

Auf einen Blick

1	Einleitung	17
TEIL I IT-Sicherheitspenetrationstests durchführen		25
2	IT-Sicherheitspenetrationstests	27
3	Red Teaming als Methode	51
4	Testszenarien in der Praxis	63
TEIL II Awareness-Schulungen mit Pentest-Hardware		105
5	Security-Awareness-Schulungen	107
6	Erfolgreiche Schulungsmethoden	115
7	Schulungsszenarien in der Praxis	125
TEIL III Hacking- & Pentest-Hardware-Tools		141
8	Pentest-Hardware-Tools	143
9	Heimliche Überwachung durch Spionage-Gadgets	169
10	Tastatureingaben und Monitorsignale mit Loggern aufzeichnen	189
11	Angriffe über die USB-Schnittstelle	223
12	Manipulation von Funkverbindungen	331
13	RFID-Tags duplizieren und manipulieren	365
14	Bluetooth-Kommunikation tracken und manipulieren	405
15	WLAN-Verbindungen manipulieren und unterbrechen	425
16	Kabelgebundene LAN-Netzwerke ausspionieren	467
17	Analyse gefundener Hardware	519

Inhalt

Geleitwort	15
------------------	----

1 Einleitung 17

1.1 An wen richtet sich dieses Buch?	18
1.2 Was wird in diesem Buch vermittelt?	19
1.3 Wie ist dieses Buch aufgebaut?	19
1.4 Über den Autor	23
1.5 Materialien zum Buch	24

TEIL I IT-Sicherheitspenetrationstests durchführen

2 IT-Sicherheitspenetrationstests 27

2.1 Einstieg: Was sind Pentests?	28
2.1.1 Vorteile von Penetrationstests	28
2.1.2 Die Grenzen von IT-Sicherheitstests	29
2.1.3 Zielsetzungen von Penetrationstests	30
2.1.4 Bedrohungen und Angriffe	32
2.2 Eigenschaften von Penetrationstests	37
2.2.1 Ausrichtung	38
2.2.2 Vorgehensweise	39
2.2.3 Organisation	40
2.2.4 Ethical Hacking	41
2.3 Ablauf von Penetrationstests	42
2.3.1 1. Phase: Pre-Engagement (Vorbereitung)	43
2.3.2 2. Phase: Reconnaissance (Informationsbeschaffung)	44
2.3.3 3. Phase: Threat Modeling (Angriffsszenarien)	44
2.3.4 4. Phase: Exploitation (aktive Eindringversuche)	45
2.3.5 5. Phase: Reporting (Abschlussanalyse)	45
2.3.6 6. Phase: Re-Testing (erneutes Testen)	46

2.4	Bewertung von Schwachstellen	46
2.5	Behebung von Schwachstellen	50

3 Red Teaming als Methode 51

3.1	Red Teaming erfolgreich einsetzen	53
3.1.1	Ziele definieren	53
3.1.2	Leitfäden und Vorgaben für Red Teaming	55
3.1.3	Vorteile des Red Teamings	56
3.2	Ablauf des Red Teamings	57
3.2.1	Voraussetzungen	57
3.2.2	Phasen des Red Teamings	58
3.3	Die Variante »Purple Team«	60

4 Testszzenarien in der Praxis 63

4.1	Szenario A: WLAN-Überwachungskamera testen	64
4.1.1	Pre-Engagement (Vorbereitung)	66
4.1.2	Reconnaissance (Informationsbeschaffung)	66
4.1.3	Threat Modeling (Angriffsszenarien)	68
4.1.4	Exploitation (aktive Eindringversuche)	70
4.1.5	Reporting (Abschlussanalyse)	76
4.1.6	Re-Testing (erneutes Testen)	76
4.2	Szenario B: RFID-Zugangskarten für ein Schließsystem untersuchen	77
4.2.1	Pre-Engagement (Vorbereitung)	78
4.2.2	Reconnaissance (Informationsbeschaffung)	79
4.2.3	Threat Modeling (Angriffsszenarien)	81
4.2.4	Exploitation (aktive Eindringversuche)	83
4.2.5	Reporting (Abschlussanalyse)	85
4.2.6	Re-Testing (erneutes Testen)	85
4.3	Szenario C: Netzwerkverbindungen eines Druckers überprüfen	86
4.3.1	Pre-Engagement (Vorbereitung)	86
4.3.2	Reconnaissance (Informationsbeschaffung)	87
4.3.3	Threat Modeling (Angriffsszenarien)	89
4.3.4	Exploitation (aktive Eindringversuche)	90

