	DoS- und DDoS-Angriffstechniken . . . . .	797
22.2.1	UDP-Flood-Angriff . . . . .	798
22.2.2	ICMP-Flood-Angriff . . . . .	798
22.2.3	Smurf-Angriff . . . . .	799
22.2.4	Syn-Flood-Angriff . . . . .	800
22.2.5	Fragmentation-Angriff . . . . .	803
22.2.6	Slowloris-Angriff . . . . .	804
22.2.7	Permanenter Denial-of-Service (PDoS) . . . . .	805
22.2.8	Distributed-Reflected-Denial-of-Service-Angriff (DRDoS) . . . . .	806
22.3	Botnetze – Funktionsweise und Betrieb . . . . .	807
22.3.1	Bots und deren Einsatzmöglichkeiten . . . . .	808
22.3.2	Aufbau eines Botnetzes . . . . .	808
22.3.3	Wie gelangen Bots auf die Opfer-Systeme? . . . . .	810
22.3.4	Mobile Systeme und IoT . . . . .	811
22.3.5	Botnetze in der Praxis . . . . .	811
22.3.6	Verteidigung gegen Botnetze und DDoS-Angriffe . . . . .	812
22.4	DoS-Angriffe in der Praxis . . . . .	814
22.4.1	SYN- und ICMP-Flood-Angriff mit hping3 . . . . .	815
22.4.2	DoS-Angriff mit Metasploit . . . . .	817
22.4.3	DoS-Angriff mit SlowHTTPTest . . . . .	819
22.4.4	Low Orbit Ion Cannon (LOIC) . . . . .	821
22.5	Verteidigung gegen DoS- und DDoS-Angriffe . . . . .	822
22.5.1	Allgemeiner Grundschutz . . . . .	822
22.5.2	Schutz vor volumetrischen DDoS-Angriffen . . . . .	823
22.6	Zusammenfassung und Prüfungstipps . . . . .	824
22.6.1	Zusammenfassung und Weiterführendes . . . . .	824
22.6.2	CEH-Prüfungstipps . . . . .	825
22.6.3	Fragen zur CEH-Prüfungsvorbereitung . . . . .	825

<b>Teil V</b>	<b>Web-Hacking</b> .....	827
<b>23</b>	<b>Web-Hacking – Grundlagen</b> .....	831
23.1	Was ist Web-Hacking? .....	831
23.2	Architektur von Webanwendungen .....	832
23.2.1	Die Schichten-Architektur .....	832
23.2.2	Die URL-Codierung .....	833
23.2.3	Das Hypertext Transfer Protocol (HTTP) .....	834
23.2.4	Cookies .....	837
23.2.5	HTTP vs. HTTPS .....	837
23.2.6	Webservices und -technologien .....	838
23.3	Die gängigsten Webserver: Apache, IIS, nginx .....	843
23.3.1	Apache HTTP Server .....	843
23.3.2	Internet Information Services (IIS) .....	845
23.3.3	nginx .....	847
23.4	Typische Schwachstellen von Webservern und -anwendungen .....	848
23.4.1	Schwachstellen in Webserver-Plattformen .....	848
23.4.2	Schwachstellen in der Webanwendung .....	849
23.5	Reconnaissance für Web-Hacking-Angriffe .....	850
23.5.1	Footprinting und Scanning .....	850
23.5.2	Web-Firewalls und Proxys entlarven .....	852
23.5.3	Hidden Content Discovery .....	852
23.5.4	Website-Mirroring .....	855
23.5.5	Security-Scanner .....	855
23.6	Praxis-Szenario: Einen Apache-Webserver mit Shellshock hacken .....	858
23.6.1	Die Laborumgebung präparieren .....	858
23.6.2	Den Angriff durchführen .....	860
23.7	Praxis-Szenario 2: Angriff auf WordPress .....	861
23.7.1	WordPress-VM bereitstellen .....	862
23.7.2	WordPress scannen und Enumeration .....	866
