

Inhaltsverzeichnis

Einleitung	13
Warum Kali Linux?	13
Über dieses Buch	15
Teil I Grundlagen von Kali Linux	17
1 Einführung	19
1.1 Unterschied zwischen Kali und Debian	19
1.2 Ein Stück Geschichte	19
1.3 Kali Linux – für jeden etwas	21
1.3.1 Varianten von Kali Linux	22
1.4 Die Hauptfeatures	25
1.4.1 Live-System	26
1.4.2 Ein maßgeschneiderter Linux-Kernel	28
1.4.3 Komplett anpassbar	28
1.4.4 Ein vertrauenswürdiges Betriebssystem	30
1.4.5 Auf einer großen Anzahl von ARM-Geräten verwendbar	30
1.5 Richtlinien von Kali Linux	31
1.5.1 Benutzer ohne root-Rechte	31
1.5.2 Netzwerkdienste sind standardmäßig deaktiviert	32
1.5.3 Eine organisierte Sammlung von Tools	32
1.6 Zusammenfassung	33
2 Linux-Grundlagen	35
2.1 Was ist Linux und wie funktioniert es?	35
2.1.1 Hardwaresteuerung	37
2.1.2 Vereinheitlichtes Dateisystem	38
2.1.3 Prozesse verwalten	39
2.1.4 Rechtemanagement	40
2.2 Die Kommandozeile (Command Line)	41
2.2.1 Wie komme ich zur Kommandozeile?	41
2.2.2 Verzeichnisbaum durchsuchen und Dateien verwalten	42

2.3	Das Dateisystem.	44
2.3.1	Dateisystem-Hierarchie-Standard	44
2.3.2	Das Home-Verzeichnis des Anwenders	45
2.4	Hilfreiche Befehle	46
2.4.1	Anzeigen und Ändern von Text-Dateien.	46
2.4.2	Suche nach Dateien und innerhalb von Dateien	46
2.4.3	Prozesse verwalten	47
2.4.4	Rechte verwalten.	47
2.4.5	Systeminformationen und Logs aufrufen.	51
2.4.6	Hardware erkennen	52
2.5	Zusammenfassung	53
3	Installation von Kali.	57
3.1	Systemanforderungen	57
3.2	Erstellen eines bootfähigen Mediums	58
3.2.1	Herunterladen des ISO-Images.	58
3.2.2	Kopieren des Images auf ein bootfähiges Medium	59
3.2.3	Aktivieren der Persistenz auf dem USB-Stick	62
3.3	Stand-Alone-Installation	64
3.3.1	Partitionierung der Festplatte	70
3.3.2	Konfigurieren des Package Managers (apt)	77
3.3.3	GRUB-Bootloader installieren	79
3.3.4	Installation abschließen und neu starten	81
3.4	Dual-Boot – Kali Linux und Windows	81
3.5	Installation auf einem vollständig verschlüsselten Dateisystem	85
3.5.1	Einführung in LVM	85
3.5.2	Einführung in LUKS	85
3.5.3	Konfigurieren verschlüsselter Partitionen	86
3.6	Kali Linux auf Windows Subsystem for Linux.	91
3.6.1	Win-KeX	94
3.7	Kali Linux auf einem Raspberry Pi.	95
3.8	Systemeinstellungen und Updates.	98
3.8.1	Repositories.	98
3.8.2	NVIDIA-Treiber für Kali Linux installieren	99
3.8.3	Terminal als Short-Cut (Tastenkombination).	100
3.9	Fehlerbehebung bei der Installation.	101
3.9.1	Einsatz der Installer-Shell zur Fehlerbehebung.	102
3.10	Zusammenfassung	103

