ÜBERSETZUNG DER 2. AUFLAGE

LINUX BASICS FÜR HACKER

EINSTIEG UND HACKING-GRUNDLAGEN MIT KALI LINUX: *NETZWERKE*, *SCRIPTING* UND *SECURITY*

OCCUPYTHEWEB

DEUTSCHE AUSGABE

no starch press

mitp

Inhaltsverzeichnis

Vorwort **15**

Danksagung **17**

Einführung **19**
Was Sie in diesem Buch erwartet 20
Was ist ethisches Hacking? 21
Penetrationstests 21
Militär und Spionage 22
Wieso Hacker Linux nutzen 22
Linux ist Open Source 22
Linux ist transparent 22
Linux bietet eine granulare Kontrolle 23
Die meisten Hacking-Tools sind für Linux geschrieben . . . 23
Die Zukunft gehört Linux/Unix 23
Kali Linux herunterladen 23
Virtuelle Maschinen 25
VirtualBox installieren 25
Ihre virtuelle Maschine einrichten 26
Kali auf der VM installieren 28
Kali einrichten 30
Kali über das Windows Subsystem for Linux installieren 36

1 Die Grundlagen **39**
1.1 Einführende Begriffe und Konzepte 39
1.2 Eine Tour durch Kali 40
1.2.1 Das Terminal 41
1.2.2 Das Linux-Dateisystem 41
1.3 Grundlegende Befehle unter Linux 43
1.3.1 Sich selbst finden mit pwd 43
1.3.2 Ihr Login mit whoami prüfen 43
1.3.3 Durch das Linux-Dateisystem navigieren 44
1.3.4 Hilfe bekommen 46
1.3.5 Das Handbuch aufrufen 47

1.4 Suchen und finden ... 48
1.4.1 Mit locate suchen ... 48
1.4.2 Mit whereis Binärdateien suchen ... 49
1.4.3 Mit which Binärdateien in der PATH-Variablen suchen ... 49
1.4.4 Mit find noch leistungsfähigere Suchen durchführen ... 49
1.4.5 Filtern mit grep ... 51
1.5 Dateien und Verzeichnisse modifizieren ... 52
1.5.1 Dateien erzeugen ... 53
1.5.2 Ein Verzeichnis anlegen ... 54
1.5.3 Eine Datei kopieren ... 55
1.5.4 Eine Datei umbenennen ... 55
1.5.5 Eine Datei entfernen ... 56
1.5.6 Ein Verzeichnis entfernen ... 56
1.6 Gehen Sie jetzt spielen! ... 57
1.7 Übungen ... 57

2 Textmanipulation ... 59
2.1 Dateien betrachten ... 59
2.1.1 Den Anfang finden ... 60
2.1.2 Das Ende finden ... 61
2.1.3 Die Zeilen nummerieren ... 62
2.2 Text filtern mit grep ... 63
2.3 Suchen und Ersetzen mit sed ... 64
2.4 Dateien betrachten mit more und less ... 66
2.4.1 Die Anzeige steuern mit more ... 66
2.4.2 Anzeigen und Filtern mit less ... 67
2.5 Zusammenfassung ... 69
2.6 Übungen ... 69

3 Netzwerke analysieren und konfigurieren ... 71
3.1 Netzwerke analysieren mit ifconfig ... 71
3.2 Netzwerkstatistiken mit netstat und ss ... 73
3.3 Drahtlose Netzwerkgeräte mit iwconfig prüfen ... 74
3.4 Ihre Netzwerkinformationen ändern ... 75
3.4.1 Eine neue IP-Adresse zuweisen ... 75
3.4.2 Netzmaske und Broadcast-Adresse ändern ... 76
3.4.3 Ihre MAC-Adresse fälschen ... 76
3.4.4 Neue IP-Adressen vom DHCP-Server aus zuweisen ... 77

3.5 Das Domain Name System manipulieren ... 78
3.5.1 Mit dig das DNS untersuchen ... 78
3.5.2 Ihren DNS-Server ändern ... 79
3.5.3 Ihre eigene IP-Adresse zuordnen ... 81
3.6 Zusammenfassung ... 82
3.7 Übungen ... 82

4 Software hinzufügen und entfernen ... 83
4.1 Die Verwendung von apt für die Verwaltung von Software ... 83
4.1.1 Nach einem Paket suchen ... 83
4.1.2 Software hinzufügen ... 84
4.1.3 Software entfernen ... 85
4.1.4 Updates von Paketen ... 86
4.1.5 Upgrades von Paketen ... 87
4.2 Repositorys zu Ihrer sources.list-Datei hinzufügen ... 87
4.3 Einen GUI-basierten Installer benutzen ... 89
4.4 Software installieren mit git ... 92
4.5 Zusammenfassung ... 93
4.6 Übungen ... 93

5 Datei- und Verzeichnisberechtigungen kontrollieren ... 95
5.1 Verschiedene Arten von Benutzern ... 95
5.2 Berechtigungen setzen ... 96
5.2.1 Einem einzelnen Benutzer die Eigentümerschaft gewähren ... 96
5.2.2 Einer Gruppe die Eigentümerschaft gewähren ... 97
5.3 Berechtigungen überprüfen ... 97
5.4 Berechtigungen ändern ... 99
5.4.1 Berechtigungen mithilfe der Dezimalnotation ändern ... 99
5.4.2 Berechtigungen mit UGO ändern ... 101
5.4.3 root die Ausführberechtigung für ein neues Tool gewähren ... 102
5.5 Mit Masken sicherere Standardberechtigungen setzen ... 104
5.6 Spezielle Berechtigungen ... 105
5.6.1 Mit SUID temporäre root-Rechte gewähren ... 105
5.6.2 Mit SGID die Gruppenberechtigungen des root-Benutzers gewähren ... 105
5.6.3 Das veraltete Sticky Bit ... 106
5.6.4 Spezielle Berechtigungen, Rechteeskalation und der Hacker ... 106
5.7 Zusammenfassung ... 108
5.8 Übungen ... 108

6 Prozessverwaltung ... 109
6.1 Prozesse anzeigen ... 109
6.1.1 Filtern nach dem Prozessnamen ... 111
6.1.2 Mit top die ressourcenhungrigsten Prozesse finden ... 112
6.2 Prozesse verwalten ... 113
6.2.1 Mit nice die Priorität von Prozessen ändern ... 113
6.2.2 Prozesse beenden ... 115
6.2.3 Prozesse im Hintergrund ausführen ... 117
6.2.4 Einen Prozess in den Vordergrund holen ... 118
6.3 Prozesse zeitgesteuert ausführen ... 118
6.4 Zusammenfassung ... 119
6.5 Übungen ... 119

7 Benutzerumgebungsvariablen verwalten ... 121
7.1 Die Standard-Shell auf bash ändern ... 121
7.2 Umgebungsvariablen anzeigen und manipulieren ... 123
7.2.1 Alle Umgebungsvariablen anzeigen ... 124
7.2.2 Nach bestimmten Variablen filtern ... 124
7.2.3 Variablenwerte für eine Sitzung ändern ... 125
7.2.4 Variablenänderungen permanent machen ... 125
7.3 Ihren Shell-Prompt ändern ... 126
7.4 Ihren PATH ändern ... 128
7.4.1 Die PATH-Variable erweitern ... 128
7.4.2 Wie Sie die PATH-Variable nicht erweitern sollten ... 129
7.5 Eine benutzerdefinierte Variable anlegen ... 130
7.6 Zusammenfassung ... 130
7.7 Übungen ... 131

8 bash-Skripte schreiben ... 133
8.1 Ein Crashkurs in bash ... 133
8.2 Ihr erstes Skript: »Hello, Hackers-Arise!« ... 136
8.2.1 Ausführberechtigungen setzen ... 137
8.2.2 HelloHackersArise ausführen ... 137
8.2.3 Mit Variablen und Benutzereingaben Funktionalität hinzufügen ... 138
8.3 Ihr erstes Hacker-Skript: Nach offenen Ports scannen ... 140
8.3.1 Ihre Aufgabe ... 141
8.3.2 Ein einfacher Scanner ... 142
8.3.3 Eine verbesserte Variante des MySQL-Scanners ... 143
8.4 Gebräuchliche eingebaute bash-Befehle ... 146
8.5 Zusammenfassung ... 147
8.6 Übungen ... 147