23.7.3	User-Hacking .....	868
23.8	Zusammenfassung und Prüfungstipps .....	868
23.8.1	Zusammenfassung und Weiterführendes .....	868
23.8.2	CEH-Prüfungstipps .....	869
23.8.3	Fragen zur CEH-Prüfungsvorbereitung .....	869
<b>24</b>	<b>Web-Hacking – OWASP Top 10</b> .....	871
24.1	Einführung in die OWASP-Projekte .....	871
24.1.1	OWASP Juice Shop .....	872
24.1.2	OWASP ModSecurity Core Rule Set (CRS) .....	873
24.1.3	OWASP Web Security Testing Guide .....	873
24.1.4	OWASP Top 10 .....	873
24.2	WebGoat & Co – virtuelle Sandsäcke für das Web-Hacking-Training .....	874
24.2.1	WebGoat .....	875
24.2.2	Mutillidae II .....	875

24.2.3	bWAPP	876
24.2.4	DVWA	877
24.2.5	Web Security Dojo	878
24.2.6	Vulnhub und Pentesterlab	879
24.3	Die OWASP Top 10 in der Übersicht	879
24.4	A01 – Broken Access Control	880
24.4.1	Unsichere direkte Objektreferenzen	880
24.4.2	Fehlerhafte Autorisierung auf Anwendungsebene	882
24.4.3	Schutzmaßnahmen	885
24.5	A02 – Cryptographic Failures	886
24.5.1	Welche Daten sind betroffen?	886
24.5.2	Angriffsszenarien	887
24.5.3	Schutzmaßnahmen	888
24.6	A03 – Injection	889
24.6.1	Kategorien von Injection-Angriffen	889
24.6.2	Beispiel für einen Injection-Angriff	889
24.6.3	Cross-Site-Scripting (XSS)	892
24.6.4	Wie funktioniert XSS?	892
24.6.5	Ein einfaches XSS-Beispiel	893
24.6.6	XSS-Varianten	895
24.6.7	Ein Beispiel für Stored XSS	897
24.6.8	Exkurs: Cross-Site-Request-Forgery (CSRF)	898
24.6.9	Schutzmaßnahmen gegen XSS-Angriffe	900
24.7	A04 – Insecure Design	901
24.7.1	Was bedeutet unsicheres Design?	901
24.7.2	Sichere Webentwicklung	902
24.7.3	Schutzmaßnahmen	902
24.8	A05 – Security Misconfiguration	903
24.8.1	Typische Fehlkonfigurationen	903
24.8.2	Directory Browsing	903
24.8.3	Allgemeine Schutzmaßnahmen	905
24.8.4	A4 – XML External Entities (XXE)	906
24.8.5	XML-Entities	906
24.8.6	Ein Beispiel für einen XXE-Angriff	907
24.8.7	Schutzmaßnahmen	908
24.9	A06 – Vulnerable and Outdated Components	909
24.9.1	Worin liegt die Gefahr und wer ist gefährdet?	909
24.9.2	Verwundbare JavaScript-Bibliotheken aufdecken mit Retire.js	909
24.9.3	Schutzmaßnahmen	910
24.10	A07 – Identification and Authentication Failures	911
24.10.1	Grundlagen	911
24.10.2	Identitätsdiebstahl durch Token-Manipulation	911
24.10.3	Schutzmaßnahmen	914
24.11	A08 – Software and Data Integrity Failures	914

24.11.1	Was bedeutet Integritätsverletzung? . . . . .	915
24.11.2	Unsichere Deserialisierung . . . . .	915
24.11.3	Was bedeutet Serialisierung von Daten?. . . . .	915
24.11.4	Wie wird die Deserialisierung zum Problem? . . . . .	916
24.11.5	Schutzmaßnahmen . . . . .	916
24.12	A09 – Security Logging and Monitoring Failures. . . . .	917
24.12.1	Herausforderungen beim Logging & Monitoring . . . . .	917
24.12.2	Sind unserer Systeme gefährdet? . . . . .	918