4	Erste Schritte mit Kali	105
4.1	Konfiguration von Kali Linux	105
4.1.1	Netzwerkeinstellungen	106
4.1.2	Verwalten von Benutzern und Gruppen	109
4.1.3	Services konfigurieren	111
4.2	Managing Services.	119
4.3	Hacking-Labor einrichten	121
4.4	Sichern und Überwachen mit Kali Linux	123
4.4.1	Sicherheitsrichtlinien definieren.	124
4.4.2	Mögliche Sicherheitsmaßnahmen	126
4.4.3	Netzwerkservices absichern.	127
4.4.4	Firewall- oder Paketfilterung	128
4.5	Weitere Tools installieren	136
4.5.1	Meta-Packages mit kali-tweaks installieren	136
4.5.2	Terminator statt Terminal	137
4.5.3	OpenVAS zur Schwachstellenanalyse.	138
4.5.4	SSLstrip2	141
4.5.5	Dns2proxy	142
4.6	Kali Linux ausschalten.	143
4.7	Zusammenfassung	143

Teil II Einführung in Penetration Testing

5	Einführung in Security Assessments	149
5.1	Kali Linux in einem Assessment	151
5.2	Arten von Assessments	152
5.2.1	Schwachstellenanalyse	154
5.2.2	Compliance-Test.	159
5.2.3	Traditioneller Penetrationstest	160
5.2.4	Applikations-Assessment.	162
5.3	Normierung der Assessments	164
5.4	Arten von Attacken	165
5.4.1	Denial of Services (DoS)	166
5.4.2	Speicherbeschädigungen	167
5.4.3	Schwachstellen von Webseiten	167
5.4.4	Passwort-Attacken	168
5.4.5	Clientseitige Angriffe	169
5.5	Zusammenfassung	169

6	Kali Linux für Security Assessments vorbereiten	171
6.1	Kali-Pakete anpassen	171
6.1.1	Quellen finden	173
6.1.2	Build-Abhängigkeiten installieren	176
6.1.3	Änderungen durchführen	177
6.1.4	Build erstellen	181
6.2	Linux-Kernel kompilieren	181
6.2.1	Einführung und Voraussetzungen	182
6.2.2	Quellen finden	183
6.2.3	Kernel konfigurieren	184
6.2.4	Pakete kompilieren und erstellen	187
6.3	Erstellen eines individuellen Kali-Live-ISO-Images	188
6.3.1	Voraussetzungen	189
6.3.2	Erstellen von Live-Images mit verschiedenen Desktop-Umgebungen	190
6.3.3	Ändern der Liste installierter Pakete	191
6.3.4	Verwenden von Hooks zum Optimieren des Live-Images	192
6.3.5	Hinzufügen von Dateien zum ISO-Image oder Live-Filesystem	192
6.4	Hinzufügen von Persistenz auf einem USB-Stick	193
6.4.1	Erstellen einer unverschlüsselten Persistenz auf einem USB-Stick	194
6.4.2	Erstellen einer verschlüsselten Persistenz auf einem USB-Stick	195
6.4.3	Verwenden von mehreren Persistenzspeichern	197
6.5	»Automatisierte« Installation	198
6.5.1	Antworten auf Installationsabfragen vorbereiten	198
6.5.2	Erstellen der Voreinstellungsdatei	200
6.6	Zusammenfassung	201
6.6.1	Kali-Pakete ändern	201
6.6.2	Linux-Kernel neu kompilieren	202
6.6.3	Benutzerdefinierte ISO-Images erstellen	203
7	Ablauf eines Penetrationstests	205
7.1	Informationen sammeln	209
7.1.1	Was nun?	209
7.1.2	Kali-Tools zur Informationsbeschaffung	211
7.1.3	Informationen nach angreifbaren Zielen durchsuchen	211

7.2	Scannen	212
7.2.1	Pings	215
7.2.2	Portscan.....	217
7.2.3	Nmap Script Engine – Transformationen eines Tools	225
7.2.4	Schwachstellen-Scan	228
7.3	Eindringen über das lokale Netzwerk	229
7.3.1	Zugriff auf Remotedienste.....	230
7.3.2	Übernahme von Systemen	231
7.3.3	Passwörter hacken	234
7.3.4	Abrissbirnen-Technik – Passwörter zurücksetzen	239
7.3.5	Netzwerkverkehr ausspähen	240
7.4	Webgestütztes Eindringen	242
7.4.1	Schwachstellen in Webapplikationen finden.....	245
7.4.2	Webseite analysieren	245
7.4.3	Informationen abfangen	245
7.4.4	Auf Schwachstellen scannen.....	246
7.5	Nachbearbeitung und Erhaltung des Zugriffs.....	246
7.6	Abschluss eines Penetrationstests	248
7.7	Zusammenfassung	249