9 Komprimieren und archivieren 149
9.1 Was ist Komprimierung? 149
9.2 Dateien mit tar zusammenfassen 150
9.3 Dateien komprimieren 152
9.3.1 Mit gzip komprimieren 152
9.3.2 Mit bzip2 komprimieren 153
9.3.3 Mit compress komprimieren 154
9.4 Bit für Bit kopieren oder physische Kopien von Speichergeräten erstellen 154
9.5 Zusammenfassung 156
9.6 Übungen 156

10 Verwaltung von Dateisystem und Speichergeräten 157
10.1 Das Geräteverzeichnis /dev 157
10.1.1 Wie Linux Speichergeräte repräsentiert 159
10.1.2 Laufwerkspartitionen 159
10.1.3 Zeichen- und Blockgeräte 161
10.1.4 Block-Geräte und Informationen mit lsblk und lsusb auflisten 162
10.2 Mounten und unmounten 163
10.2.1 Speichergeräte manuell mounten 163
10.2.2 Unmounten mit umount 164
10.3 Dateisysteme überwachen 164
10.3.1 Informationen über gemountete Laufwerke erhalten 164
10.3.2 Auf Fehler überprüfen 165
10.4 Zusammenfassung 166
10.5 Übungen 167

11 Das Logging-System 169
11.1 Das Dienstprogramm journalctl 169
11.2 Log-Prioritäten und Facilitys 171
11.3 journalctl-Abfragen 173
11.4 Mit journalctl Ihre Spuren verwischen 174
11.5 Das Logging deaktivieren 176
11.6 Zusammenfassung 178
11.7 Übungen 178

12 Dienste benutzen und missbrauchen 179
12.1 Dienste starten, stoppen und neu starten 179
12.2 Mit dem Apache-Webserver einen HTTP-Server erstellen 180
12.2.1 Erste Schritte mit Apache 180
12.2.2 Die Datei index.html bearbeiten 181

12.2.3 Ein bisschen HTML hinzufügen 182
12.2.4 Sehen, was passiert 183
12.3 OpenSSH und der Raspberry-Pi-Spion 183
12.3.1 Den Raspberry Pi einrichten 184
12.3.2 Den Raspberry-Pi-Spion bauen 184
12.3.3 Die Kamera konfigurieren 186
12.3.4 Beginnen Sie mit dem Spionieren 186
12.4 Informationen aus MySQL/MariaDB extrahieren 187
12.4.1 MySQL oder MariaDB starten 188
12.4.2 Mit SQL interagieren 188
12.4.3 Ein Passwort festlegen 189
12.4.4 Auf eine entfernte Datenbank zugreifen 190
12.4.5 Mit einer Datenbank verbinden 191
12.4.6 Datenbanktabellen erkunden 192
12.4.7 Die Daten untersuchen 193
12.5 Zusammenfassung 194
12.6 Übungen 194

13 Sicher und anonym werden 195
13.1 Wie das Internet Sie verrät 195
13.2 Das Onion-Router-System 197
13.2.1 Wie Tor funktioniert 197
13.2.2 Sicherheitsbedenken 199
13.3 Proxy-Server 199
13.3.1 Proxys in der Konfigurationsdatei festlegen 200
13.3.2 Weitere interessante Optionen konfigurieren 203
13.3.3 Noch ein Wort zur Sicherheit 206
13.4 Virtuelle private Netzwerke 206
13.5 Verschlüsselte E-Mail 207
13.6 Zusammenfassung 208
13.7 Übungen 209

14 Drahtlose Netzwerke verstehen und untersuchen 211
14.1 Wi-Fi-Netzwerke 211
14.1.1 Grundlegende WLAN-Befehle 212
14.2 Wi-Fi-Aufklärung mit aircrack-ng 216
14.3 Bluetooth ausfindig machen und damit verbinden 219
14.3.1 Wie Bluetooth funktioniert 219
14.3.2 Bluetooth scannen und auskundschaften 220
14.4 Zusammenfassung 224
14.5 Übungen 224

15 Den Linux-Kernel und ladbare Kernel-Module verwalten 225
15.1 Was ist ein Kernel-Modul? 226
15.2 Die Kernel-Version prüfen 227
15.3 Kernel-Tuning mit sysctl 227
15.4 Kernel-Module verwalten 230
15.4.1 Mit modinfo weitere Informationen finden 231
15.4.2 Mit modprobe Module hinzufügen und entfernen 231
15.4.3 Ein Kernel-Modul hinzufügen und entfernen 232
15.5 Zusammenfassung 233
15.6 Übungen 233

16 Aufgaben automatisieren mit Job-Scheduling 235
16.1 Ein Event oder einen Job für die automatische Ausführung planen 235
16.1.1 Eine Backup-Aufgabe planen 238
16.1.2 Ihren MySQLscanner mit crontab planen 239
16.1.3 crontab-Kürzel 240
16.2 Mit rc-Skripten Jobs beim Systemstart ausführen 241
16.2.1 Linux-Runlevel 241
16.2.2 Dienste zu rc.d hinzufügen 241
16.3 Über eine GUI Dienste zum Boot-Skript hinzufügen 243
16.4 Zusammenfassung 244
16.5 Übungen 244

17 Grundlagen des Python-Skriptings für Hacker 245
17.1 Python-Module hinzufügen 245
17.2 Der Einstieg in das Skripting mit Python 247
17.2.1 Variablen 248
17.2.2 Kommentare 251
17.2.3 Funktionen 252
17.3 Listen 253
17.4 Module 254
17.5 Objektorientierte Programmierung (OOP) 254
17.6 Netzwerkkommunikation in Python 256
17.6.1 Einen TCP-Client erstellen 256
17.6.2 Einen TCP-Listener erstellen 258
17.7 Dictionarys, Kontrollanweisungen und Schleifen 260
17.7.1 Dictionarys 260
17.7.2 Kontrollstrukturen 261
17.7.3 Schleifen 262
17.8 Ihre Hacking-Skripte verbessern 263
17.9 Ausnahmen und Passwort-Cracker 265
17.10 Zusammenfassung 268
17.11 Übungen 268

18 Künstliche Intelligenz für Hacker 269
18.1 Zusammenarbeit ist entscheidend 270
18.2 Die wichtigsten Player im Bereich der KI 270
18.3 KI in der Cybersicherheit einsetzen 271
18.4 Social-Engineering-Angriffe mit KI 272
18.5 Mit KI ein bash-Skript schreiben 274
18.6 Zusammenfassung 275
18.7 Übungen 275

Stichwortverzeichnis 277

Einführung

Hacking ist die wichtigste Fertigkeit des 21. Jahrhunderts! Ich sage das nicht so leichthin. Die Schlagzeilen, die uns seit einigen Jahren jeden Morgen erwarten, bestätigen es. Nationen spähen einander aus, Cyberkriminelle stehlen Milliarden Dollar, digitale Würmer erpressen Lösegelder von ihren Opfern, politische Gegner beeinflussen Wahlen und Kriegsparteien schalten die Kampfmittel ihrer Feinde aus. Betrachten Sie nur einmal den Cyberkrieg zwischen der Ukraine und Russland als Beispiel. Diese Ereignisse sind alle das Werk von Hackern und man beginnt jetzt erst, ihre Macht in unserer zunehmend digitalen Welt zu verstehen.

Ich beschloss, das Buch zu schreiben, nachdem ich mit Zehntausenden angehenden Hackern bei Null-Byte, Hackers Arise (*https://www.hackers-arise.com*) und in nahezu jedem Zweig von US-Militär, Nachrichtendiensten und Ermittlungsbehörden gearbeitet habe (einschließlich NSA, DIA, CIA und FBI). Diese Erfahrungen haben mich gelehrt, dass viele aufstrebende Hacker kaum oder gar keine Erfahrungen mit Linux haben. Dieser Mangel an Erfahrung ist die größte Hürde, die ihrem Weg zum Profi im Weg steht. Die meisten der besten Hacker-Tools laufen unter Linux, sodass Sie zumindest grundlegende Linux-Kenntnisse benötigen, wenn Sie professioneller Hacker werden wollen. Ich habe dieses Buch geschrieben, um Ihnen über diese Hürde zu helfen.