4.3.5	Reporting (Abschlussanalyse)	92
4.3.6	Re-Testing (erneutes Testen)	93
4.4	Szenario D: Die Schnittstellen eines Client-Rechners analysieren	93
4.4.1	Pre-Engagement (Vorbereitung)	94
4.4.2	Reconnaissance (Informationsbeschaffung)	95
4.4.3	Threat Modeling (Angriffsszenarien)	96
4.4.4	Exploitation (aktive Eindringversuche)	98
4.4.5	Reporting (Abschlussanalyse)	102
4.4.6	Re-Testing (erneutes Testen)	103

TEIL II Awareness-Schulungen mit Pentest-Hardware

5 Security-Awareness-Schulungen 107

5.1	Social Engineering	108
5.2	Verschiedene Schulungsarten	109
5.3	Security-Awareness-Trainings mit Pentest-Hardware	111
5.3.1	Zielsetzung	111
5.3.2	Planung	112
5.3.3	Ausführung	112
5.3.4	Auswertung	113

6 Erfolgreiche Schulungsmethoden 115

6.1	Interesse wecken	116
6.1.1	Bezug	116
6.1.2	Storytelling	117
6.1.3	Visualisierung	118
6.2	Motivation fördern	118
6.2.1	Praxisbeispiele	119
6.2.2	Live Hacking	119
6.3	Aktivierung steuern	119
6.3.1	Quiz	120
6.3.2	Blitzlicht-Methode	120
6.3.3	Fachbezogenes Kurzgespräch	121
6.3.4	Gruppenpuzzle	121

6.4	Interaktion anregen	122
6.4.1	Learning by doing	122
6.4.2	Gruppenarbeit	123
6.4.3	Gamification	124

7 Schulungsszenarien in der Praxis 125

7.1	Szenario A: Verseuchter Arbeitsplatz	126
7.1.1	Vorbereitung	126
7.1.2	Durchführung	128
7.2	Szenario B: Hardware-Schnitzeljagd	129
7.2.1	Vorbereitung	129
7.2.2	Durchführung	131
7.3	Szenario C: USB-Sticks im öffentlichen Bereich	132
7.3.1	Vorbereitungen	132
7.3.2	Durchführung	139

TEIL III Hacking- & Pentest-Hardware-Tools

8 Pentest-Hardware-Tools 143

8.1	Überblick über die Hardware	144
8.1.1	Spionage-Gadgets	144
8.1.2	Logger	145
8.1.3	USB	146
8.1.4	Funk	146
8.1.5	RFID	147
8.1.6	Bluetooth	148
8.1.7	WLAN	149
8.1.8	Netzwerk	149
8.2	Rechtliche Aspekte	150
8.3	Bezugsquellen	152
8.3.1	Internationale Shops	152
8.3.2	Shops in der Europäischen Union	153
8.3.3	Shops in Deutschland	153

8.4	Laborumgebung	154
8.4.1	VirtualBox	154
8.4.2	Kali Linux	156
8.4.3	Windows 10	160
8.4.4	Cloud C ² von Hak5	164

9 Heimliche Überwachung durch Spionage-Gadgets 169

9.1	Angriffsszenario	170
9.2	Mini-Aufnahmegeräte – geheime Audioaufzeichnungen	173
9.3	GSM-Aufnahmegerät – weltweite Audioübertragungen	176
9.4	Spionagekameras – unbemerkte Videoaufnahmen	179
9.5	WLAN-Minikameras – vielfältige Kameramodule	180
9.6	GPS-Tracker – Position heimlich tracken und übermitteln	182
9.7	Gegenmaßnahmen	184
9.7.1	Audio-Spionage-Gadgets	184
9.7.2	Video-Spionage-Gadgets	185
9.7.3	Funkverbindungen	186
9.8	Analyse von gefundenen Geräten	187

