

Aigner, Gebeshuber, Hackner, Kania, Kloep,
Kofler, Neugebauer, Widl, Zingsheim

Hacking & Security

Das umfassende Handbuch

Inhalt

Vorwort	13
Grußwort	17
TEIL I Einführung und Tools	
1 Einführung	21
1.1 Hacking	21
1.2 Sicherheit	29
1.3 Exploits	41
1.4 Authentifizierung und Passwörter	48
1.5 Sicherheitsrisiko IPv6	52
1.6 Gesetzliche Rahmenbedingungen	54
1.7 Security-Organisationen und staatliche Einrichtungen	58
2 Kali Linux	61
2.1 Kali Linux ohne Installation ausprobieren	62
2.2 Kali Linux in eine virtuelle Maschine installieren	69
2.3 Kali Linux im Windows-Subsystem für Linux	77
2.4 Interna	78
2.5 Einfache Anwendungsbeispiele	81
2.6 PentestBox	85
3 Test- und Lernumgebung einrichten (Metasploitable)	87
3.1 Metasploitable 2 (Ubuntu)	88
3.2 Metasploitable 3 (Windows)	94
4 Hacking-Tools	115
4.1 nmap	116
4.2 hydra	120

4.3	nikto	126
4.4	sslyze, sslscan und testssl	129
4.5	whois, host und dig	133
4.6	Wireshark	135
4.7	tcpdump	141
4.8	Netcat (nc)	144
4.9	SPARTA	147
4.10	OpenVAS	148
4.11	Metasploit Framework	159
4.12	Metasploit Community	169
4.13	Armitage	180
4.14	Empire Framework	182
4.15	Social Engineering Toolkit (SET)	192
4.16	Burp Suite	199

TEIL II Hacking und Absicherung

5	Offline Hacking	209
5.1	BIOS/EFI-Grundlagen	209
5.2	Auf fremde Systeme zugreifen	212
5.3	Auf externe Festplatten oder SSDs zugreifen	219
5.4	Windows-Passwort zurücksetzen	220
5.5	Linux- und macOS-Passwort zurücksetzen	227
5.6	Festplatten verschlüsseln	229
6	Passwörter	239
6.1	Hash-Verfahren	240
6.2	Brute-Force Password Cracking	243
6.3	Rainbow Tables	244
6.4	Wörterbuch-Attacken	246
6.5	Passwort-Tools	248
6.6	Default-Passwörter	256
6.7	Data Breaches	257
6.8	Multi-Faktor-Authentifizierung	259
6.9	Sicheres Passwort-Handling implementieren	260

7	WLAN, Bluetooth und SDR	263
7.1	802.11x-Systeme (WiFi)	263
7.2	Bluetooth	281
7.3	Software-Defined Radios (SDR)	298
8	Angriffsvektor USB-Schnittstelle	309
8.1	USB-Rubber-Ducky	310
8.2	Digispark – ein Wolf im Schafspelz	319
8.3	Bash Bunny	329
8.4	Gegenmaßnahmen	351
9	Externe Sicherheitsüberprüfungen	355
9.1	Gründe für professionelle Überprüfungen	355
9.2	Typen von Sicherheitsüberprüfungen	356
9.3	Rechtliche Absicherung	366
9.4	Zielsetzung und Abgrenzung	368
9.5	Methodologien zur Durchführung	369
9.6	Reporting	371
9.7	Auswahl des richtigen Anbieters	374
10	Client-Side Penetration-Testing	377
10.1	Open Source Intelligence (OSINT)	377
10.2	E-Mail-Phishing-Kampagnen für Unternehmen	394
10.3	Phishing-Angriffe mit .PDF.EXE-Dateien	403
10.4	Praxisbeispiel: Phishing-Angriffe mit Office-Makros	414
10.5	Praxisbeispiel: Phishing-Angriffe mit Word-DDE-Code	418
10.6	Angriffsvektor USB-Phishing	424
10.7	Man-in-the-Middle-Angriffe auf unverschlüsselte Verbindungen	425
10.8	Man-in-the-Middle-Angriff auf SSL/TLS-Verbindungen	432
10.9	Man-in-the-Middle-Angriffe auf Remote Desktop	437
10.10	Angriffe auf Netzwerk-Hashes	443
10.11	SMB-Relaying mit der Impacket-Library (Angriff auf Administratoren)	445
10.12	SMB-Relaying mit snarf (Angriff auf normale Domänenbenutzer)	449