Hacking ist im IT-Bereich ein Eliteberuf. Entsprechend erfordert es ein umfassendes und detailliertes Verständnis von IT-Konzepten und -Technologien. Linux ist das grundlegende Fundament. Ich empfehle Ihnen dringend, die Zeit und Energie aufzuwenden, um es zu verstehen, wenn Sie Hacking und Informationssicherheit tatsächlich als Karriereweg wählen möchten.

Dieses Buch richtet sich nicht an erfahrene Hackerinnen oder Linux-Admins. Stattdessen ist es für all jene gedacht, die noch am Anfang des aufregenden Wegs von Hacking, Cybersecurity und Pentesting stehen. Es soll auch keine vollständige Abhandlung über Linux oder Hacking sein, sondern will lediglich als Startpunkt in diese Welten dienen. Es beginnt mit den wesentlichen Linux-Elementen und einigen Skripting-Grundlagen in bash und Python. Wo immer es angemessen erscheint, nutze ich Hacking-Beispiele, um die Linux-Prinzipien zu verdeutlichen.

In dieser Einführung erhalten Sie einen Einblick in die Entwicklung des ethischen Hackings für die Cybersecurity und ich zeige Ihnen die Vorgehensweise für das

Aufsetzen einer virtuellen Maschine, damit Sie auf Ihrem System Kali Linux installieren können, ohne das Betriebssystem zu stören, das Sie bereits benutzen.

Was Sie in diesem Buch erwartet

In den ersten Kapiteln machen Sie sich mit den Grundlagen von Linux vertraut. **Kapitel 1** stellt Ihnen das Dateisystem und das Terminal vor und zeigt Ihnen einige grundlegende Befehle. In **Kapitel 2** erfahren Sie, wie Sie Text manipulieren, um Software und Dateien zu finden, zu untersuchen und zu verändern.

In **Kapitel 3** befassen Sie sich mit Netzwerken. Sie werden nach Netzwerken scannen, Informationen über Verbindungen finden und sich selbst tarnen, indem Sie Ihre Netzwerk- und DNS-Informationen verschleiern.

Kapitel 4 lehrt Sie, Software zu installieren, zu entfernen und zu aktualisieren. Außerdem erfahren Sie, wie Sie Ihr System auf dem neuesten Stand halten.

In **Kapitel 5** manipulieren Sie Datei- und Verzeichnisberechtigungen, um zu kontrollieren, wer worauf zugreifen darf. Sie lernen außerdem einige Eskalationstechniken für Berechtigungen kennen.

In **Kapitel 6** erfahren Sie, wie Sie Dienste verwalten. Dazu gehört das Starten und Stoppen von Prozessen und das Zuweisen von Ressourcen, um Ihnen eine größere Kontrolle zu gewähren. In **Kapitel 7** arbeiten Sie mit Umgebungsvariablen für eine optimale Leistung, zur größeren Bequemlichkeit und sogar zur Tarnung. Sie werden Variablen suchen und filtern, Ihre `PATH`-Variable ändern und neue Umgebungsvariablen erzeugen.

Kapitel 8 führt Sie in das bash-Skripting ein, quasi ein Muss für jeden ernsthaften Hacker. Sie lernen die Grundlagen der bash kennen und schreiben ein Skript zum Scannen nach Ziel-Ports, die Sie später vielleicht infiltrieren werden.

Kapitel 9 und **10** vermitteln Ihnen einige grundlegende Kenntnisse für die Dateiverwaltung. Sie erfahren hier, wie Sie Dateien komprimieren und archivieren, um Ihr System sauber zu halten, wie Sie ganze Speichergeräte kopieren und Informationen zu Dateien und verbundenen Festplatten erhalten.

In den später folgenden Kapiteln steigen Sie tiefer in die Hacking-Themen ein. In **Kapitel 11** benutzen und manipulieren Sie das Protokollierungs- bzw. das Loggingsystem, um an Informationen zu den Aktivitäten Ihres Ziels zu gelangen und Ihre eigenen Spuren zu verwischen. **Kapitel 12** zeigt Ihnen, wie Sie drei wichtige Linux-Dienste benutzen und missbrauchen: den Apache-Webserver, OpenSSH und MySQL. Sie werden einen Webserver anlegen, einen Remote-Kamera-Spion bauen und Datenbanken und deren Schwachstellen kennenlernen. In **Kapitel 13** lernen Sie, wie Sie mit Proxy-Servern, dem Tor-Netzwerk, virtuellen privaten Netzwerken und verschlüsselten E-Mails sicher und anonym bleiben.

In **Kapitel 14** geht es um drahtlose Netzwerke. Sie lernen die grundlegenden Netzwerkbefehle kennen, knacken dann Wi-Fi-Access-Points, machen Bluetooth-Signale ausfindig und verbinden sich mit Bluetooth-Geräten.

Kapitel 15 taucht dann tiefer in Linux selbst ein. Es gibt einen Überblick darüber, wie der Kernel funktioniert und wie man seine Treiber missbrauchen kann, sodass sie bösartige Software ausliefern. In **Kapitel 16** erwerben Sie wichtige Fähigkeiten, um Ihre Hacking-Skripte zu automatisieren. **Kapitel 17** lehrt Sie grundlegende Python-Konzepte und Sie entwickeln zwei Hacking-Tools: einen Scanner zum Ausspähen von TCP/IP-Verbindungen und einen einfachen Passwort-Cracker. **Kapitel 18** untersucht die Schnittstelle von Hacking und künstlicher Intelligenz, stellt einige grundlegende Konzepte vor und demonstriert, wie die KI Sie bei der Cybersecurity unterstützen kann.

Was ist ethisches Hacking?

Mit der Vergrößerung des Felds der Informationssicherheit in den letzten Jahren ging ein dramatisches Wachstum im Bereich des ethischen Hackings einher, das auch als White-Hat-Hacking bezeichnet wird (in alten Western waren die mit den weißen Hüten immer die Guten). Ethisches Hacking ist die Praxis des Infiltrierens und Ausspähen eines Systems, um dessen Schwächen zu ermitteln und es besser abzusichern. Ich unterteile das Feld des ethischen Hackings in zwei Hauptkomponenten: das Durchführen von Penetrationstests für ein rechtmäßiges Informationssicherheitsunternehmen und Tätigkeiten für die militärischen oder zivilen Nachrichtendienste Ihres Lands. Beides sind rasant wachsende Bereiche und die Nachfrage ist riesig.

Penetrationstests

Da das Sicherheitsbewusstsein von Unternehmen immer weiter zunimmt und die Kosten für Sicherheitsvorfälle exponentiell ansteigen, sind viele große Organisationen dazu übergegangen, die Sicherheitsdienste an externe Vertragspartner auszulagern. Zu den wichtigsten Sicherheitsdiensten zählt das Penetration Testing (auch: Pen Testing oder Pentesting). Ein *Penetrationstest* ist im Prinzip ein legal beauftragter Hack, der die Schwächen des Netzwerks und der Systeme eines Unternehmens aufdecken soll.

Im Allgemeinen führen Organisationen zuerst eine Schwachstellenanalyse durch, um potenzielle Schwächen in ihren Netzwerken, Betriebssystemen und Diensten zu finden. Ich schreibe extra »potenziell«, da dieser Schwachstellenscan eine beträchtliche Anzahl von falsch-positiven Ergebnissen enthält (Dinge, die als Schwachstellen identifiziert werden, obwohl sie es nicht sind). Aufgabe eines Penetrationstesters ist der Versuch, diese Schwachstellen zu hacken bzw. zu »pene-

Die Grundlagen

Hacker sind Macher, das liegt in ihrem Wesen. Sie wollen Dinge anfassen und mit ihnen herumspielen. Sie möchten etwas erschaffen und (manchmal auch) kaputtmachen. Nur wenige von ihnen wollen dicke Wälzer voller IT-Theorie lesen, bevor sie mit dem loslegen, was sie am meisten lieben: Hacken. Angesichts all dessen soll dieses Kapitel Ihnen einige grundlegende Fertigkeiten vermitteln, damit Sie den Einstieg in Kali finden ..., und zwar jetzt!

