

# Inhalt

Vorwort .....	13
Grußwort .....	18

## TEIL I Einführung und Tools

---

<b>1 Einführung</b> .....	21
1.1 Hacking .....	21
1.2 Sicherheit .....	30
1.3 Exploits .....	43
1.4 Authentifizierung und Passwörter .....	51
1.5 Sicherheitsrisiko IPv6 .....	57
1.6 Gesetzliche Rahmenbedingungen .....	58
1.7 Security-Organisationen und staatliche Einrichtungen .....	62
<b>2 Kali Linux</b> .....	65
2.1 Kali Linux Live ohne Installation ausprobieren .....	66
2.2 Kali Linux in VirtualBox installieren .....	73
2.3 Kali Linux und Hyper-V .....	82
2.4 Kali Linux im Windows-Subsystem für Linux .....	84
2.5 Kali Linux auf dem Raspberry Pi .....	87
2.6 Kali Linux auf Apple-PCs mit ARM-CPU ausführen .....	88
2.7 Einfache Anwendungsbeispiele .....	91
2.8 Kali-Interna .....	94
<b>3 Lernumgebung einrichten (Metasploitable, Juice Shop)</b> .....	101
3.1 Metasploitable 2 .....	103
3.2 Metasploitable 3 (Ubuntu-Variante) .....	109
3.3 Metasploitable 3 (Windows-Variante) .....	116
3.4 Juice Shop .....	126

<b>4</b>	<b>Hacking-Tools</b>	131
4.1	nmap	132
4.2	hydra	136
4.3	sslyze, sslscan und testssl	142
4.4	whois, host und dig	145
4.5	Wireshark	148
4.6	tcpdump	154
4.7	Netcat (nc)	157
4.8	OpenVAS	161
4.9	Metasploit Framework	172
4.10	Empire Framework	184
4.11	Das Post-Exploitation-Framework Koadic	195
4.12	Social-Engineer Toolkit (SET)	203
4.13	Burp Suite	210
4.14	Sliver	218

## TEIL II Hacking und Absicherung

---

<b>5</b>	<b>Offline Hacking</b>	227
5.1	BIOS/EFI-Grundlagen	228
5.2	Auf fremde Systeme zugreifen	230
5.3	Auf externe Festplatten oder SSDs zugreifen	237
5.4	Windows-Passwort zurücksetzen	238
5.5	Linux- und macOS-Passwort zurücksetzen	245
5.6	Datenträger verschlüsseln	248
<b>6</b>	<b>Passwörter</b>	259
6.1	Hash-Verfahren	260
6.2	Brute-Force Password Cracking	263
6.3	Rainbow Tables	265
6.4	Wörterbuch-Attacken	266
6.5	Passworttools	268
6.6	Default-Passwörter	277

---

6.7	Data Breaches .....	278
6.8	Multi-Faktor-Authentifizierung .....	280
6.9	Sicheres Passwort-Handling implementieren .....	281
<b>7</b>	<b>IT-Forensik .....</b>	<b>285</b>
7.1	Methodische Analyse von Vorfällen .....	287
7.2	Post-Mortem-Untersuchung .....	290
7.3	Live-Analyse .....	307
7.4	Forensic Readiness .....	310
7.5	Zusammenfassung .....	313
<b>8</b>	<b>WLAN, Bluetooth und SDR .....</b>	<b>315</b>
8.1	802.11x-Systeme (WiFi) .....	315
8.2	WPA-2-Handshakes mit dem Pwnagotchi einsammeln .....	335
8.3	Bluetooth .....	342
8.4	Software-Defined Radios (SDR) .....	360
<b>9</b>	<b>Angriffsvektor USB-Schnittstelle .....</b>	<b>369</b>
9.1	USB-Rubber-Ducky .....	370
9.2	Digispark – ein Wolf im Schafspelz .....	377
9.3	Bash Bunny .....	385
9.4	P4wnP1 – das Universaltalent .....	407
9.5	MalDuino W .....	418
9.6	Gegenmaßnahmen .....	425
<b>10</b>	<b>Externe Sicherheitsüberprüfungen .....</b>	<b>431</b>
10.1	Gründe für professionelle Überprüfungen .....	431
10.2	Typen von Sicherheitsüberprüfungen .....	432
10.3	Rechtliche Absicherung .....	444
10.4	Zielsetzung und Abgrenzung .....	446
10.5	Methodologien zur Durchführung .....	448
10.6	Reporting .....	449
10.7	Auswahl des richtigen Anbieters .....	452

