

Hacking & Security

Das umfassende Handbuch

DAS INHALTS- VERZEICHNIS

» Hier geht's
direkt
zum Buch

Auf einen Blick

TEIL I

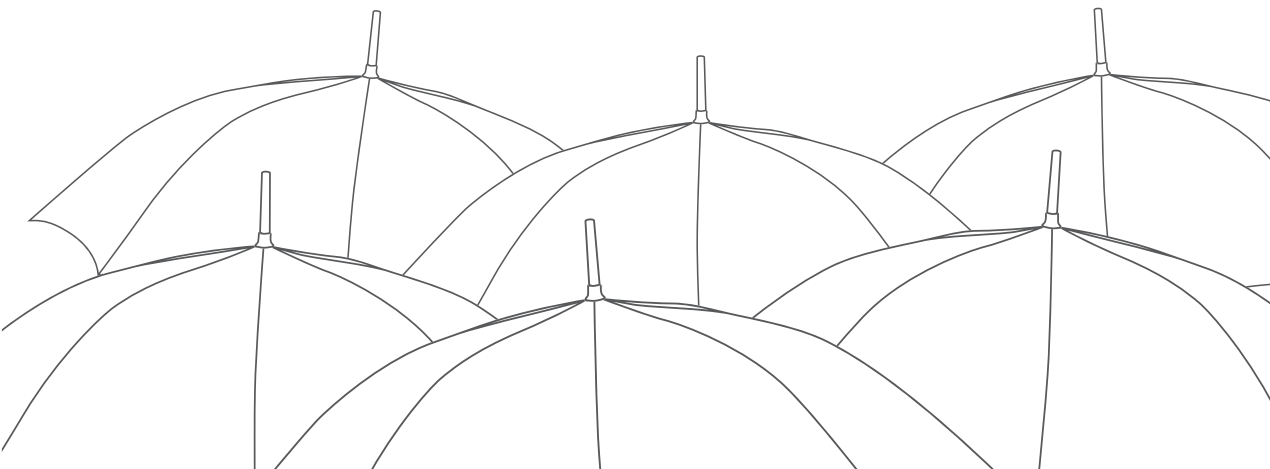
Einführung und Tools 19

TEIL II

Hacking und Absicherung 243

TEIL III

Cloud, Smartphones, IoT 1039



Inhaltsverzeichnis

Vorwort	13
---------------	----

TEIL I Einführung und Tools

1 Einführung	21
---------------------	-----------

1.1 Hacking	21
1.2 Sicherheit	31
1.3 Exploits	47
1.4 Authentifizierung und Passwörter	55
1.5 Künstliche Intelligenz	61
1.6 Sicherheitsrisiko IPv6	63
1.7 Gesetzliche Rahmenbedingungen	65
1.8 Security-Organisationen und staatliche Einrichtungen	68

2 Kali Linux	71
---------------------	-----------

2.1 Kali Linux ausprobieren	72
2.2 Kali Linux mit VirtualBox ausführen	75
2.3 Kali Linux installieren	77
2.4 Kali Linux im Windows-Subsystem für Linux	80
2.5 Kali Linux mit UTM ausführen	83
2.6 Kali Linux auf dem Raspberry Pi	85
2.7 Kali-Download verifizieren	86
2.8 Konfiguration und Kali-Interna	88
2.9 Einfache Anwendungsbeispiele	94

3 Hacking-Tools	99
------------------------	-----------

3.1 nmap	100
3.2 hydra	106
3.3 sslyze, sslscan und testssl	111

3.4	whois, host und dig	115
3.5	Wireshark	117
3.6	tcpdump	124
3.7	Netcat (nc)	127
3.8	OpenVAS	130
3.9	Metasploit Framework	142
3.10	Empire Framework	157
3.11	Das Post-Exploitation-Framework Koadic	167
3.12	Social-Engineer Toolkit (SET)	176
3.13	Burp Suite	183
3.14	Sliver	190

4 Hacking lernen 197

4.1	Übungsumgebung einrichten	199
4.2	Basic Pentesting 1 und 2	205
4.3	Mr. Robot und Necromancer	218
4.4	Metasploitable	223
4.5	pwn.college	225
4.6	Juice Shop	228

5 Bug-Bounty-Programme 233

5.1	Die Idee hinter Bug Bounties	233
5.2	Reporting von Schwachstellen	236
5.3	Tipps & Tricks für Analysten	238
5.4	Tipps für Unternehmen	241