24.13	A10 – Server-Side Request Forgery (SSRF). . . . .	919
24.13.1	Wie funktioniert SSRF? . . . . .	919
24.13.2	Ein SSRF-Beispiel. . . . .	920
24.14	Zusammenfassung und Prüfungstipps . . . . .	923
24.14.1	Zusammenfassung und Weiterführendes . . . . .	923
24.14.2	CEH-Prüfungstipps . . . . .	923
24.14.3	Fragen zur CEH-Prüfungsvorbereitung . . . . .	924
<b>25</b>	<b>SQL-Injection. . . . .</b>	<b>925</b>
25.1	Mit SQL-Injection das Login austricksen . . . . .	926
25.1.1	Der grundlegende Ansatz. . . . .	926
25.1.2	Anmeldung als gewünschter Benutzer . . . . .	930
25.1.3	Clientseitige Sicherheit. . . . .	930
25.2	Daten auslesen mit SQL-Injection . . . . .	932
25.2.1	Manipulation eines GET-Requests . . . . .	933
25.2.2	Informationen über die Datenbank auslesen . . . . .	934
25.2.3	Die Datenbank-Tabellen identifizieren . . . . .	936
25.2.4	Spalten und Passwörter auslesen . . . . .	938
25.3	Fortgeschrittene SQL-Injection-Techniken . . . . .	939
25.3.1	Einführung in Blind SQL-Injection. . . . .	940
25.3.2	Codieren des Injection-Strings . . . . .	942
25.3.3	Blind SQLi: Eins oder null? . . . . .	945
25.3.4	Time based SQL-Injection . . . . .	946
25.4	SQLMap – automatische Schwachstellensuche . . . . .	948
25.4.1	SQLi-CheatSheets . . . . .	948
25.4.2	Einführung in SQLMap . . . . .	949
25.4.3	Weitere Analysen mit SQLMap . . . . .	954
25.5	Schutzmaßnahmen vor SQLi-Angriffen . . . . .	956
25.6	Zusammenfassung und Prüfungstipps . . . . .	957
25.6.1	Zusammenfassung und Weiterführendes . . . . .	957
25.6.2	CEH-Prüfungstipps . . . . .	957
25.6.3	Fragen zur CEH-Prüfungsvorbereitung . . . . .	958
<b>26</b>	<b>Web-Hacking – sonstige Injection-Angriffe . . . . .</b>	<b>961</b>
26.1	Command-Injection . . . . .	961
26.1.1	Einführung in Command-Injection-Angriffe . . . . .	962
26.1.2	Command-Injection in der Praxis . . . . .	962

26.1.3	Schutzmaßnahmen vor Command-Injection-Angriffen . . . . .	964
26.2	File-Injection . . . . .	965
26.2.1	Directory-Traversal-Angriffe . . . . .	965
26.2.2	File-Upload-Angriffe . . . . .	967
26.2.3	Local File Inclusion versus Remote File Inclusion . . . . .	970
26.3	Zusammenfassung und Prüfungstipps . . . . .	973
26.3.1	Zusammenfassung und Weiterführendes . . . . .	973
26.3.2	CEH-Prüfungstipps . . . . .	973
26.3.3	Fragen zur CEH-Prüfungsvorbereitung . . . . .	974
<b>27</b>	<b>Buffer-Overflow-Angriffe . . . . .</b>	<b>977</b>
27.1	Wie funktioniert ein Buffer-Overflow-Angriff? . . . . .	978
27.1.1	Das Grundprinzip . . . . .	978
27.1.2	Welche Anwendungen sind verwundbar? . . . . .	978
27.1.3	Funktionsweise des Stacks . . . . .	979
27.1.4	Register . . . . .	980
27.2	Ein Buffer-Overflow-Angriff in der Praxis . . . . .	981
27.2.1	SLmail-Exploit . . . . .	981
27.2.2	Die Laborumgebung . . . . .	981
