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 23
1.4.1 Live-System 25
1.4.2 Ein maßgeschneiderter Linux-Kernel 27
1.4.3 Komplett anpassbar 27
1.4.4 Ein vertrauenswürdiges Betriebssystem 29
1.4.5 Auf einer großen Anzahl von ARM-Geräten verwendbar 29
1.5 Richtlinien von Kali Linux 30
1.5.1 Ein einzelner Root-Benutzer als Standard 30
1.5.2 Netzwerkdienste sind standardmäßig deaktiviert 30
1.5.3 Eine organisierte Sammlung von Tools 30
1.6 Zusammenfassung 31

2 **Linux-Grundlagen** 33
2.1 Was ist Linux und wie funktioniert es? 33
2.1.1 Hardwaresteuerung 35
2.1.2 Vereinheitlichtes Dateisystem 36
2.1.3 Prozesse verwalten 37
2.1.4 Rechtemanagement 38
2.2 Die Kommandozeile (Command Line) 39
2.2.1 Wie komme ich zur Kommandozeile? 39
2.2.2 Verzeichnisbaum durchsuchen und Dateien verwalten 40

Bibliografische Informationen
http://d-nb.info/1197070893

digitalisiert durch DEUTSCHE NATIONAL BIBLIOTHEK

2.3 Das Dateisystem ... 42
2.3.1 Dateisystem-Hierarchie-Standard ... 42
2.3.2 Das Home-Verzeichnis des Anwenders ... 43
2.4 Hilfreiche Befehle ... 44
2.4.1 Anzeigen und Ändern von Text-Dateien ... 44
2.4.2 Suche nach Dateien und innerhalb von Dateien ... 44
2.4.3 Prozesse verwalten ... 45
2.4.4 Rechte verwalten ... 45
2.4.5 Systeminformationen und Logs aufrufen ... 49
2.4.6 Hardware erkennen ... 50
2.5 Zusammenfassung ... 51

3 Installation von Kali ... 55
3.1 Systemanforderungen ... 55
3.2 Erstellen eines bootfähigen Mediums ... 56
3.2.1 Herunterladen des ISO-Images ... 56
3.2.2 Kopieren des Images auf ein bootfähiges Medium ... 57
3.2.3 Aktivieren der Persistenz auf dem USB-Stick ... 60
3.3 Stand-Alone-Installation ... 62
3.3.1 Partitionierung der Festplatte ... 68
3.3.2 Konfigurieren des Package Managers (apt) ... 75
3.3.3 GRUB-Bootloaders installieren ... 76
3.3.4 Installation abschließen und neu starten ... 79
3.4 Dual-Boot – Kali Linux und Windows ... 79
3.5 Installation auf einem vollständig verschlüsselten Dateisystem ... 82
3.5.1 Einführung in LVM ... 82
3.5.2 Einführung in LUKS ... 83
3.5.3 Konfigurieren verschlüsselter Partitionen ... 83
3.6 Kali Linux auf Windows Subsystem for Linux ... 88
3.7 Kali Linux auf einem Raspberry Pi ... 91
3.8 Systemeinstellungen und Updates ... 94
3.8.1 Repositories ... 94
3.8.2 NVIDIA-Treiber für Kali Linux installieren ... 95
3.8.3 Terminal als Short-Cut (Tastenkombination) ... 98
3.9 Fehlerbehebung bei der Installation ... 99
3.9.1 Einsatz der Installer-Shell zur Fehlerbehebung ... 100
3.10 Zusammenfassung ... 101

4 **Erste Schritte mit Kali** ... 103
4.1 Konfiguration von Kali Linux ... 103
4.1.1 Netzwerkeinstellungen ... 104
4.1.2 Verwalten von Benutzern und Gruppen ... 107
4.1.3 Services konfigurieren ... 109
4.2 Managing Services ... 117
4.3 Hacking-Labor einrichten ... 119
4.4 Sichern und Überwachen mit Kali Linux ... 121
4.4.1 Sicherheitsrichtlinien definieren ... 122
4.4.2 Mögliche Sicherheitsmaßnahmen ... 124
4.4.3 Netzwerkservices absichern ... 125
4.4.4 Firewall- oder Paketfilterung ... 126
4.5 Weitere Tools installieren ... 134
4.5.1 Terminator statt Terminal ... 134
4.5.2 OpenVAS zur Schwachstellenanalyse ... 135
4.5.3 SSLstrip2 ... 138
4.5.4 Dns2proxy ... 139
4.6 Kali Linux ausschalten ... 139
4.7 Zusammenfassung ... 140