TEIL II Hacking und Absicherung

6 Offline Hacking 245

6.1	BIOS/EFI-Grundlagen	247
6.2	Auf fremde Systeme zugreifen	249
6.3	Windows-Passwort zurücksetzen	254
6.4	Linux-Passwort zurücksetzen	261
6.5	Datenträger verschlüsseln	262

7	Passwörter	269
7.1	Hash-Verfahren	270
7.2	Brute-Force Password Cracking	273
7.3	Rainbow Tables	275
7.4	Wörterbuch-Attacken	277
7.5	Passworttools	278
7.6	Default-Passwörter	287
7.7	Data Breaches	288
7.8	Multi-Faktor-Authentifizierung	291
7.9	Sicheres Passwort-Handling implementieren	292
7.10	Passwortlose Anmeldung mit FIDO2	294
8	IT-Forensik	299
8.1	Methodische Analyse von Vorfällen	301
8.2	Post-Mortem-Untersuchung	306
8.3	Live-Analyse	321
8.4	Forensic Readiness	325
8.5	Zusammenfassung	328
9	WLAN, Bluetooth und SDR	329
9.1	802.11x-Systeme (WiFi)	329
9.2	WPA-2-Handshakes mit dem Pwnagotchi einsammeln	348
9.3	Bluetooth	355
9.4	Software-Defined Radios (SDR)	374
9.5	Wireless-Analysen mit dem Flipper Zero	383
10	Angriffsvektor USB-Schnittstelle	395
10.1	USB Rubber Ducky	396
10.2	Digispark – ein Wolf im Schafspelz	404
10.3	Bash Bunny	411
10.4	MalDuino W	434
10.5	Gegenmaßnahmen	441

11 Externe Sicherheitsüberprüfungen 447

11.1	Gründe für professionelle Überprüfungen	447
11.2	Typen von Sicherheitsüberprüfungen	448
11.3	Rechtliche Absicherung	462
11.4	Zielsetzung und Abgrenzung	464
11.5	Methodologien zur Durchführung	465
11.6	Reporting	467
11.7	Auswahl des richtigen Anbieters	470

12 Penetration-Testing 473

12.1	Informationssammlung	474
12.2	Initialer Zugriff mit Codeausführung	484
12.3	Scanning von interessanten Zielen	488
12.4	Suche nach bekannten Schwachstellen mit nmap	495
12.5	Bekannte Schwachstellen mit Metasploit ausnutzen	497
12.6	Angriff über bekannte oder schwache Passwörter	503
12.7	E-Mail-Phishing-Kampagnen für Unternehmen	507
12.8	Phishing-Angriffe mit Office-Makros	516
12.9	Phishing-Angriffe mit ISO- und ZIP-Dateien	521
12.10	Angriffsvektor USB-Phishing	527
12.11	Network Access Control (NAC) und 802.1X in lokalen Netzwerken	530
12.12	Rechteerweiterung am System	534
12.13	Sammeln von Zugangsdaten und -Tokens	541
12.14	SMB-Relaying-Angriff auf normale Domänenbenutzer	566

13 Windows Server absichern 571

13.1	Lokale Benutzer, Gruppen und Rechte	572
13.2	Manipulationen am Dateisystem	583
13.3	Serverhärtung	588
13.4	Microsoft Defender	591
13.5	Windows-Firewall	594
13.6	Windows-Ereignisanzeige	599
13.7	Angriffe auf Zertifizierungsstellen: Exploit Secure Channels	608

14 Active Directory 611

14.1	Was ist das Active Directory?	611
14.2	Manipulation der Active-Directory-Datenbank bzw. ihrer Daten	625
14.3	Manipulation von Gruppenrichtlinien	629
14.4	Domänenauthentifizierung (Kerberos)	636
14.5	Kerberos Armoring (FAST)	643
14.6	Angriffe gegen die Authentifizierungsprotokolle und LDAP	646
14.7	Pass-the-Hash-Angriffe (mimikatz)	648
14.8	Golden Ticket, Silver Ticket und Diamond Ticket	660
14.9	Sensible Information aus der Active-Directory-Datenbank auslesen	665
14.10	Grundabsicherung	667
14.11	Mehr Sicherheit durch Tiers (Schichten)	672
14.12	Schutzmaßnahmen gegen Pass-the-Hash- und Pass-the-Ticket-Angriffe	676