27.2.3	Der Immunity Debugger . . . . .	984
27.2.4	Fuzzing . . . . .	986
27.2.5	Einen eindeutigen String erstellen . . . . .	990
27.2.6	Den EIP lokalisieren . . . . .	992
27.2.7	Den Shellcode platzieren . . . . .	992
27.2.8	Bad Characters identifizieren . . . . .	994
27.2.9	Grundüberlegung: Wohin soll der EIP zeigen? . . . . .	996
27.2.10	Mona und die Module . . . . .	996
27.2.11	Die Anweisung JMP ESP auffinden . . . . .	997
27.2.12	Den Programmablauf über den EIP steuern . . . . .	999
27.2.13	Den Shellcode erstellen und ausführen . . . . .	1001
27.3	Heap-Overflow-Angriffe . . . . .	1005
27.3.1	Der Heap . . . . .	1005
27.3.2	Heap Overflow versus Stack Overflow . . . . .	1006
27.3.3	Use-after-free . . . . .	1006
27.3.4	Heap Spraying . . . . .	1006
27.4	Schutzmaßnahmen gegen Buffer-Overflow-Angriffe . . . . .	1007
27.4.1	Address Space Layout Randomization (ASLR) . . . . .	1007
27.4.2	Data Execution Prevention (DEP) . . . . .	1008
27.4.3	SEHOP und SafeSEH . . . . .	1008
27.4.4	Stack Canary . . . . .	1008
27.4.5	Wie sicher sind die Schutzmaßnahmen? . . . . .	1009
27.5	Zusammenfassung und Prüfungstipps . . . . .	1010
27.5.1	Zusammenfassung und Weiterführendes . . . . .	1010
27.5.2	CEH-Prüfungstipps . . . . .	1011
27.5.3	Fragen zur CEH-Prüfungsvorbereitung . . . . .	1011

<b>Teil VI</b>	<b>Angriffe auf WLAN und Next-Gen-Technologien</b>	<b>1013</b>
<b>28</b>	<b>WLAN-Hacking</b>	<b>1017</b>
28.1	WLAN-Grundlagen	1017
28.1.1	Frequenzen und Kanäle	1018
28.1.2	Der IEEE-802.11-Standard	1019
28.1.3	Infrastruktur	1020
28.1.4	Verbindungsaufbau	1023
28.1.5	Verschlüsselungsmethoden	1026
28.2	Setup für das WLAN-Hacking	1029
28.2.1	Die WLAN-Hacking-Plattform	1029
28.2.2	Der richtige WLAN-Adapter	1030
28.2.3	Den Monitor Mode aktivieren	1031
28.3	WLAN-Scanning und -Sniffing	1032
28.3.1	Scanning	1033
28.3.2	WLAN-Sniffing	1033
28.3.3	Hidden SSIDs aufspüren	1035
28.4	Angriffe auf WLAN	1037
28.4.1	Denial of Service durch Störsender	1037
28.4.2	Deauthentication-Angriff	1037
28.4.3	Angriff auf WEP	1039
28.4.4	Angriff auf WPA/WPA2	1043
28.4.5	Angriff auf WPA3	1045
28.4.6	Angriff auf WPS	1046
28.4.7	MAC-Filter umgehen	1049
28.4.8	WLAN-Passwörter auslesen	1052
28.4.9	Standard-Passwörter	1054
28.4.10	Captive Portals umgehen	1055
28.5	Rogue Access Points	1057
28.5.1	Fake-Access-Point bereitstellen	1057
28.5.2	WLAN-Phishing	1060
28.6	Schutzmaßnahmen	1062
28.6.1	Allgemeine Maßnahmen	1062
28.6.2	Fortgeschrittene Sicherheitsmechanismen	1063
28.7	Zusammenfassung und Prüfungstipps	1064
28.7.1	Zusammenfassung und Weiterführendes	1064
28.7.2	CEH-Prüfungstipps	1065
28.7.3	Fragen zur CEH-Prüfungsvorbereitung	1065
<b>29</b>	<b>Mobile Hacking</b>	<b>1067</b>
29.1	Grundlagen	1067
29.1.1	Mobile Betriebssysteme	1067
29.1.2	Apps und App-Stores	1069
29.2	Angriffe auf mobile Geräte	1071