Sie werden in diesem Kapitel keines der Konzepte in aller Ausführlichkeit kennenlernen, sondern gerade so viel erfahren, dass Sie mit Linux, dem Betriebssystem der Hacker, herumspielen und es erkunden können. Tiefergehende Diskussionen erwarten Sie dann in späteren Kapiteln.

1.1 Einführende Begriffe und Konzepte

Bevor Sie mit der Reise durch die wunderbare Welt von *Linux Basics für Hacker* beginnen, möchte ich Ihnen einige Begriffe vorstellen, die einige der später in diesem Kapitel diskutierten Konzepte näher erklären.

- **Binärdateien (Binaries)** – Dieser Begriff bezieht sich auf Dateien, die ausgeführt werden können, also vergleichbar den ausführbaren Programmdateien unter Windows. Im Allgemeinen befinden sich die Binärdateien im Verzeichnis */usr/bin* oder */usr/sbin* und umfassen Dienstprogramme wie `ps`, `cat`, `ls` und `ifconfig` (Sie werden im Laufe dieses Kapitels mehr über diese vier Programme erfahren) ebenso wie Anwendungen wie das Wi-Fi-Hacking-Tool aircrack-ng und das Intrusion-Detection-System (System zum Erkennen von Angriffen) Snort.
- **Case Sensitivity** – Anders als in Windows achtet Linux auf Groß- und Kleinschreibung, ist also case-sensitiv. Das bedeutet, dass *Desktop* sich von *desktop* und auch von *DeskTop* unterscheidet. Jede dieser Varianten würde einen anderen Datei- oder Verzeichnisnamen repräsentieren. Viele, die eher an eine Windows-Umgebung gewöhnt sind, finden das frustrierend. Falls Sie die Fehlermeldung »File or directory not found« erhalten und sich sicher sind, dass die Datei oder das Verzeichnis existiert, sollten Sie die Groß-/Kleinschreibung überprüfen.

- **Verzeichnis (Directory)** – Hiermit ist dasselbe gemeint wie ein Ordner unter Windows. Ein Verzeichnis bietet eine Möglichkeit, Dateien zu organisieren, und dies normalerweise auf hierarchische Weise.
- **Home** – Jeder Benutzer hat ein eigenes */home*-Verzeichnis. Das ist im Allgemeinen die Stelle, an der Dateien, die Sie erzeugen, standardmäßig gespeichert werden.
- **Kali** – Kali Linux ist eine Linux-Distribution, die speziell für Penetrationstests geschaffen wurde. Darin sind Hunderte von Tools vorinstalliert, sodass Sie diese nicht selbst zeitaufwendig suchen, herunterladen und installieren müssen.
- **root** – Wie fast alle Betriebssysteme hat Linux einen Administrator- oder *Superuser*-Zugang, der für die Benutzung durch eine vertrauenswürdige Person gedacht ist, die auf dem System fast alles machen kann. Dazu gehören Dinge wie das Neukonfigurieren des Systems, das Hinzufügen von Benutzern und das Ändern von Passwörtern. Unter Linux wird dieser Zugang *root* genannt. Als Hacker oder Pentester werden Sie den root-Zugang oft benutzen, um sich selbst Kontrolle über das System zu verschaffen. Tatsächlich ist es für viele Hacker-Tools erforderlich, den root-Zugang zu benutzen.
- **Skript** – Hierbei handelt es sich um eine Abfolge von Befehlen, die interpretiert und direkt ausgeführt werden. Viele Hacking-Tools sind einfach nur Skripte. Skripte können mit dem bash-Interpreter oder anderen Skriptsprachen-Interpretern ausgeführt werden, wie Python, Perl oder Ruby. Python ist momentan der beliebteste Interpreter bei Hackern.
- **Shell** – Dies ist eine Umgebung und ein Interpreter für das Ausführen von Befehlen unter Linux. Die am weitesten verbreitete Shell ist die bash – die sogenannte *Bourne again*-Shell. Andere beliebte Shells sind die C-Shell und die Z-Shell. Ich werde in diesem Buch ausschließlich die bash verwenden.
- **Terminal** – Dies ist eine Kommandozeilenschnittstelle, auch Command Line Interface oder CLI genannt.

Jetzt haben Sie also die grundlegenden Begriffe kennengelernt und werden nun beginnen, systematisch die wichtigsten Linux-Fertigkeiten zu entwickeln, die Sie brauchen, um ein Hacker oder Pentester zu werden. In diesem ersten Kapitel werde ich mir mit Ihnen zusammen den Einstieg in Kali Linux anschauen.

1.2 Eine Tour durch Kali

Nach dem Start von Kali begrüßt Sie ein Login-Bildschirm. Melden Sie sich mit dem Benutzernamen *kali* und dem Standard-Passwort *kali* an (falls Sie dieses Passwort vorhin geändert haben, nehmen Sie natürlich hier dieses neue Passwort). Sie sollten nun Zugang zu Ihrem Kali-Desktop haben. Sie werden im Folgenden zwei der grundlegendsten Aspekte des Desktops kennenlernen: die Terminalschnittstelle und die Dateistruktur.

1.2.1 Das Terminal

Der erste Schritt für die Benutzung von Kali besteht darin, das *Terminal* zu öffnen. Dabei handelt es sich um die Kommandozeilenschnittstelle (auch Command Line Interface oder CLI), die in diesem Buch benutzt wird. Klicken Sie auf dieses Icon, um das Terminal zu starten. Es sollte ungefähr so aussehen wie in Abbildung 1.1.

Abb. 1.1: Das Kali-Terminal

Dieses Terminal öffnet die Kommandozeilenumgebung, die sogenannte *Shell*, die es Ihnen erlaubt, Befehle auf dem darunter liegenden Betriebssystem auszuführen und Skripte zu schreiben. Linux besitzt viele unterschiedliche Shell-Umgebungen. Die beliebteste ist die bash, die in vielen Linux-Distributionen standardmäßig eingestellt ist.

Um Ihr Passwort zu ändern, können Sie den Befehl `passwd` verwenden.

1.2.2 Das Linux-Dateisystem

Die Linux-Dateisystemstruktur unterscheidet sich ein wenig von der unter Windows. Linux besitzt kein physisches Laufwerk (wie das Laufwerk *C:*) als Basis für das Dateisystem, sondern verwendet stattdessen ein logisches Dateisystem. An der Spitze der Dateisystemstruktur liegt */*, das oft als *root* oder *Wurzel* des Dateisystems bezeichnet wird, so, als würde man einen auf dem Kopf stehenden Baum vor sich sehen (Abbildung 1.2). Beachten Sie jedoch, dass das nichts mit dem root-Benutzer zu tun hat. Diese Bezeichnungen mögen zunächst verwirrend sein, lassen sich aber leicht auseinanderhalten, wenn Sie sich erst einmal an Linux gewöhnt haben.