15 Linux absichern 689

15.1	Installation	690
15.2	Software-Updates	694
15.3	Kernel-Updates (Live-Patches)	699
15.4	SSH absichern	701
15.5	2FA mit Google Authenticator	707
15.6	Fail2ban	713
15.7	Firewall	720
15.8	Geo-Blocking mit nft	736
15.9	SELinux	742
15.10	AppArmor	748
15.11	Kernel Hardening	753
15.12	Apache	756
15.13	MySQL und MariaDB	763
15.14	Postfix	770
15.15	Dovecot	776
15.16	Docker	778
15.17	Logging und Monitoring	784
15.18	Rootkit-Erkennung und Intrusion Detection	789

16	Sicherheit bei Samba-Fileservern	799
16.1	Vorüberlegungen	799
16.2	Basisinstallation	801
16.3	Konfiguration des Samba-Domaincontrollers	804
16.4	Konfiguration des Samba-Servers	805
16.5	Samba-Server im Active Directory	808
16.6	Freigaben auf dem Samba-Server	812
16.7	Umstellung auf die Registry	817
16.8	Samba-Audit-Funktionen	821
16.9	Firewall	823
16.10	Angriffsszenarien auf Samba-Fileserver	828
17	Sicherheit von Webanwendungen	839
17.1	Architektur von Webapplikationen	839
17.2	Angriffe gegen Webanwendungen	842
17.3	Praktische Analyse einer Webanwendung	876
17.4	Schutzmechanismen und Abwehr von Webangriffen	898
17.5	Sicherheitsanalyse von Webanwendungen	907
18	Intrusion-Detection-Systeme	911
18.1	Verfahren zur Intrusion Detection	911
18.2	Host- versus netzwerkbasierte IDS	914
18.3	Reaktionen	920
18.4	IDS umgehen und manipulieren	922
18.5	Snort	925
18.6	Snort-Regeln	932
18.7	Wazuh	941
18.8	Wazuh-Beispiel: Brute-Force-Angriffe	951
19	Software-Exploitation	955
19.1	Schwachstellen von Software	955
19.2	Aufdecken von Sicherheitslücken	958
19.3	Programmausführung auf x86-Systemen	959
19.4	Ausnutzung von Buffer-Overflows	970

19.5	Structured Exception Handling (SEH)	985
19.6	Heap Spraying	987
19.7	Schutzmechanismen gegen Buffer-Overflows	989
19.8	Schutzmaßnahmen gegen Buffer-Overflows umgehen	994
19.9	Buffer-Overflows als Entwickler verhindern	1000
19.10	Spectre und Meltdown	1002

20 Sichere KI-Anwendungen 1011

20.1	Einführung in LLMs	1012
20.2	Die Angriffsfläche von GenAI-Anwendungen	1014
20.3	Prompt Injections	1017
20.4	Schwachstellen in (Gen)AI-Anwendungen finden	1022
20.5	GenAI-Anwendungen absichern	1030
20.6	Hacking mit KI	1034

TEIL III Cloud, Smartphones, IoT

21 Sicherheit in der Cloud 1041

21.1	Überblick	1042
21.2	Amazon S3	1045
21.3	Nextcloud	1054

22 Microsoft 365 sicher betreiben 1063

22.1	Angriffe auf die Cloud	1063
22.2	Angriffsvektoren und Risiken	1065
22.3	Microsoft-365-Tenants absichern	1072
22.4	Geräte, Konten und Gäste verwalten	1077
22.5	Entra ID Protection und Conditional Access	1081
22.6	App-Registrierung verwalten	1088
22.7	Exchange Online absichern	1091
22.8	Microsoft Defender XDR	1095
22.9	Endpoint-Management	1107
22.10	Datenzugriffe steuern und überwachen	1112
22.11	Datenklassifizierung und Microsoft Purview Information Protection	1115

23 Mobile Security 1119

23.1	Sicherheitsgrundlagen von Android und iOS	1119
23.2	Bedrohungen von mobilen Endgeräten	1126
23.3	Malware und Exploits	1138
23.4	Technische Analyse von Apps	1146
23.5	Schutzmaßnahmen für Android und iOS	1157
23.6	Apple Supervised Mode und Apple Configurator	1171
23.7	Enterprise Mobility Management	1178

24 IoT-Sicherheit 1187

24.1	Was ist das Internet der Dinge?	1187
24.2	IoT-Schwachstellen finden	1189
24.3	Absicherung von IoT-Geräten in Netzwerken	1210
24.4	IoT-Protokolle und -Dienste	1212
24.5	IoT-Funktechniken	1227
24.6	IoT aus Entwicklersicht	1232
24.7	Programmiersprachen für Embedded Controller	1237
24.8	Regeln für die sichere IoT-Programmierung	1240

Die Autoren	1253
-------------------	------

Index	1255
-------------	------