11	Penetration-Testing in Netzwerken	453
11.1	Externe IP-Adressen der PTA überprüfen	453
11.2	Network Access Control (NAC) und 802.1X in lokalen Netzwerken	457
11.3	Scanning von interessanten Zielen	461
11.4	Suche nach bekannten Schwachstellen mit nmap	468
11.5	Bekannte Schwachstellen mit Metasploit ausnutzen	469
11.6	Angriff auf schwache Passwörter	475
11.7	Post-Exploitation von Systemen	478
12	Windows Server absichern	495
12.1	Lokale Benutzer, Gruppen und Rechte	496
12.2	Manipulationen am Dateisystem	504
12.3	Server-Härtung	509
12.4	Windows Defender	517
12.5	Windows Firewall	520
12.6	Windows Ereignisanzeige	524
13	Active Directory	535
13.1	Was ist das Active Directory?	535
13.2	Manipulation der Active-Directory-Datenbank bzw. ihrer Daten	549
13.3	Manipulation von Gruppenrichtlinien	553
13.4	Domänenauthentifizierung (Kerberos)	559
13.5	Pass-the-Hash-Angriffe (mimikatz)	567
13.6	Golden Ticket und Silver Ticket	579
13.7	Grundabsicherung	582
13.8	Mehr Sicherheit durch Tiers (Schichten)	587
13.9	Schutzmaßnahmen gegen Pass-the-Hash und Pass-the-Ticket-Angriffe	592
14	Linux absichern	601
14.1	Installation	602
14.2	Software-Updates	605
14.3	Kernel-Updates (Live Patches)	610
14.4	SSH absichern	613
14.5	Google Authenticator	620
14.6	Fail2ban	626

14.7	Firewall	632
14.8	SELinux	642
14.9	AppArmor	649
14.10	Apache	654
14.11	MySQL und MariaDB	660
14.12	Postfix	668
14.13	Dovecot	674
14.14	Rootkit-Erkennung und Intrusion Detection	676
15	Sicherheit bei Samba-Fileservern	687
15.1	Vorüberlegungen	688
15.2	CentOS-Basisinstallation	689
15.3	Debian-Basisinstallation	693
15.4	Konfiguration des Samba-Servers	695
15.5	Samba-Server im Active Directory	699
15.6	Freigaben auf dem Samba-Server	703
15.7	Umstellung auf die Registry	708
15.8	Samba-Audit-Funktionen	712
15.9	Firewall	714
15.10	Angriffsszenarien auf Samba-Fileserver	719
15.11	Prüfen von Samba-Fileservern	722
16	Sicherheit von Webanwendungen	731
16.1	Architektur von Webapplikationen	731
16.2	Angriffe gegen Webanwendungen	734
16.3	Praktische Analyse einer Webanwendung	759
16.4	Schutzmechanismen und Abwehr von Webangriffen	778
16.5	Sicherheitsanalyse von Webanwendungen	786
17	Software-Exploitation	791
17.1	Schwachstellen von Software	791
17.2	Aufdecken von Sicherheitslücken	794
17.3	Programmausführung auf x86-Systemen	795
17.4	Ausnutzung von Buffer-Overflows	805
17.5	Structured Exception Handling (SEH)	821

17.6	Heap Spraying	823
17.7	Schutzmechanismen gegen Buffer-Overflows umgehen	825
17.8	Schutzmaßnahmen gegen Buffer-Overflows	829
17.9	Buffer-Overflows als Entwickler verhindern	835
17.10	Spectre und Meltdown	837

TEIL III Cloud, Smartphones, IoT

18	Sicherheit in der Cloud	847
18.1	Überblick	847
18.2	Amazon S3	851
18.3	Nextcloud/ownCloud	859
19	Office 365 absichern	867
19.1	Identitäten und Zugriffsverwaltung	868
19.2	Mehrstufige Authentifizierung	877
19.3	Bedingter Zugriff	883
19.4	Identity Protection	891
19.5	Office 365 Cloud App Security	893
19.6	Privileged Identities	897
19.7	Viren- und Spamschutz im E-Mail-Verkehr	905
19.8	Schadcode-Erkennung in E-Mails mit ATP	913
19.9	Sicherheit in den Rechenzentren	921
20	Mobile Security	927
20.1	Sicherheitsgrundlagen von Android und iOS	927
20.2	Bedrohungen von mobilen Endgeräten	935
20.3	Malware und Exploits	946
20.4	Technische Analyse von Apps	957
20.5	Schutzmaßnahmen für Android und iOS	966
20.6	Apple Supervised Mode und Apple Configurator	979
20.7	Enterprise Mobility Management	986

21	IoT-Sicherheit	997
21.1	Was ist das Internet der Dinge?	997
21.2	IoT-Schwachstellen finden	999
21.3	Absicherung von IoT-Geräten in Netzwerken	1016
21.4	IoT-Protokolle und -Dienste	1017
21.5	IoT-Funktechniken	1026
21.6	IoT aus Entwicklersicht	1031
21.7	Programmiersprachen für Embedded Controller	1036
21.8	Regeln für die sichere IoT-Programmierung	1039
	Die Autoren	1051
	Index	1053