<b>11</b>	<b>Penetration-Testing</b>	455
11.1	Informationssammlung	456
11.2	Initialer Zugriff mit Codeausführung	474
11.3	Scanning von interessanten Zielen	479
11.4	Suche nach bekannten Schwachstellen mit nmap	486
11.5	Bekannte Schwachstellen mit Metasploit ausnutzen	488
11.6	Angriff über bekannte oder schwache Passwörter	494
11.7	E-Mail-Phishing-Kampagnen für Unternehmen	497
11.8	Phishing-Angriffe mit Office-Makros	507
11.9	Phishing-Angriffe mit ISO- und ZIP-Dateien	511
11.10	Angriffsvektor USB-Phishing	521
11.11	Network Access Control (NAC) und 802.1X in lokalen Netzwerken	524
11.12	Rechteerweiterung am System	527
11.13	Sammeln von Zugangsdaten und -Tokens	535
11.14	SMB-Relaying-Angriff auf normale Domänenbenutzer	560
<b>12</b>	<b>Windows Server absichern</b>	565
12.1	Lokale Benutzer, Gruppen und Rechte	566
12.2	Manipulationen am Dateisystem	576
12.3	Serverhärtung	582
12.4	Microsoft Defender	585
12.5	Windows-Firewall	588
12.6	Windows-Ereignisanzeige	592
<b>13</b>	<b>Active Directory</b>	603
13.1	Was ist das Active Directory?	603
13.2	Manipulation der Active-Directory-Datenbank bzw. ihrer Daten	617
13.3	Manipulation von Gruppenrichtlinien	621
13.4	Domänenauthentifizierung (Kerberos)	627
13.5	Angriffe gegen die Authentifizierungsprotokolle und LDAP	635
13.6	Pass-the-Hash-Angriffe (mimikatz)	637
13.7	Golden Ticket und Silver Ticket	650
13.8	Sensible Information aus der Active-Directory-Datenbank auslesen	654

---


13.9	Grundabsicherung .....	657
13.10	Mehr Sicherheit durch Tiers (Schichten) .....	661
13.11	Schutzmaßnahmen gegen Pass-the-Hash- und Pass-the-Ticket-Angriffe .....	666
<b>14</b>	<b>Linux absichern .....</b>	<b>677</b>
14.1	Installation .....	678
14.2	Software-Updates .....	683
14.3	Kernel-Updates (Live Patches) .....	687
14.4	SSH absichern .....	690
14.5	2FA mit Google Authenticator .....	695
14.6	2FA mit YubiKey .....	701
14.7	Fail2ban .....	703
14.8	Firewall .....	710
14.9	SELinux .....	725
14.10	AppArmor .....	731
14.11	Kernel Hardening .....	736
14.12	Apache .....	739
14.13	MySQL und MariaDB .....	745
14.14	Postfix .....	752
14.15	Dovecot .....	758
14.16	Rootkit-Erkennung und Intrusion Detection .....	760
<b>15</b>	<b>Sicherheit bei Samba-Fileservern .....</b>	<b>769</b>
15.1	Vorüberlegungen .....	770
15.2	CentOS-Basisinstallation .....	771
15.3	Debian-Basisinstallation .....	776
15.4	Konfiguration des Samba-Servers .....	778
15.5	Samba-Server im Active Directory .....	781
15.6	Freigaben auf dem Samba-Server .....	785
15.7	Umstellung auf die Registry .....	790
15.8	Samba-Audit-Funktionen .....	794
15.9	Firewall .....	796
15.10	Angriffsszenarien auf Samba-Fileserver .....	801
15.11	Prüfen von Samba-Fileservern .....	804