29.2.1	Schutzziele	1071

29.2.2	Angriffsvektoren	1072
29.2.3	OWASP Mobile Top 10	1074
29.3	Mobile Hacking in der Praxis	1075
29.3.1	Android über den PC	1075
29.3.2	Android-Rooting	1079
29.3.3	Jailbreaking iOS	1084
29.3.4	SIM-Unlock	1085
29.3.5	Hacking-Tools für Android	1086
29.3.6	Android-Tojaner erstellen	1088
29.3.7	Angriffe auf iOS	1093
29.3.8	Spyware für mobile Geräte	1094
29.4	Bring Your Own Device (BYOD)	1095
29.4.1	BYOD-Vorteile	1095
29.4.2	BYOD-Risiken	1095
29.4.3	BYOD-Sicherheit	1096
29.5	Mobile Device Management (MDM)	1097
29.6	Schutzmaßnahmen	1098
29.7	Zusammenfassung und Prüfungstipps	1100
29.7.1	Zusammenfassung und Weiterführendes	1100
29.7.2	CEH-Prüfungstipps	1101
29.7.3	Fragen zur CEH-Prüfungsvorbereitung	1102
<b>30</b>	<b>IoT- und OT-Hacking und -Security</b>	<b>1105</b>
30.1	Das Internet of Things	1105
30.1.1	Was ist das Internet of Things?	1106
30.1.2	Was umfasst das Internet of Things?	1106
30.1.3	Die grundlegende Sicherheitsproblematik von IoT-Geräten	1107
30.2	IoT-Technik – Konzepte und Protokolle	1107
30.2.1	IoT-Betriebssysteme	1108
30.2.2	IoT-Kommunikationsmodelle	1108
30.2.3	IoT-Übertragungstechnologien	1110
30.2.4	IoT-Kommunikationsprotokolle	1112
30.3	Schwachstellen von IoT-Systemen	1113
30.3.1	OWASP Top 10 IoT 2018	1113
30.3.2	Angriffsvektoren auf IoT-Systeme	1116
30.4	IoT-Angriffsszenarien	1118
30.4.1	Rolling-Code-Angriff	1118
30.4.2	Mirai – Botnet und DDoS-Angriffe	1120
30.4.3	Lokale Angriffe über die UART-Schnittstelle	1121
30.4.4	Command-Injection via Web-Frontend	1122
30.4.5	Der BlueBorne-Angriff	1123
30.4.6	Angriffe auf ZigBee-Geräte mit Killerbee	1124
30.4.7	Angriffe auf Firmware	1125
30.5	Weitere Angriffsformen auf IoT-Ökosysteme	1126
30.5.1	Exploit Kits	1126

	30.5.2	IoT-Suchmaschinen	1126
30.6		OT-Hacking	1128
	30.6.1	OT-Grundlagen und -Konzepte	1128
	30.6.2	Konvergenz von IT und OT	1129
	30.6.3	Das Purdue-Modell	1130
	30.6.4	OT-Sicherheitsherausforderungen	1131
	30.6.5	OT-Schwachstellen und Bedrohungen	1132
	30.6.6	OT-Malware	1133
	30.6.7	OT-Hackingtools und -Enumeration	1134
	30.6.8	Schutzmaßnahmen vor OT-Angriffen	1135
30.7		Schutzmaßnahmen vor IoT-Angriffen	1136
30.8		Zusammenfassung und Prüfungstipps	1138
	30.8.1	Zusammenfassung und Weiterführendes	1138
	30.8.2	CEH-Prüfungstipps	1138
	30.8.3	Fragen zur CEH-Prüfungsvorbereitung	1138
<b>31</b>		<b>Angriffe auf die Cloud</b>	<b>1141</b>
31.1		Grundlagen des Cloud Computings	1141
	31.1.1	Was ist eigentlich »die Cloud?«	1142
	31.1.2	Cloud-Service-Modelle	1143
	31.1.3	Deployment-Modelle für die Cloud	1144
	31.1.4	Besondere Computing-Varianten	1146
	31.1.5	Große Cloud-Anbieter	1147
31.2		Wichtige Cloud-Technologien	1148
	31.2.1	Virtualisierung	1148
	31.2.2	Container-Technologien	1149
	31.2.3	Docker	1152
