

Inhalt

Vorwort	13
Grußwort	18

TEIL I Einführung und Tools

1 Einführung	21
1.1 Hacking	21
1.2 Sicherheit	29
1.3 Exploits	42
1.4 Authentifizierung und Passwörter	49
1.5 Sicherheitsrisiko IPv6	55
1.6 Gesetzliche Rahmenbedingungen	57
1.7 Security-Organisationen und staatliche Einrichtungen	60
2 Kali Linux	63
2.1 Kali Linux ohne Installation ausprobieren	64
2.2 Kali Linux in VirtualBox installieren	72
2.3 Kali Linux und Hyper-V	81
2.4 Kali Linux im Windows-Subsystem für Linux	83
2.5 Kali Linux auf dem Raspberry Pi	85
2.6 Kali-Interna	87
2.7 Einfache Anwendungsbeispiele	91
2.8 PentestBox	94
3 Lernumgebung einrichten (Metasploitable, Juice Shop)	97
3.1 Metasploitable 2	98
3.2 Metasploitable 3	104
3.3 Juice Shop	121

4	Hacking-Tools	125
4.1	nmap	126
4.2	hydra	130
4.3	nikto	136
4.4	sslyze, sslscan und testssl	139
4.5	whois, host und dig	143
4.6	Wireshark	145
4.7	tcpdump	152
4.8	Netcat (nc)	155
4.9	SPARTA	158
4.10	OpenVAS	160
4.11	Metasploit Framework	170
4.12	Armitage	184
4.13	Empire Framework	186
4.14	Das Post-Exploitation-Framework Koadic	195
4.15	Social-Engineer Toolkit (SET)	204
4.16	Burp Suite	211

TEIL II Hacking und Absicherung

5	Offline Hacking	221
5.1	BIOS/EFI-Grundlagen	221
5.2	Auf fremde Systeme zugreifen	224
5.3	Auf externe Festplatten oder SSDs zugreifen	231
5.4	Windows-Passwort zurücksetzen	232
5.5	Linux- und macOS-Passwort zurücksetzen	239
5.6	Festplatten verschlüsseln	241
6	Passwörter	251
6.1	Hash-Verfahren	252
6.2	Brute-Force Password Cracking	255
6.3	Rainbow Tables	257
6.4	Wörterbuch-Attacken	258
6.5	Passwort-Tools	260
6.6	Default-Passwörter	269

6.7	Data Breaches	270
6.8	Multi-Faktor-Authentifizierung	272
6.9	Sicheres Passwort-Handling implementieren	273
7	WLAN, Bluetooth und SDR	277
7.1	802.11x-Systeme (WiFi)	277
7.2	WPA-2-Handshakes mit dem Pwnagotchi einsammeln	297
7.3	Bluetooth	303
7.4	Software-Defined Radios (SDR)	322
8	Angriffsvektor USB-Schnittstelle	331
8.1	USB-Rubber-Ducky	332
8.2	Digispark – ein Wolf im Schafspelz	341
8.3	Bash Bunny	350
8.4	P4wnP1 – Das Universaltalent	373
8.5	Gegenmaßnahmen	384
9	Externe Sicherheitsüberprüfungen	389
9.1	Gründe für professionelle Überprüfungen	389
9.2	Typen von Sicherheitsüberprüfungen	390
9.3	Rechtliche Absicherung	400
9.4	Zielsetzung und Abgrenzung	402
9.5	Methodologien zur Durchführung	403
9.6	Reporting	405
9.7	Auswahl des richtigen Anbieters	408
10	Client-Side Penetration-Testing	411
10.1	Open Source Intelligence (OSINT)	411
10.2	E-Mail-Phishing-Kampagnen für Unternehmen	431
10.3	Phishing-Angriffe mit .PDF.EXE-Dateien	440
10.4	Praxisbeispiel: Phishing-Angriffe mit Office-Makros	450
10.5	Angriffsvektor USB-Phishing	456
10.6	Man-in-the-Middle-Angriffe auf unverschlüsselte Verbindungen	457
10.7	Man-in-the-Middle-Angriff auf SSL/TLS-Verbindungen	464
10.8	Man-in-the-Middle-Angriffe auf Remotedesktop	469