Teil III Tools in Kali Linux 251

8	Tools zur Informationsbeschaffung und Schwachstellenanalyse ...	253
8.1	Tools zur Informationssammlung.....	253
8.1.1	Nmap – Das Schweizer Taschenmesser für Portscanning.....	253
8.1.2	TheHarvester – E-Mail-Adressen aufspüren und ausnutzen	258
8.1.3	Dig – DNS-Informationen abrufen.....	260
8.1.4	Fierce – falls der Zonentransfer nicht möglich ist.....	260
8.1.5	MetaGooFil – Metadaten extrahieren	261
8.1.6	HTTrack – Webseite als Offline-Kopie	263
8.1.7	Maltego – gesammelte Daten in Beziehung setzen.....	265
8.1.8	Legion – Automation in der Informationsbeschaffung.	267
8.2	Schwachstellenanalyse-Tools	269
8.2.1	OpenVAS – Sicherheitslücken aufdecken	269
8.2.2	Nikto – Aufspüren von Schwachstellen auf Webservern ...	273
8.2.3	Siege – Performance Test von Webseiten	274

8.3	Sniffing und Spoofing	276
8.3.1	Dsniff – Sammlung von Werkzeugen zum Ausspionieren von Netzwerkdatenverkehr	276
8.3.2	Ettercap – Netzwerkverkehr ausspionieren	277
8.3.3	Wireshark – der Hai im Datenmeer	280
9	Tools für Attacken	283
9.1	Wireless-Attacken	283
9.1.1	aircrack-ng	283
9.1.2	wifiphisher	287
9.1.3	Kismet	289
9.2	Webseiten-Penetration-Testing	291
9.2.1	WebScarab	291
9.2.2	Skipfish	296
9.2.3	Zed Attack Proxy	297
9.3	Exploitation-Tools	300
9.3.1	Metasploit	300
9.3.2	Armitage	308
9.3.3	Social Engineer Toolkit (SET)	309
9.3.4	Searchsploit	312
9.4	Passwort-Angriffe	314
9.4.1	Medusa	315
9.4.2	Hydra	317
9.4.3	John the Ripper	318
9.4.4	Samdump2	322
9.4.5	chntpw	323
10	Forensik-Tools	327
10.1	Dcfldd – Abbild für forensische Untersuchung erstellen	327
10.2	Autopsy	329
10.3	Binwalk	332
10.4	chkrootkit	334
10.5	Bulk_extractor	334
10.6	Foremost	335
10.7	Galleta	336
10.8	Hashdeep	336
10.9	Volafox	338
10.10	Volatility	339

11	Tools für Reports	341
11.1	Cutycapt	341
11.2	Faraday-IDE	343
11.3	Pipal	346
11.4	RecordMyDesktop	347
A	Terminologie und Glossar	349
B	Übersicht Kali-Meta-Pakete	353
B.1	kali-linux.	353
B.2	kali-linux-full	353
B.3	kali-linux-all	354
B.4	kali-linux-top10	354
B.5	kali-linux-forensic	354
B.6	kali-linux-gpu	355
B.7	kali-linux-pwtools.	355
B.8	kali-linux-rfid	355
B.9	kali-linux-sdr	355
B.10	kali-linux-voip.	355
B.11	kali-linux-web.	356
B.12	kali-linux-wireless	356
C	Checkliste: Penetrationstest	357
C.1	Scope	357
C.2	Expertise	359
C.3	Lösung	359
D	Installation von Xfce und Undercover-Modus	361
	Stichwortverzeichnis	365