Teil II Einführung in Penetration Testing ... 143

5 **Einführung in Security Assessments** ... 145
5.1 Kali Linux in einem Assessment ... 147
5.2 Arten von Assessments ... 148
5.2.1 Schwachstellenanalyse ... 150
5.2.2 Compliance-Test ... 155
5.2.3 Traditioneller Penetrationstest ... 156
5.2.4 Applikations-Assessment ... 158
5.3 Normierung der Assessments ... 160
5.4 Arten von Attacken ... 161
5.4.1 Denial of Services (DoS) ... 162
5.4.2 Speicherbeschädigungen ... 163
5.4.3 Schwachstellen von Webseiten ... 163
5.4.4 Passwort-Attacken ... 164
5.4.5 Clientseitige Angriffe ... 165
5.5 Zusammenfassung ... 165

6 Kali Linux für Security Assessments vorbereiten ... 167
6.1 Kali-Pakete anpassen ... 167
6.1.1 Quellen finden ... 169
6.1.2 Build-Abhängigkeiten installieren ... 172
6.1.3 Änderungen durchführen ... 173
6.1.4 Build erstellen ... 177
6.2 Linux-Kernel kompilieren ... 177
6.2.1 Einführung und Voraussetzungen ... 178
6.2.2 Quellen finden ... 179
6.2.3 Kernel konfigurieren ... 180
6.2.4 Pakete kompilieren und erstellen ... 182
6.3 Erstellen eines individuellen Kali-Live-ISO-Images ... 183
6.3.1 Voraussetzungen ... 184
6.3.2 Erstellen von Live-Images mit verschiedenen Desktop-Umgebungen ... 185
6.3.3 Ändern der Liste installierter Pakete ... 186
6.3.4 Verwenden von Hooks zum Optimieren des Live-Images ... 187
6.3.5 Hinzufügen von Dateien zum ISO-Image oder Live-Filesystem ... 187
6.4 Hinzufügen von Persistenz auf einem USB-Stick ... 188
6.4.1 Erstellen einer unverschlüsselten Persistenz auf einem USB-Stick ... 189
6.4.2 Erstellen einer verschlüsselten Persistenz auf einem USB-Stick ... 190
6.4.3 Verwenden von mehreren Persistenzspeichern ... 191
6.5 »Automatisierte« Installation ... 193
6.5.1 Antworten auf Installationsabfragen vorbereiten ... 193
6.5.2 Erstellen der Voreinstellungsdatei ... 195
6.6 Zusammenfassung ... 195
6.6.1 Kali-Pakete ändern ... 196
6.6.2 Linux-Kernel neu kompilieren ... 197
6.6.3 Benutzerdefinierte ISO-Images erstellen ... 198

7 Ablauf eines Penetrationstests ... 201
7.1 Informationen sammeln ... 205
7.1.1 Was nun? ... 205
7.1.2 Kali-Tools zur Informationsbeschaffung ... 207
7.1.3 Informationen nach angreifbaren Zielen durchsuchen ... 207

7.2 Scannen ... 208
7.2.1 Pings ... 211
7.2.2 Portscan ... 213
7.2.3 Nmap Script Engine – Transformationen eines Tools ... 221
7.2.4 Schwachstellen-Scan ... 224
7.3 Eindringen über das lokale Netzwerk ... 225
7.3.1 Zugriff auf Remotedienste ... 226
7.3.2 Übernahme von Systemen ... 227
7.3.3 Passwörter hacken ... 230
7.3.4 Abrissbirnen-Technik – Passwörter zurücksetzen ... 235
7.3.5 Netzwerkverkehr ausspähen ... 236
7.4 Webgestütztes Eindringen ... 238
7.4.1 Schwachstellen in Webapplikationen finden ... 241
7.4.2 Webseite analysieren ... 241
7.4.3 Informationen abfangen ... 241
7.4.4 Auf Schwachstellen scannen ... 242
7.5 Nachbearbeitung und Erhaltung des Zugriffs ... 242
7.6 Abschluss eines Penetrationstests ... 244
7.7 Zusammenfassung ... 245