10.9	Angriffe auf Netzwerk-Hashes	474
10.10	SMB-Relaying mit der Impacket-Library (Angriff auf Administratoren)	476
10.11	SMB-Relaying-Angriff auf normale Domänenbenutzer	480
11	Penetration-Testing in Netzwerken	483
11.1	Externe IP-Adressen der PTA überprüfen	483
11.2	Network Access Control (NAC) und 802.1X in lokalen Netzwerken	488
11.3	Scanning von interessanten Zielen	491
11.4	Suche nach bekannten Schwachstellen mit nmap	498
11.5	Bekannte Schwachstellen mit Metasploit ausnutzen	499
11.6	Angriff auf schwache Passwörter	505
11.7	Post-Exploitation von Systemen	508
12	Windows Server absichern	525
12.1	Lokale Benutzer, Gruppen und Rechte	526
12.2	Manipulationen am Dateisystem	536
12.3	Serverhärtung	541
12.4	Windows Defender	549
12.5	Windows-Firewall	552
12.6	Windows-Ereignisanzeige	556
13	Active Directory	567
13.1	Was ist das Active Directory?	567
13.2	Manipulation der Active-Directory-Datenbank bzw. ihrer Daten	581
13.3	Manipulation von Gruppenrichtlinien	585
13.4	Domänenauthentifizierung (Kerberos)	591
13.5	Angriffe gegen die Authentifizierungsprotokolle und LDAP	599
13.6	Pass-the-Hash-Angriffe (mimikatz)	601
13.7	Golden Ticket und Silver Ticket	614
13.8	Sensible Information aus der Active-Directory-Datenbank auslesen	618
13.9	Grundabsicherung	621
13.10	Mehr Sicherheit durch Tiers (Schichten)	625
13.11	Schutzmaßnahmen gegen Pass-the-Hash- und Pass-the-Ticket-Angriffe	630

14	Linux absichern	639
14.1	Installation	640
14.2	Software-Updates	644
14.3	Kernel-Updates (Live Patches)	649
14.4	SSH absichern	652
14.5	Google Authenticator	659
14.6	Fail2ban	666
14.7	Firewall	673
14.8	SELinux	684
14.9	AppArmor	690
14.10	Apache	695
14.11	MySQL und MariaDB	702
14.12	Postfix	711
14.13	Dovecot	717
14.14	Rootkit-Erkennung und Intrusion Detection	719
15	Sicherheit bei Samba-Fileservern	731
15.1	Vorüberlegungen	732
15.2	CentOS-Basisinstallation	733
15.3	Debian-Basisinstallation	737
15.4	Konfiguration des Samba-Servers	739
15.5	Samba-Server im Active Directory	743
15.6	Freigaben auf dem Samba-Server	747
15.7	Umstellung auf die Registry	752
15.8	Samba-Audit-Funktionen	756
15.9	Firewall	758
15.10	Angriffsszenarien auf Samba-Fileserver	763
15.11	Prüfen von Samba-Fileservern	766
16	Sicherheit von Webanwendungen	773
16.1	Architektur von Webapplikationen	773
16.2	Angriffe gegen Webanwendungen	777
16.3	Praktische Analyse einer Webanwendung	811
16.4	Schutzmechanismen und Abwehr von Webangriffen	833
16.5	Sicherheitsanalyse von Webanwendungen	842

- 17 Software-Exploitation** 845
- 17.1 Schwachstellen von Software 845
- 17.2 Aufdecken von Sicherheitslücken 848
- 17.3 Programmausführung auf x86-Systemen 849
- 17.4 Ausnutzung von Buffer-Overflows 859
- 17.5 Structured Exception Handling (SEH) 875
- 17.6 Heap Spraying 877
- 17.7 Schutzmechanismen gegen Buffer-Overflows 879
- 17.8 Schutzmaßnahmen gegen Buffer-Overflows umgehen 883
- 17.9 Buffer-Overflows als Entwickler verhindern 890
- 17.10 Spectre und Meltdown 891

TEIL III Cloud, Smartphones, IoT

- 18 Sicherheit in der Cloud** 901
- 18.1 Überblick 902
- 18.2 Amazon S3 905
- 18.3 Nextcloud/ownCloud 914

- 19 Office 365 absichern** 925
- 19.1 Identitäten und Zugriffsverwaltung 926
- 19.2 Secure Score 935
- 19.3 Mehrstufige Authentifizierung 937
- 19.4 Bedingter Zugriff 943
- 19.5 Identity Protection 951
- 19.6 Office 365 Cloud App Security 953
- 19.7 Privileged Identities 957
- 19.8 Viren- und Spamschutz im E-Mail-Verkehr 964
- 19.9 Schadcode-Erkennung in E-Mails mit Office 365 ATP 972
- 19.10 Sicherheit in den Rechenzentren 981

- 20 Mobile Security** 987
- 20.1 Sicherheitsgrundlagen von Android und iOS 987
- 20.2 Bedrohungen von mobilen Endgeräten 995

20.3	Malware und Exploits	1006
20.4	Technische Analyse von Apps	1017
20.5	Schutzmaßnahmen für Android und iOS	1027
20.6	Apple Supervised Mode und Apple Configurator	1042
20.7	Enterprise Mobility Management	1049
21	IoT-Sicherheit	1059
21.1	Was ist das Internet der Dinge?	1059
21.2	IoT-Schwachstellen finden	1061
21.3	Absicherung von IoT-Geräten in Netzwerken	1078
21.4	IoT-Protokolle und -Dienste	1080
21.5	IoT-Funktechniken	1092
21.6	IoT aus Entwicklersicht	1098
21.7	Programmiersprachen für Embedded Controller	1103
21.8	Regeln für die sichere IoT-Programmierung	1106
	Die Autoren	1117
	Index	1119