	31.2.4	Kubernetes	1154
	31.2.5	Schwachstellen von Container-Technologien	1155
	31.2.6	Serverless Computing	1156
	31.2.7	Schwachstellen von Serverless Computing	1157
	31.2.8	Weitere Cloud-Dienstleistungen	1158
31.3		Bedrohungen der Sicherheit und Integrität in der Cloud	1158
	31.3.1	Kontrollverlust	1158
	31.3.2	Unsichere Cloud-Infrastruktur	1159
	31.3.3	Missbrauchs-Risiken beim Cloud-Anbieter	1160
	31.3.4	Unsichere Kommunikation mit der Cloud	1161
	31.3.5	Unzureichende Zugangskontrolle	1163
	31.3.6	Cloud Computing für Hacker	1163
	31.3.7	Übersicht und Zusammenfassung	1164
31.4		Angriffe auf Cloud-Infrastrukturen	1164
	31.4.1	Zugangsdaten ermitteln	1164
	31.4.2	Persistenter Zugang sichern	1165
	31.4.3	Malware einschleusen	1166
	31.4.4	Unsichere Voreinstellungen ausnutzen	1166



31.4.5	Cryptojacking . . . . .	1167
31.4.6	Zugang über Federation Services . . . . .	1167
31.4.7	Angriffsvektor Webanwendung . . . . .	1168
31.5	Cloud-Security-Tools . . . . .	1169
31.5.1	Security-Tools des Cloud-Anbieters . . . . .	1169
31.5.2	Drittanbieter-Security-Software . . . . .	1169
31.5.3	Pentest-Simulation mit CloudGoat und Pacu . . . . .	1170
31.6	Zusammenfassung und Prüfungstipps . . . . .	1171
31.6.1	Zusammenfassung und Weiterführendes . . . . .	1171
31.6.2	CEH-Prüfungstipps . . . . .	1172
31.6.3	Fragen zur CEH-Prüfungsvorbereitung . . . . .	1173
<b>32</b>	<b>Durchführen von Penetrationstests . . . . .</b>	<b>1175</b>
32.1	Begriffsbestimmung Penetrationstest . . . . .	1175
32.1.1	Was bedeutet »Penetrationstest« eigentlich? . . . . .	1176
32.1.2	Wozu einen Penetrationstest durchführen? . . . . .	1176
32.1.3	Penetrationstest vs. Security Audit vs. Vulnerability Assessment . . . . .	1177
32.1.4	Arten des Penetrationstests . . . . .	1178
32.2	Rechtliche Bestimmungen . . . . .	1179
32.2.1	In Deutschland geltendes Recht . . . . .	1180
32.2.2	US-amerikanisches und internationales Recht . . . . .	1181
32.3	Vorbereitung und praktische Durchführung des Penetrationstests . . . . .	1183
32.3.1	Die Beauftragung . . . . .	1183
32.3.2	Methodik der Durchführung . . . . .	1185
32.3.3	Praxistipps . . . . .	1188
32.4	Der Pentest-Report . . . . .	1191
32.4.1	Dokumentation während des Pentests . . . . .	1191
32.4.2	Was umfasst der Pentest-Report? . . . . .	1192
32.4.3	Aufbau des Pentest-Reports . . . . .	1193
32.5	Abschluss und Weiterführendes . . . . .	1195
32.5.1	Das Abschluss-Meeting . . . . .	1196
32.5.2	Weiterführende Tätigkeiten . . . . .	1196
32.6	Zusammenfassung und Prüfungstipps . . . . .	1196
32.6.1	Zusammenfassung und Weiterführendes . . . . .	1196
32.6.2	CEH-Prüfungstipps . . . . .	1197
32.6.3	Fragen zur CEH-Prüfungsvorbereitung . . . . .	1198
<b>A</b>	<b>Lösungen . . . . .</b>	<b>1201</b>
	<b>Stichwortverzeichnis . . . . .</b>	<b>1215</b>