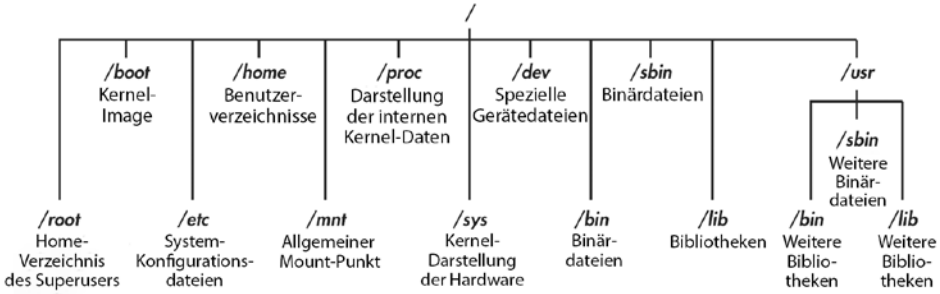

Abb. 1.2: Das Linux-Dateisystem

Die Wurzel (/) des Dateisystems befindet sich an der Spitze des Baums. Die im Folgenden aufgeführten Verzeichnisse sind die wichtigsten Unterverzeichnisse, die Sie kennen sollten:

- */root* – Das Home-Verzeichnis des allmächtigen root-Benutzers
- */etc* – Enthält im Allgemeinen die Linux-Konfigurationsdateien – Dateien, die kontrollieren, wann und wie Programme starten
- */home* – Das Home-Verzeichnis der Benutzerin oder des Benutzers
- */mnt* – Die Stelle, an der andere Dateisysteme an dieses Dateisystem angehängt bzw. »gemountet« sind
- */media* – Die Stelle, an der CD- und USB-Geräte normalerweise an das Dateisystem angehängt bzw. »gemountet« sind
- */bin* – Hier befinden sich die *Binärdateien* oder *Binaries* (diese sind äquivalent zu den ausführbaren Dateien in Windows oder den Anwendungen in macOS)
- */lib* – Die Stelle, an der Sie die *Bibliotheken* oder *Libraries* finden (gemeinsam genutzte Programme, die vergleichbar mit den Windows-DLLs sind)

Sie werden im Verlauf des Buchs noch eine Menge Zeit mit diesen wichtigen Verzeichnissen verbringen. Um von der Kommandozeile aus durch das Dateisystem navigieren zu können, ist es jedenfalls wichtig, diese Verzeichnisse zu verstehen.

Wichtig ist außerdem, dass Sie sich nicht als root anmelden sollten, wenn Sie einfach nur Routineaufgaben erledigen wollen, da jeder, der Ihr System hackt (ja, auch Hacker sind manchmal Opfer von Hackerangriffen), wenn Sie als root angemeldet sind, sofort root-Rechte erhält und damit Ihr System »besitzt«. Melden Sie sich als normaler Benutzer an, wenn Sie normale Anwendungen starten, im Web surfen, Tools wie Wireshark ausführen wollen usw. Für die Übungen, die Sie in diesem Buch durchführen, ist es in Ordnung, als root angemeldet zu bleiben.

1.3 Grundlegende Befehle unter Linux

Schauen Sie sich zu Beginn einige grundlegende Befehle an, die Ihnen helfen, den Einstieg unter Linux zu finden und loszulegen.

1.3.1 Sich selbst finden mit pwd

Anders als beim Arbeiten mit einer grafischen Oberfläche, einem sogenannten Graphical User Interface oder GUI, wie in Windows oder macOS, ist es auf der Kommandozeile unter Linux nicht immer offensichtlich, in welchem Verzeichnis Sie sich gerade befinden. Um zu einem neuen Verzeichnis zu navigieren, müssen Sie normalerweise wissen, wo Sie gerade sind. Der Befehl `pwd` zum Ausgeben des Arbeitsverzeichnisses (*print working directory*) liefert Ihnen Ihren momentanen Ort innerhalb der Verzeichnisstruktur zurück.

Geben Sie in Ihrem Terminal `pwd` ein um festzustellen, wo Sie sich gerade befinden:

```
kali> pwd
/home/kali
```

Linux gibt in diesem Fall `/home/kali` zurück und sagt mir damit, dass ich gerade im Verzeichnis des Benutzers *kali* bin. Da Sie sich beim Start von Linux ebenfalls als *kali* angemeldet haben, sollten Sie sich auch im Verzeichnis des Benutzers *kali* befinden, das zwei Ebenen unter der Wurzel der Dateisystemstruktur (`/`) liegt.

Sind Sie in einem anderen Verzeichnis, liefert `pwd` stattdessen diesen Verzeichnisnamen zurück.

1.3.2 Ihr Login mit whoami prüfen

Unter Linux wird der »allmächtige« Superuser oder Systemadministrator als root bezeichnet und besitzt alle Systemberechtigungen, um Benutzer anzulegen, Passwörter zu ändern, Berechtigungen zu ändern usw. Natürlich wollen Sie nicht, dass jede beliebige Person das Recht hat, solche Änderungen vorzunehmen – es soll jemand sein, der vertrauenswürdig ist und sich mit dem Betriebssystem angemessen auskennt. Als Hacker müssen Sie normalerweise all diese Rechte haben, um die notwendigen Programme und Tools auszuführen (viele Hacker-Tools funktionieren nur, wenn Sie root-Rechte haben), sodass Sie sich als root anmelden sollten.

Falls Sie vergessen haben, ob Sie als root oder als ein anderer Benutzer angemeldet sind, können Sie mit dem Befehl `whoami` herausfinden, wer Sie sind:

```
kali> whoami
kali
```

Wäre ich als ein anderer Benutzer angemeldet gewesen, z.B. mit meinem persönlichen Zugang, hätte `whoami` stattdessen meinen Benutzernamen zurückgeliefert:

```
kali> whoami
OTW
```

Denken Sie außerdem daran, und ja, man kann das nicht oft genug sagen, dass Sie sich nicht als root anmelden sollten, wenn Sie nur Routineaufgaben ausführen, da ansonsten jeder, der Ihr System hackt (ja, auch Hacker werden manchmal gehackt), sonst automatisch root-Rechte erhält.

1.3.3 Durch das Linux-Dateisystem navigieren

Das Navigieren des Linux-Dateisystems vom Terminal aus ist eine ausgesprochen wichtige Linux-Fertigkeit. Um irgendetwas tun zu können, müssen Sie in der Lage sein, sich durch die Dateistruktur zu bewegen, um Anwendungen, Dateien und Verzeichnisse zu finden, die in anderen Verzeichnissen liegen. In einem grafischen System können Sie die Verzeichnisse sehen, doch in einer Kommandozeilenschnittstelle ist die Struktur vollkommen textbasiert und Sie brauchen Befehle, um durch das Dateisystem zu navigieren.

Verzeichnisse wechseln mit cd

Um vom Terminal aus Verzeichnisse zu wechseln, verwenden Sie den Befehl `cd` (für *change directory*). So wechseln Sie z.B. in das Verzeichnis */etc*, in dem sich Konfigurationsdateien befinden:

```
kali> cd /etc
kali:/etc>
```

Der Prompt ändert sich zu `kali:/etc`, wodurch signalisiert wird, dass Sie nun im Verzeichnis */etc* sind. Sie können dies bestätigen, indem Sie `pwd` eingeben:

```
kali:/etc> pwd
/etc
```

Um sich in der Dateistruktur eine Ebene nach oben zu bewegen (in Richtung der Wurzel der Dateistruktur oder */*), verwenden Sie `cd`, gefolgt von zwei Punkten (`..`):

```
kali:/etc> cd ..
kali> pwd
/
```

Dies bringt Sie eine Ebene nach oben von */etc* in das Wurzelverzeichnis (/). Sie können so viele Ebenen nach oben gehen, wie Sie wollen. Verwenden Sie dazu einfach so viele Punkte-Paare, wie Sie Ebenen hinaufwandern wollen:

- Mit `..` gehen Sie eine Ebene nach oben.
- Mit `../..` bewegen Sie sich zwei Ebenen nach oben.
- Mit `../../..` würden Sie drei Ebenen nach oben wandern usw.

Um z.B. zwei Ebenen nach oben zu gehen, geben Sie cd ein, gefolgt von zwei Gruppen aus doppelten Punkten, die durch einen Schrägstrich getrennt sind:

```
kali> cd ../..
```

Sie können sich außerdem von einer beliebigen Stelle in die Wurzelebene begeben, indem Sie `cd /` eintippen, wobei / die Wurzel des Dateisystems repräsentiert.

Den Inhalt eines Verzeichnisses mit ls auflisten

Um den Inhalt eines Verzeichnisses (die Dateien und Unterverzeichnisse) zu sehen, benutzen Sie den Befehl `ls` (*list*). Das ist vergleichbar mit dem `dir`-Befehl in Windows.

```
kali> ls
Debian              Music              usr
Desktop             Picture            Videos
Documents           Public
Downloads           Templates
```

Dieser Befehl listet sowohl die Dateien als auch die Verzeichnisse auf, die in diesem Verzeichnis enthalten sind. Sie können den Befehl auch bei einem ganz bestimmten Verzeichnis einsetzen, also nicht nur an dem, in dem Sie sich gerade befinden. Dazu geben Sie nach dem Befehl den entsprechenden Verzeichnisnamen an. So zeigt z.B. `ls /etc` den Inhalt des */etc*-Verzeichnisses an.

