

Einstieg in Kali Linux

Penetration Testing und
Ethical Hacking mit Linux

DAS INHALTS- VERZEICHNIS

» Hier geht's
direkt
zum Buch

Inhaltsverzeichnis

Einleitung	13
Warum Kali Linux?	13
Über dieses Buch	15
Teil I Grundlagen von Kali Linux	17
<hr/>	
1 Einführung	19
1.1 Unterschied zwischen Kali und Debian	19
1.2 Ein Stück Geschichte	19
1.3 Kali Linux – für jeden etwas	22
1.3.1 Varianten von Kali Linux	23
1.4 Die Hauptfeatures	25
1.4.1 Live-System	27
1.4.2 Ein maßgeschneiderter Linux-Kernel	29
1.4.3 Komplett anpassbar	29
1.4.4 Ein vertrauenswürdige Betriebssystem	31
1.4.5 Auf einer großen Anzahl von ARM-Geräten verwendbar	31
1.5 Richtlinien von Kali Linux	32
1.5.1 Benutzer ohne root-Rechte	32
1.5.2 Netzwerkdienste sind standardmäßig deaktiviert	32
1.5.3 Eine organisierte Sammlung von Tools	33
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
4.3.1	Kali Linux – Test Lab Environment	123
4.4	Sichern und Überwachen mit Kali Linux	127
4.4.1	Sicherheitsrichtlinien definieren.	127
4.4.2	Mögliche Sicherheitsmaßnahmen	129
4.4.3	Netzwerkservices absichern.	131
4.4.4	Firewall- oder Paketfilterung	131
4.5	Weitere Tools installieren	140
4.5.1	Meta-Packages mit kali-tweaks installieren	140
4.5.2	Terminator statt Terminal	141
4.5.3	OpenVAS zur Schwachstellenanalyse.	142
4.5.4	SSLstrip2.	146
4.5.5	Dns2proxy.	147
4.6	Kali Linux ausschalten.	148
4.7	Zusammenfassung	148
Teil II Einführung in Penetration Testing		151
5	Einführung in Security Assessments	153
5.1	Kali Linux in einem Assessment	155
5.2	Arten von Assessments	156
5.2.1	Schwachstellenanalyse	158
5.2.2	Compliance-Test.	163
5.2.3	Traditioneller Penetrationstest	164
5.2.4	Applikations-Assessment.	166
5.3	Normierung der Assessments	168
5.4	Arten von Attacken	169
5.4.1	Denial of Services (DoS)	170
5.4.2	Speicherbeschädigungen	171
5.4.3	Schwachstellen von Webseiten	171
5.4.4	Passwort-Attacken	172
5.4.5	Clientseitige Angriffe	173
5.5	Zusammenfassung	173

6	Kali Linux für Security Assessments vorbereiten	175
6.1	Kali-Pakete anpassen	175
6.1.1	Quellen finden	177
6.1.2	Build-Abhängigkeiten installieren	180
6.1.3	Änderungen durchführen	181
6.1.4	Build erstellen	185
6.2	Linux-Kernel kompilieren	185
6.2.1	Einführung und Voraussetzungen	186
6.2.2	Quellen finden	187
6.2.3	Kernel konfigurieren	188
6.2.4	Pakete kompilieren und erstellen	191
6.3	Erstellen eines individuellen Kali-Live-ISO-Images	192
6.3.1	Voraussetzungen	193
6.3.2	Erstellen von Live-Images mit verschiedenen Desktop- Umgebungen	194
6.3.3	Ändern der Liste installierter Pakete	195
6.3.4	Verwenden von Hooks zum Optimieren des Live-Images	196
6.3.5	Hinzufügen von Dateien zum ISO-Image oder Live- Filesystem	196
6.4	Hinzufügen von Persistenz auf einem USB-Stick	197
6.4.1	Erstellen einer unverschlüsselten Persistenz auf einem USB-Stick	198
6.4.2	Erstellen einer verschlüsselten Persistenz auf einem USB-Stick	199
6.4.3	Verwenden von mehreren Persistenzspeichern	201
6.5	»Automatisierte« Installation	202
6.5.1	Antworten auf Installationsabfragen vorbereiten	202
6.5.2	Erstellen der Voreinstellungsdatei	204
6.6	Zusammenfassung	205
6.6.1	Kali-Pakete ändern	205
6.6.2	Linux-Kernel neu kompilieren	206
6.6.3	Benutzerdefinierte ISO-Images erstellen	207
7	Ablauf eines Penetrationstests	209
7.1	Informationen sammeln	213
7.1.1	Was nun?	213
7.1.2	Kali-Tools zur Informationsbeschaffung	215
7.1.3	Informationen nach angreifbaren Zielen durchsuchen	215