<b>16</b>	<b>Intrusion-Detection-Systeme</b>	811
16.1	Verfahren zur Intrusion Detection	811
16.2	Host- versus netzwerkbasierte IDS	814
16.3	Reaktionen	820
16.4	IDS umgehen und manipulieren	822
16.5	Snort	825
16.6	Snort-Regeln	832
<b>17</b>	<b>Sicherheit von Webanwendungen</b>	841
17.1	Architektur von Webapplikationen	841
17.2	Angriffe gegen Webanwendungen	844
17.3	Praktische Analyse einer Webanwendung	878
17.4	Schutzmechanismen und Abwehr von Webangriffen	900
17.5	Sicherheitsanalyse von Webanwendungen	909
<b>18</b>	<b>Software-Exploitation</b>	913
18.1	Schwachstellen von Software	913
18.2	Aufdecken von Sicherheitslücken	916
18.3	Programmausführung auf x86-Systemen	917
18.4	Ausnutzung von Buffer-Overflows	927
18.5	Structured Exception Handling (SEH)	943
18.6	Heap Spraying	945
18.7	Schutzmechanismen gegen Buffer-Overflows	947
18.8	Schutzmaßnahmen gegen Buffer-Overflows umgehen	951
18.9	Buffer-Overflows als Entwickler verhindern	958
18.10	Spectre und Meltdown	959
<b>19</b>	<b>Bug-Bounty-Programme</b>	967
19.1	Die Idee hinter Bug Bounties	967
19.2	Reporting von Schwachstellen	970
19.3	Tipps & Tricks für Analysten	972
19.4	Tipps für Unternehmen	975

## TEIL III Cloud, Smartphones, IoT

<b>20</b>	<b>Sicherheit in der Cloud</b> .....	979
20.1	Überblick .....	980
20.2	Amazon S3 .....	983
20.3	Nextcloud/ownCloud .....	992
<b>21</b>	<b>Microsoft 365 absichern</b> .....	1001
21.1	Identitäten und Zugriffsverwaltung .....	1002
21.2	Sicherheitsbewertung .....	1008
21.3	Mehrstufige Authentifizierung .....	1010
21.4	Bedingter Zugriff .....	1018
21.5	Identity Protection .....	1023
21.6	Privileged Identities .....	1025
21.7	Schadcode-Erkennung .....	1030
21.8	Sicherheit in den Rechenzentren .....	1040
<b>22</b>	<b>Mobile Security</b> .....	1045
22.1	Sicherheitsgrundlagen von Android und iOS .....	1045
22.2	Bedrohungen von mobilen Endgeräten .....	1053
22.3	Malware und Exploits .....	1064
22.4	Technische Analyse von Apps .....	1076
22.5	Schutzmaßnahmen für Android und iOS .....	1087
22.6	Apple Supervised Mode und Apple Configurator .....	1102
22.7	Enterprise Mobility Management .....	1109
<b>23</b>	<b>IoT-Sicherheit</b> .....	1121
23.1	Was ist das Internet der Dinge? .....	1121
23.2	IoT-Schwachstellen finden .....	1123
23.3	Absicherung von IoT-Geräten in Netzwerken .....	1141
23.4	IoT-Protokolle und -Dienste .....	1143
23.5	IoT-Funktechniken .....	1155
23.6	IoT aus Entwicklersicht .....	1160

23.7	Programmiersprachen für Embedded Controller .....	1165
23.8	Regeln für die sichere IoT-Programmierung .....	1168
Die Autoren .....		1181
Index .....		1183

Diese Leseprobe haben Sie beim  
 **edv-buchversand.de** heruntergeladen.  
Das Buch können Sie online in unserem  
Shop bestellen.

[Hier zum Shop](#)