Um weitere Informationen über die Dateien und Verzeichnisse zu bekommen, wie etwa ihre Zugriffsberechtigungen, Eigentümer, Größen und Daten der letzten Änderung, setzen Sie hinter den Befehl `ls` den Schalter (auch *Flag* genannt) `-l` (für *long*). Oft wird dies als *langes Listing* bezeichnet. Versuchen Sie es einmal:

```
kali> ls -l
total 32
drw-r--r-- 1   kali kali 4096 Dec 5 11:15 Debian
drw-r--r-- 2   kali kali 4096 Dec 5 11:15 Desktop
drw-r--r-- 3   kali kali 4096 Dec 9 13:10 Documents
```

```
drw-r--r-- 18   kali kali 4096 Dec 9 13:43 Downloads
--schnippschnapp--
drw-r--r-- 1    kali kali 4096 Dec 5 11:15 Videos
```

Wie Sie sehen, liefert `ls -l` Ihnen bedeutend mehr Informationen, wie etwa, ob ein Objekt eine Datei oder ein Verzeichnis ist, die Anzahl der Links, den Eigentümer, die Gruppe, seine Größe, wann es erzeugt oder modifiziert wurde sowie seinen Namen.

Ich nutze den Schalter `-l` eigentlich immer, wenn ich ein Verzeichnis unter Linux auflisten lasse, aber das müssen Sie am Ende selbst für sich entscheiden. Sie werden in Kapitel 5 mehr über `ls` erfahren.

Manche Dateien unter Linux sind verborgen und lassen sich mit einem einfachen `ls` oder `ls -l` nicht auflisten. Um solche verborgenen Dateien anzeigen zu lassen, fügen Sie den Schalter `-a` hinzu:

```
kali> ls -la
```

Falls Sie eine Datei vermissen, die Sie eigentlich zu sehen erwarten, lohnt es sich, das Flag `a` einzusetzen. Sie können mehrere Flags miteinander kombinieren, wie Sie das hier mit `-la` gemacht haben, und müssen sie nicht einzeln als `-l -a` angeben.

1.3.4 Hilfe bekommen

Nahezu alle Befehle, Anwendungen oder Dienstprogramme haben unter Linux jeweils eigene Hilfedateien, in denen Sie Hinweise zur Benutzung erhalten. Falls ich z.B. Hilfe für die Verwendung des besten Wi-Fi-Cracking-Tools aircrack-ng bräuchte, könnte ich einfach den Befehl `aircrack-ng`, gefolgt vom Befehl `--help`, eingeben:

```
kali> aircrack-ng --help
```

Beachten Sie hier den doppelten Bindestrich. Die Konvention unter Linux besteht darin, einen doppelten Bindestrich (`--`) vor Optionen einzusetzen, die aus einem kompletten Wort bestehen, wie etwa `help`. Vor Optionen, die nur einen einzigen Buchstaben umfassen, wie `-h`, reicht ein einfacher Bindestrich (`-`).

Wenn Sie diesen Befehl eingeben, sollten Sie eine kurze Beschreibung des Tools sowie Hinweise zu seiner Benutzung erhalten. In manchen Fällen können Sie sowohl `-h` als auch `-?` verwenden, um zur Hilfedatei zu gelangen. Falls ich z.B. Hilfe

zur Benutzung des besten Portscanners nmap haben möchte, gebe ich Folgendes ein:

```
kali> nmap -h
```

Obwohl viele Anwendungen alle drei Optionen (`--help`, `-h` und `-?`) unterstützen, gibt es leider keine Garantie, dass das immer so ist. Sollte also eine der Optionen nicht funktionieren, versuchen Sie es mit einer der anderen.

1.3.5 Das Handbuch aufrufen

Neben der Hilfe besitzen die meisten Befehle und Anwendungen ein Handbuch (Manual Pages) mit weiteren Informationen, wie etwa einer Beschreibung und einer Synopsis des Befehls oder der Anwendung. Sie können sich eine der sogenannten *Manpages* anschauen, indem Sie vor dem Befehl, dem Dienstprogramm oder der Anwendung `man` angeben. Um z.B. die Manpage für aircrack-ng zu öffnen, geben Sie Folgendes ein:

```
kali> man aircrack-ng
NAME
        aircrack-ng - a 802.11 WEP / WPA-PSK key cracker
SYNOPSIS
        aircrack-ng [options] <.cap / .ivs file(s)>
DESCRIPTION
        aircrack-ng is an 802.11 WEP and WPA/WPA2-PSK key cracking program. It
        can recover the WEP key once enough encrypted packets have been
        captured with airodump-ng. This part of the aircrack-ng suite
        determines the WEP key using two fundamental methods. The first method
        is via the PTW approach (Pyshkin, Tews, Weinmann). The main advantage
        of the PTW approach is that very few data packets are required to crack
        the WEP key. The second method is the FMS/KoreK method. The FMS/KoreK
        method incorporates various statistical attacks to discover the WEP
        key and uses these in combination with brute forcing. Additionally, the
        program offers a dictionary method for determining the WEP key. For
        cracking WPA/WPA2 pre-shared keys, a wordlist (file or stdin) or an
        airolib-ng has to be used.
```

Hier wird das Handbuch für aircrack-ng geöffnet, in dem Sie deutlich mehr Informationen finden als mit der Hilfe. Sie können mithilfe der Enter-Taste durch diese Handbuchdatei scrollen bzw. mit den Bild↑- und Bild↓-Tasten seitenweise blättern; aber auch die Pfeiltasten lassen sich verwenden. Um die Manpage zu verlassen, drücken Sie Q (für *quit*) und Sie gelangen wieder zurück zum Befehlsprompt.

Stichwortverzeichnis

Symbole

= (Zuweisungssymbol) 130
$-Zeichen 128
802.11 IEEE 75
& (Ampersand) 117
# (Hash-Zeichen) 136
.onion 198
#! (Shebang) 136
#-Symbol 251

A

Access List 183
Administrator 40
Advanced Packaging Tool (apt) 83
Ahmia 198
aircrack-ng 216
Ampersand (&) 117
AP (Access Point) 211
Apache-Webserver 180, 183
apt 83
apt-Paketmanager 83
Archivierung 150
  Overhead 151
Assoziatives Array 260
Asterisk 51
at 118
at-Daemon 119
Aufgabe
  automatisieren 235
  Backup 238
Aufklärung 260

B

Banner Grabbing 256
bash 40, 41, 121, 133
  als Standard-Shell 133
  Befehle 146
bash-Interpreter 136, 139
bash-Shell-Skript 133
Befehl 43
Benutzer
  anzeigen 44
  Gruppen 95
  root 95
Benutzer-ID setzen 105
Berechtigung 96
  ändern 99
  ausführen 96, 137
  Benutzer-ID 105
  chown 96
  Datei 98
  Dezimalnotation 99
  Gruppe 99, 105
  Gruppen-ID 105
  lesen 96
  Oktalnotation 99
  root-Benutzer 105
  root-Rechte 102
  schreiben 96
  Sticky Bit 105, 106
  überprüfen 97
  UGO-Syntax 101
  umask-Methode 104
Berkeley Internet Name Domain 79
Betriebssystem 225
bg 117

Bibliothek 42
Binärdatei 39
  suchen 49
BIND 79
BIOS 30
Black-Hat-Hacker 140
blockorientierte Geräte 161
Bluetooth 211, 219
  Bereitschaftsmodus 219, 221
  BlueZ 220
  Ericsson 219
  Frequenzsprungverfahren 219
  Harald I. »Blauzahn« Gormsson 219
  Nahfeldkommunikation 219
  Pairing 219
  Ping 223
  Scannen 221
  Service Discovery Protocol (SDP) 222
BlueZ 220
  sdptool 222
Booten 164
Bootloader 33
Bourne-Again-SHell (BASH) 121
Broadcast-Adresse 72, 76
BSSID (Basic Service Set Identifier) 211
bunzip2 153
bzip2 152, 153