Teil III Tools in Kali Linux ... 247

8 **Tools zur Informationsbeschaffung und Schwachstellenanalyse** ... 249
8.1 Tools zur Informationssammlung ... 249
8.1.1 Nmap – Das Schweizer Taschenmesser für Portscanning ... 249
8.1.2 TheHarvester – E-Mail-Adressen aufspüren und ausnutzen ... 254
8.1.3 Dig – DNS-Informationen abrufen ... 256
8.1.4 Fierce – falls der Zonentransfer nicht möglich ist ... 256
8.1.5 MetaGooFil – Metadaten extrahieren ... 257
8.1.6 HTTrack – Webseite als Offline-Kopie ... 258
8.1.7 Maltego – gesammelte Daten in Beziehung setzen ... 260
8.1.8 Sparta – Automation in der Informationsbeschaffung ... 262
8.2 Schwachstellenanalyse-Tools ... 264
8.2.1 OpenVAS – Sicherheitslücken aufdecken ... 264
8.2.2 Nikto – Aufspüren von Schwachstellen auf Webservern ... 268
8.2.3 Siege – Performance Test von Webseiten ... 270

8.3 Sniffing und Spoofing ... 271
8.3.1 Dsniff – Sammlung von Werkzeugen zum Ausspionieren von Netzwerkdatenverkehr ... 272
8.3.2 Ettercap – Netzwerkverkehr ausspionieren ... 273
8.3.3 Wireshark – der Hai im Datenmeer ... 275

9 Tools für Attacken ... 279
9.1 Wireless-Attacken ... 279
9.1.1 aircrack-ng ... 279
9.1.2 Ghost Phisher ... 283
9.1.3 Kismet ... 284
9.2 Webseiten-Penetration-Testing ... 286
9.2.1 WebScarab ... 286
9.2.2 Skipfish ... 291
9.2.3 Zed Attack Proxy ... 292
9.3 Exploitation-Tools ... 295
9.3.1 Metasploit ... 295
9.3.2 Armitage ... 303
9.3.3 Social Engineer Toolkit (SET) ... 304
9.3.4 Searchsploit ... 307
9.4 Passwort-Angriffe ... 309
9.4.1 Medusa ... 310
9.4.2 Hydra ... 312
9.4.3 John the Ripper ... 313
9.4.4 Samdump2 ... 317
9.4.5 chntpw ... 318

10 Forensik-Tools ... 321
10.1 Dcfldd – Abbild für forensische Untersuchung erstellen ... 321
10.2 Autopsy ... 323
10.3 Binwalk ... 326
10.4 Chkrootkit ... 328
10.5 Bulk_extrator ... 328
10.6 Foremost ... 329
10.7 Galleta ... 330
10.8 Hashdeep ... 330
10.9 Volafox ... 332
10.10 Volatility ... 333

11 Tools für Reports ... 335
11.1 Cutycapt ... 335
11.2 Faraday-IDE ... 337
11.3 Pipal ... 341
11.4 RecordMyDesktop ... 341

A Terminologie und Glossar ... 343

B Übersicht Kali-Meta-Pakete ... 347
B.1 kali-linux ... 347
B.2 kali-linux-full ... 347
B.3 kali-linux all ... 348
B.4 kali-linux-top10 ... 348
B.5 kali-linux-forensic ... 348
B.6 kali-linux-gpu ... 349
B.7 kali-linux-pwtools ... 349
B.8 kali-linux-rfid ... 349
B.9 kali-linux-sdr ... 349
B.10 kali-linux-voip ... 349
B.11 kali-linux-web ... 350
B.12 kali-linux-wireless ... 350

C Checkliste: Penetrationstest ... 351
C.1 Scope ... 351
C.2 Expertise ... 353
C.3 Lösung ... 353

D Installation von Xfce und Undercover-Modus ... 355

Stichwortverzeichnis ... 359