10 Tastatureingaben und Monitorsignale mit Loggern aufzeichnen 189

10.1	Angriffsszenario	190
10.2	Keylogger – Unauffällige Tastaturüberwachung	193
10.2.1	USB-Keylogger	193
10.2.2	Keylogger mit WLAN	197
10.2.3	EvilCrow Keylogger – flexible Plattform	201
10.3	Screenlogger – heimliche Bildschirmüberwachung	207
10.3.1	VideoGhost – heimliche Screenshots	208
10.3.2	Screen Crab – Screenlogger per WLAN	211
10.4	Gegenmaßnahmen	220
10.4.1	Keylogger	220

10.4.2	Screenlogger	221
10.5	Analyse von gefundenen Geräten	221
11	Angriffe über die USB-Schnittstelle	223
<hr/>		
11.1	Angriffsszenario	225
11.2	BadUSB-Hardware	228
11.2.1	Rubber Ducky – der BadUSB-Klassiker	228
11.2.2	Digispark – ein günstiges BadUSB-Device	235
11.2.3	Teensy – ein universelles Board	248
11.2.4	MalDuino – BadUSB mit Schalter	257
11.2.5	Arduino Leonardo – BadUSB mit Arduino	265
11.2.6	EvilCrow-Cable – getarnter BadUSB	270
11.3	Steuerung per Bluetooth oder WLAN	273
11.3.1	InputStick – drahtloser Bluetooth-Empfänger	273
11.3.2	USBNinja – Bluetooth-Steuerung	278
11.3.3	Cactus WHID – BadUSB mit WLAN	285
11.3.4	DSTIKE WIFI Duck – WLAN-Keystroke-Injection	292
11.4	USB-Geräte simulieren	297
11.4.1	Bash Bunny – das BadUSB-Multitool	297
11.4.2	Signal Owl – eine universelle Plattform	302
11.4.3	Key Croc – ein smarterer Keylogger	306
11.4.4	P4wnP1 A.L.O.A. – das BadUSB-Supertool	319
11.5	Rechner mit USB-Killern zerstören	322
11.5.1	USBKill – Geräte irreparabel schädigen	323
11.5.2	Alternative Killer	325
11.6	Gegenmaßnahmen	326
11.6.1	Softwarelösungen	326
11.6.2	Hardwarelösungen	328
11.7	Analyse von gefundenen Geräten	330
12	Manipulation von Funkverbindungen	331
<hr/>		
12.1	Angriffsszenario	332
12.2	Frequenzen und Antennen	334

12.3	Funk-Cloner – Funkverbindungen duplizieren	337
12.4	NooElec NESDR SMARt – Funkverbindungen analysieren	338
12.4.1	Einrichtung	339
12.4.2	Anwendung	341
12.5	HackRF One – Funkkommunikation einfach duplizieren	345
12.5.1	Einrichtung	346
12.5.2	Anwendung	348
12.5.3	Mobile Version	350
12.6	LimeSDR Mini – Funkverbindungen angreifen	351
12.6.1	Einrichtung	352
12.7	YARD Stick One – Funksignale manipulieren	354
12.7.1	Einrichtung	355
12.7.2	Anwendung	357
12.8	Crazyradio PA – Übernahme von Funkverbindungen	359
12.8.1	Einrichtung	360
12.8.2	Anwendung	361
12.9	Störsender – Funkverbindungen unterbrechen	362
12.10	Gegenmaßnahmen	364
12.11	Analyse von gefundenen Geräten	364

13 RFID-Tags duplizieren und manipulieren 365

13.1	Angriffsszenario	368
13.2	Detektoren – RFID-Reader und -Tags aufspüren	371
13.2.1	RFID Diagnostic Card	371
13.2.2	RF Field Detector	372
13.2.3	Tiny RFID Detector	373
13.2.4	Weitere Lösungen	373
13.3	Cloner – RFID-Tags einfach kopieren	374
13.3.1	Handheld RFID Writer	375
13.3.2	CR66 Handheld RFID	376
13.3.3	Handheld RFID IC/ID	377
13.3.4	RFID Multi Frequenz Replikator	378
13.4	Keysy – ein universeller RFID-Schlüssel	379