C

Case Sensitivity 39
cat 53, 59
cd 44
CERN 208
Chaining
  dynamisches 204
  zufälliges 204
ChatGPT 270
chgrp 97
chmod 99, 137, 139, 143, 258
chown 96
Claude 2 (Anthropic) 271
CLI 40
Command Line Interface 40
compress 152, 154
Computer Emergency Response Team (CERT) 141
Computer-Forensik 154
Content-Management-System 187
Copilot (Microsoft) 270
cp 55
CPU 24
cron 235
crond-Daemon 118
crontab 235, 236
  Kürzel 240
cron-Tabelle 235
Cross-Site-Scripting (XSS) 180
C-Shell 133
Cyberkrieg 22
Cybersicherheit 269
  Cyber Threat Intelligence 271
  Social Engineering 272
Cyberspionage 22
Cyber Threat Intelligence 271

D

Daemon 77
  dhcpd 77
Darknet 198
  Ahmia 198
Datei
  anzeigen 59
  Beginn anzeigen 60
  Berechtigung 95, 137
  Bit-für-Bit-Kopie 154
  crontab 236, 238, 240
  Dateimanagement 157
  durchsuchen 67
  Eigentümerschaft 96
  Ende anzeigen 61
  entfernen 56
  erzeugen 53, 54

filtern 67
gelöschte wiederherstellen 154
Inhalt anzeigen 53
Inhalt filtern 63
komprimieren 152
kopieren 55
seitenweise anzeigen 66
umbenennen 55
verborgene 46
Zeilennummern 62
Dateimanagement 157
Dateisystem 41, 157
Baumstruktur 157
device (Gerät) 157
Geräteverzeichnis 157
Laufwerk 157
logisches 41
navigieren 44
Speichergerät 157
überwachen 164
Wurzel 41
Dateisystemprüfung 165
Dateityp 98
Datenbank
Datentyp 193
relationale 188
Schlüssel 193
dd 154
Debian 24, 88
Denial-of-Service-Angriff 75
dev 157
device (Gerät) 157
df 164
dhclient 77
dhcpd 77
DHCP-Daemon 77
DHCP-Server 77
Dictionary 260
Dictionary Attack 64
Dienst 179
neu starten 179, 180
starten 179
stoppen 179
Syntax zum Verwalten 179
dig 78
Directory 40
Diskettenlaufwerk 159
DNS 71, 78, 180
DNS-Server 79
Domainname 31, 80
Domain Name System 78, 180

E

echo 135, 136, 139
Eigentümer 96
Eingabe 138
emacs 136
E-Mail
verschlüsselte 207
env 123
ESSID 211, 215
eth0 72
Ethernet 72
Ethisches Hacking 21
exFAT-Dateisystem 161
export 125
ExpressVPN 207
ext 161

F

FAT-Dateisystem 161
fdisk 160
Festplatte 158, 159
Partition 32
virtuelle 160
fg 118
find 49
Flag 45
Frequenzsprungverfahren 219
fsck 165

G

gedit 136
Gemini (Google) 270

Gerät
Fehlerprüfung 165
Mount-Punkt 163
unmounten 164
Geräteverzeichnis 157
git 83, 92
GitHub 92
GPL (GNU General Public License) 187
Grand Unified Bootloader 33
Gray-Hat-Hacker 140, 141
grep 51, 63, 74, 111
Grok (X) 270
GRUB 33
Gruppe
Eigentümerschaft 97
root 96, 97
Gruppen-ID setzen 105
GUI 43
gunzip 153, 154
gzip 152

H

Hacking-Tool 23
Handbuch 47
Harald I. »Blauzahn« Gormsson 219
Hash-Wert 190
Hash-Zeichen (#) 136
hciconfig 220
hcidump 220
hcitool 220, 221
head 60
Hilfe 46
Hintergrundprozess 118
HISTSIZE 124
Hochgewinnantenne 214
Home 40
Hostname 31
hosts-Datei 81
HPFS-Dateisystem 161
HTTP-Server 180
Hyper-V 30

I

ID 110
IEEE 802.11 211
ifconfig 71, 75, 142, 185, 212
Image 28
initd 241
Installationsmanager 83, 89
Gdebi 89
Synaptic 89
Internet
Aktivitäten 195
Anonymität 195, 199
Hop (Router-Durchläufe) 196
Interpreter 136
IP-Adresse 37, 71, 75, 195, 196
ändern 75
eigene zuordnen 81
hosts-Datei 81
Scan 142
ipconfig 142
iwconfig 74, 213
iwlist 213, 214

J

Job-Scheduling 235, 239
Backup 238
cron 235
cron-Tabelle 235
MySQLscanner 239
rcconf 243
rc.d-Skript 242
rc-Skript 241
journalctl 170, 173, 175, 176

K

Kali Linux
einrichten 30
herunterladen 23
installieren 28
kali-tweaks 133
kate 136

Kernel 24, 225
Kernel-Log 174
Kernel-Modul 226
  entfernen 232
  hinzufügen 232
  insmod-Suite 230
  modinfo 231
  modprobe 230, 231
  Modulabhängigkeiten 231
  verwalten 230
Kernel-Tuning 227
KI 269
  bash-Skripting 274
  Claude 2 (Anthropic) 271
  Copilot (Microsoft) 270
  Cybersicherheit 269
  Cyber Threat Intelligence 271
  Einschränkungen 269
  Gemini (Google) 270
  Grok (X) 270
  Llama (Meta) 271
  Perplexity (Perplexity AI) 271
  Routineaufgaben automatisieren 269
  Social Engineering 272
kill 115
Klasse 249
Kommandozeilenschnittstelle 41
Kommentar 136
Komprimierung 149
  Datei 152
  gzip 152
  verlustbehaftete 149
  verlustfreie 149, 150
Konfigurationsdatei 42, 59
  entfernen 85
Kontrollanweisung 260
Korn-Shell 133
Künstliche Intelligenz 269

L

l2ping 223
LAMP 180
LAN 73
Langes Listing 45
Laufwerk
  mounten 157, 163
  Partitionen 159
less 67
Library 42
Linux 22
  Betriebssystem 225
  Runlevel 241
Linux-Kernel 110, 174, 225
  Dateisystemtreiber 226
  Gerätetreiber 226
  Kernel-Modul 226
  Kernel-Tuning 227
  Kernel-Version prüfen 227
  ladbare Kernel-Module 226
  modprobe 231
  Modulabhängigkeiten 231
  sysctl 227
  Systemerweiterung 226
Linux-Runlevel 241
LKM 226, 231
Llama (Meta) 271
Localhost 72, 190
locate 48
Log-Datei 169, 171
  apache2-Webserver 172
  deaktivieren 176
  Facility 171
  Priorität 171
  schreddern 176
Loopback-Adresse 72
ls 45
lsblk 162
ls -l 97
lsusb 162

M

Mac 26
MAC-Adresse 37, 72, 76
  ändern 76
  fälschen 76
Mail Exchange Server 79
Mailserver 78
Mailsystem 79
Major Number 159
Malware
  Rootkit 226
Man-in-the-Middle-Angriff (MITM) 225, 228
Manpage 47
Manual Page 47
MariaDB 187
  starten 188
Metasploit 64, 69, 111
Mirror 33
mkdir 54
Mobilgerät 25
modinfo 231
modprobe 231
more 66
mount 163
Mounten 157
Mount-Punkt 162, 163
mousepad 136
Munging 65
mv 55
MySQL 142, 180, 187
  entfernte Datenbank ansprechen 191
  Kommandozeilenschnittstelle 191
  mit Datenbank verbinden 191
  Passwort 188, 189
  starten 188
  Tabellen 192
  Wildcard 194
MySQL-Scanner 143

N

Nahfeldkommunikation 219
Nameserver 78, 80
netstat 73
Network Interface Card (NIC) 72
Network Manager Command Line Interface 214
Netzwerk 71, 211
  analysieren 71
  Bluetooth 211, 219
  drahtloses 74, 211
  Socket 257
  Typ 72
  Wi-Fi 211
Netzwerkkarte 213
Netzwerkmanager 214
Netzwerkmaske 72
nice 113
nl 62
nmap 140, 142, 200
  Syntax 140
nmcli 214
NordVPN 207
NSA (National Security Agency) 195
  Tor 199
  Traffic Correlation 199
NTFS-Dateisystem 161

