

Linux-Basics für Hacker

Einstieg in die Hacking-Grundlagen mit Kali Linux:
Netzwerke, Scripting und Security

DAS INHALTS- VERZEICHNIS

» Hier geht's
direkt
zum Buch

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