7.2	Scannen	216
7.2.1	Pings	219
7.2.2	Portscan.....	221
7.2.3	Nmap Script Engine – Transformationen eines Tools	229
7.2.4	Schwachstellen-Scan	232
7.3	Eindringen über das lokale Netzwerk	233
7.3.1	Zugriff auf Remotedienste.....	234
7.3.2	Übernahme von Systemen	235
7.3.3	Passwörter hacken	238
7.3.4	Abrissbirnen-Technik – Passwörter zurücksetzen	243
7.3.5	Netzwerkverkehr ausspähen	244
7.4	Webgestütztes Eindringen	246
7.4.1	Schwachstellen in Webapplikationen finden.....	249
7.4.2	Webseite analysieren	249
7.4.3	Informationen abfangen	249
7.4.4	Auf Schwachstellen scannen.....	250
7.5	Nachbearbeitung und Erhaltung des Zugriffs.....	250
7.6	Abschluss eines Penetrationstests	252
7.7	Zusammenfassung	253

Teil III Tools in Kali Linux 255

8	Tools zur Informationsbeschaffung und Schwachstellenanalyse ...	257
8.1	Tools zur Informationssammlung.....	257
8.1.1	Nmap – Das Schweizer Taschenmesser für Portscanning.....	257
8.1.2	TheHarvester – E-Mail-Adressen aufspüren und ausnutzen	262
8.1.3	Dig – DNS-Informationen abrufen.....	264
8.1.4	Fierce – falls der Zonentransfer nicht möglich ist.....	264
8.1.5	MetaGooFil – Metadaten extrahieren	265
8.1.6	HTTrack – Webseite als Offline-Kopie	267
8.1.7	Maltego – gesammelte Daten in Beziehung setzen.....	269
8.1.8	Legion – Automation in der Informationsbeschaffung.....	271
8.2	Schwachstellenanalyse-Tools	273
8.2.1	OpenVAS – Sicherheitslücken aufdecken	273
8.2.2	Nikto – Aufspüren von Schwachstellen auf Webservern ...	277
8.2.3	Siege – Performance Test von Webseiten	278

8.3	Sniffing und Spoofing	280
8.3.1	Dsniff – Sammlung von Werkzeugen zum Ausspionieren von Netzwerkdatenverkehr	280
8.3.2	Ettercap – Netzwerkverkehr ausspionieren	281
8.3.3	Wireshark – der Hai im Datenmeer	284
9	Tools für Attacks	287
9.1	Wireless-Attacks	287
9.1.1	aircrack-ng	287
9.1.2	wifiphisher	291
9.1.3	Kismet	293
9.2	Webseiten-Penetration-Testing	295
9.2.1	WebScarab	295
9.2.2	Skipfish	300
9.2.3	Zed Attack Proxy	301
9.3	Exploitation-Tools	304
9.3.1	Metasploit	304
9.3.2	Armitage	312
9.3.3	Social Engineer Toolkit (SET)	313
9.3.4	Searchsploit	316
9.4	Passwort-Angriffe	318
9.4.1	Medusa	319
9.4.2	Hydra	321
9.4.3	John the Ripper	322
9.4.4	Samdump2	326
9.4.5	chntpw	327
10	Forensik-Tools	331
10.1	Dcfldd – Abbild für forensische Untersuchung erstellen	331
10.2	Autopsy	333
10.3	Binwalk	336
10.4	chkrootkit	338
10.5	Bulk_extractor	338
10.6	Foremost	339
10.7	Galleta	340
10.8	Hashdeep	340
10.9	Volafox	342
10.10	Volatility	343

11	Tools für Reports	345
11.1	Cutycapt	345
11.2	Faraday-IDE	347
11.3	Pipal	350
11.4	RecordMyDesktop	351
A	Terminologie und Glossar	353
B	Übersicht Kali-Meta-Pakete	357
B.1	System-Pakete	358
B.2	Tools	360
B.3	Menü	368
C	Checkliste: Penetrationstest	381
C.1	Scope	381
C.2	Expertise	383
C.3	Lösung	383
D	Installation von Xfce und Undercover-Modus	385
	Stichwortverzeichnis	389