O

Objektorientierte Programmierung (OOP)
  Klasse 255
  Methoden 255, 257
  Objekt 255
  Python 254
Offensive Security 24
Onion-Netzwerk 195
ONR (US Office of Naval Research) 197
OOP 254
OpenAI 270
Open Source 22, 187

OpenSSH 183
Option 46
Oracle 25
Ordner 40

P

Paket 196
Paketweiterleitung 228
Partition 32
Partitionen 159
  Minor Number 159
Passwort
  knacken 69
PATH-Variable 49
  Verzeichnis hinzufügen 128
Penetrationstest 21
Perplexity (Perplexity AI) 271
Physische Kopie eines Speichergeräts 154
PIA 207
PID 110
ping 37
Pipe 52, 64
Pipeline 52
pip (Pip Installs Packages) 246
Portscan 140, 142
PowerShell 36
Preshared Key 212
Private verschlüsselte E-Mail 195
Promiscuous-Modus 75
Protokolldatei 169
Protokollsystem 170
ProtonMail 207
ProtonVPN 207
proxychains 200, 201, 203
  zufälliges Chaining 204
Proxy-Server 195, 199
  Anonymität 199
  dynamisches Chaining 204
  Sicherheit 206
  zufälliges Chaining 204
Prozess 109
  anzeigen 109
  auflisten 110
  beenden 115
  bg 117
  fg 118
  filtern 111
  im Hintergrund ausführen 117
  in den Vordergrund holen 118
  nice 113
  PID 110
  Priorität 113, 114
  Prozess-ID 110
  Ressourcen 112
  top 112
  verwalten 109, 113
  zeitlich planen 118
  Zombie-Prozess 115
ps 52, 109
PS1 125, 127
pwd 43
PyCharm 247
PyPI (Python Package Index) 246
Python 40, 245
  Anführungszeichen 251
  Array 253
  Dictionary 250, 260
  Dokumentation 253
  Einrückung 261
  Exception Handling 246, 265
  Formatierung 248
  for-Schleife 262
  Funktionen 252
  IDE 247
  if-Anweisung 261
  if...else-Struktur 261
  Index 253
  Interpreter 249
  Klasse 249
  Kommentare 251
  Kontrollanweisung 260

Kontrollblock 261
Kontrollstruktur 261
Listen 253
Methoden 257
Modul 254
Module hinzufügen 245
Netzwerkkommunikation 256
objektorientierte Programmierung (OOP) 254
Passwort-Cracker 260, 265
pip (Pip Installs Packages) 246
PyCharm 247
PyPI (Python Package Index) 246
Schleife 262
Skript 249
socket-Modul 256
Standardbibliotheken 245
#-Symbol 251
TCP-Client 256
TCP-Listener 258
try/except-Struktur 265
Variable 248
Variablentyp 249
while-Schleife 262

R

Raspberry Pi 25, 184
IP-Adresse 185
Kameramodul 185, 186
Raspberry Pi OS 184
Raspberry-Pi-Spion 185, 186
Raspbian 186
rcconf 243
rc.d-Skript 242
rc-Skript 241
read 135
Rechteeskalation 106
renice 113, 114
Repository 83, 87
hinzufügen 88
Ressource 112
rm 56
root 32, 40, 157
root-Benutzer 95
Benutzer-ID 173
root (Dateisystem) 41
Rootkit 226
root-Recht 102

S

Sammeln von Informationen 260
Schalter 45
Scheduling 235
Schleife 260
Schlüsselwort
suchen 51
Schwachstellenanalyse 21
Secure Shell 183
sed 64
Service Discovery Protocol (SDP) 222
set 124
SGID 105
Shebang 136
Shell 40, 41, 117, 121, 133
bash 133
bash-Shell-Interpreter 136
bash-Shell-Skript 133
Bourne-Again-SHell (BASH) 121
Korn-Shell 133
Prompt 126
Shell-Prompt ändern 126
Standard-Shell 121
Variable 121
zsh 121
Z-Shell 121
Shodan.io 258
shred 175
Skript 40, 133
ausführen 137
Benutzereingaben 138
Kommentar 136, 251
Passwort-Cracker 260, 265
Python 245
Schleife 262

TCP-Listener 258
Variable 138
Social Engineering 272
Software 83
aktualisieren 86
apt-Paketmanager 83
entfernen 83, 85
git 83, 92
hinzufügen 84
Installationsmanager 83, 89
installieren 83
Repository 83, 87
Softwarepaket 83
Update 86
Upgrade 86, 87
Software-Repository 87
sources.list 87
Speichergerät 157
Speichermanagement 157
Sprache 31
Spur verwischen 174, 176
Spyder 247
SQL 188
Befehle 188
ss 73
SSH 183, 184, 258
SSID 211, 215
Standardberechtigung 104
Standard-Shell 121
Sticky Bit 106
setzen 105
Stream 64
String 138
Suche 48
in Verzeichnis 50
Wildcard 51
Suchen und Ersetzen 64
sudo 76
SUID 105, 106
Superuser 40
SurfShark 207
Swap-Partition 160
sysctl 227
syslog-Daemon 169
Systemadministrator 32
System-Backup 238
systemd 169
Systemvariable 130

T

Tablet 25
tail 61
tar 150
Tarball 150
TCP-Connect-Scan 141
TCP-Scan 142
Terminal 40, 41, 121
Text
anzeigen 59
ersetzen 65
Textdatei 59
Texteditor 135
mousepad 136
The Onion Router 197
top 112, 114
Tor 197
Tor-Browser 198
Tor-Projekt 197
Torrent 25
touch 54
traceroute 196
Tracking-Methode 195
Traffic 197
Traffic Correlation 199

U

umask-Methode 104
Umgebungsvariable 121
export 125
HISTSIZE 125
löschen 130
manipulieren 123

PATH 128
PATH-Variable erweitern 128
set 124
Umleitung 53
doppelte 53
umount 164
uncompress 154
unset 130
Update 86
Upgrade 86
USB-Geräte 162
Userland 225
US Office of Naval Research (ONR) 197

V

Variable 121, 138, 248
benutzerdefinierte 130
Benutzerumgebung 121
Datentyp 250
definieren in Python 249
filtern 124
HISTSIZE 125
PATH 128
PATH-Variable erweitern 128
Shell-Variablen 121
Werte permanent ändern 125
Werte temporär ändern 125
VDI 27
Verschlüsselte E-Mail 207
Verzeichnis 40, 42
aktuelles Verzeichnis ausgeben 43
Berechtigung 95
entfernen 56
erzeugen 54
Geräteverzeichnis 157
Inhalt auflisten 45
navigieren 43
umbenennen 56
wechseln 44
vi 136
vim 136
VirtualBox 25
herunterladen 25
installieren 26
Virtuelle Maschine 25
anlegen 27
einrichten 26
Festplatte 27, 28
Kali installieren 28
RAM 27
Virtuelles privates Netzwerk 195, 206
VM 25
VPN 206

W

WAMP 181
Webserver 23, 179, 180
whereis 49
which 49
White-Hat-Hacker 140
whoami 43
Wi-Fi 211
Access-Point 211
Frequenz 212
IEEE 802.11 211
Kanäle (Channel) 212
Leistung (Power) 212
Modi (Modes) 212
Monitor-Modus 216
Passwort knacken 218
Reichweite 212
Sicherheit (Security) 212
Sicherheitsprotokoll 212
Wi-Fi-Modus 213
managed 213
master 213
monitor 213, 216
Wi-Fi-Sicherheitsprotokoll
Wi-Fi Protected Access (WPA) 212
Wired Equivalent Privacy (WEP) 212

WPA2-PSK 212
WPA3 212
Wi-Fi-Standard
802.11 IEEE 75
Wildcard 51, 153, 176, 194, 238
Windows 22
Windows Subsystem for Linux 24, 36
Wörterbuchangriff 64
WPA1 215
WPA2 215

Z

zeichenorientierte Geräte 161
Zeilennummer 62
leere Zeilen 63
zsh 121
Z-Shell 121, 133
zufälliges Chaining 204
Zuweisungssymbol (=) 130