13.5 ChameleonMini/Tiny – ein RFID-Multitool	380
13.5.1 Varianten	382
13.5.2 Einrichtung	383
13.5.3 Anwendung	384
13.6 Proxmark – eine leistungsstarke RFID-Hardware	386
13.6.1 Einrichtung	388
13.6.2 Anwendung	390
13.6.3 Portable Variante	394
13.7 iCopy-X – ein weiteres RFID-Multitool	396
13.7.1 Einrichtung	397
13.7.2 Anwendung	397
13.8 NFCKill – RFID/NFC-Tags zerstören	399
13.8.1 Anwendung	401
13.8.2 Der RFID-Zapper des CCC	401
13.9 Gegenmaßnahmen	402
13.10 Analyse von gefundenen Geräten	403

14 Bluetooth-Kommunikation tracken und manipulieren 405

14.1 Angriffsszenario	406
14.2 Bluefruit LE Sniffer – Bluetooth Low Energy tracken	408
14.2.1 Einrichtung	409
14.2.2 Anwendung	409
14.3 BtleJack mit BBC micro:bit – Bluetooth-LE-Verbindungen abhören	412
14.3.1 Einrichtung	413
14.3.2 Anwendung	414
14.4 Ubertooth One – Bluetooth-Verbindungen analysieren	418
14.4.1 Einrichtung	419
14.4.2 Anwendung	421
14.5 Gegenmaßnahmen	423
14.6 Analyse von gefundenen Geräten	423

15 WLAN-Verbindungen manipulieren und unterbrechen

425

15.1	Angriffsszenario	426
15.2	DSTIKE Deauther – WLAN-Verbindungen unterbrechen	428
15.2.1	Varianten	429
15.2.2	Einrichtung	432
15.2.3	Anwendung	435
15.3	Maltronics WiFi Deauther – ferngesteuerter Angriff	436
15.3.1	Einrichtung	437
15.3.2	Anwendung	437
15.4	WiFi Pineapple – WLAN-Netzwerke fälschen	442
15.4.1	Varianten	443
15.4.2	Einrichtung	444
15.4.3	Anwendung	451
15.4.4	Cloud C ²	458
15.5	Gegenmaßnahmen	462
15.6	Analyse von gefundenen Geräten	465

16 Kabelgebundene LAN-Netzwerke ausspionieren

467

16.1	Angriffsszenario	468
16.2	Throwing Star LAN Tap – Daten einfach ausleiten	470
16.2.1	Anwendung	472
16.3	Plunder Bug – Daten elegant ausleiten	474
16.3.1	Einrichtung	475
16.3.2	Anwendung	477
16.4	Packet Squirrel – Netzwerkverkehr mitschneiden	479
16.4.1	Einrichtung	481
16.4.2	Anwendung	482
16.5	Shark Jack – vorab definierte Aktionen ausführen	495
16.5.1	Einrichtung	496
16.5.2	Anwendung	498
16.6	LAN Turtle – heimlicher Netzwerkzugang	502
16.6.1	Einrichtung	504
16.6.2	Anwendung	508

16.7	Gegenmaßnahmen	515
16.8	Analyse von gefundenen Geräten	517
17	Analyse gefundener Hardware	519
<hr/>		
17.1	Dokumentation	520
17.2	Geräte mit Datenspeicher	521
17.2.1	Schutz vor Veränderung (Write-Blocker)	521
17.2.2	Eine 1:1-Kopie gefundener Hardware erstellen	524
17.2.3	Untersuchung des Dateisystems und der Dateien	525
17.2.4	Gelöschte Daten wiederherstellen	530
17.3	Netzwerkverkehr protokollieren	532
17.4	WLAN-Netzwerke aufspüren und analysieren	536
17.4.1	Analyse via Hardware – WiFi Pineapple	536
17.4.2	Analyse per Software – Aircrack-ng	537
17.5	Fazit	541
	Index	543