

# linux hacker's guide

sicherheit für linux-server und -netze



anonymous

new technology

Markt&Technik Verlag

# Inhaltsverzeichnis

---

<b>Vorwort</b>	11
Die Struktur dieses Buchs	13
Querverweise in diesem Buch	13
Verwendung dieses Buchs	16
Verschiedenes	17
Zusammenfassung	18
<b>Kapitel 1 Einführung in Linux</b>	<b>19</b>
1.1 Was ist Linux?	20
1.2 Linux als Einzelplatzsystem	25
1.3 Linux als Intranet-/Internet-Server	26
1.4 Ein Überblick über Linux-Sicherheit	27
1.5 Zusammenfassung	35
<b>Kapitel 2 Physikalische Sicherheit</b>	<b>37</b>
2.1 Serverstandort und physikalischer Zugriff	38
2.2 Netzwerktopologie	41
2.3 Netzwerk-Hardware	46
2.4 Workstations und Sicherheit	50
2.5 Zusammenfassung	63
<b>Kapitel 3 Installation</b>	<b>65</b>
3.1 Sicherheit und Installation bei den unterschiedlichen Linux-Distributionen	66
3.2 Partitionen und Sicherheit	69
3.3 Auswahl von Netzwerkdiensten während der Installation	91
3.4 Bootloader	94
3.5 Zusammenfassung	97

<b>Kapitel 4</b>	<b>Grundlagen der Linux-Systemadministration</b>	99
4.1	Der Grundgedanke	100
4.2	Accounts einrichten und verwalten	102
4.3	Administrative Aufgaben mit su durchführen	112
4.4	Zugriffskontrolle	116
4.5	Zugriffsrechte und Eigentümer	116
4.6	Gruppen aus der Nähe betrachtet	128
4.7	Herunterfahren Ihres Systems	134
4.8	Zusammenfassung	135
<b>Kapitel 5</b>	<b>Passwortangriffe</b>	137
5.1	Was ist ein Passwortangriff?	138
5.2	Wie Linux Passwörter erzeugt und speichert	139
5.3	Der Data Encryption Standard (DES)	142
5.4	Fallstudie: Knacken von Linux-Passwörtern mit Hilfe eines Passwortangriffs	145
5.5	Passwort-Shadowing und die shadow-Suite	155
5.6	Nach der Installation der shadow-Suite	174
5.7	Weitere Gefahren für die Passwortsicherheit	179
5.8	Pluggable Authentication Modules (PAMs)	183
5.9	Weitere Anwendungen für die Passwortsicherheit	184
5:10	Zusammenfassung	186
<b>Kapitel 6</b>	<b>Bösartiger Code</b>	189
6.1	Was ist bössartiger Code?	190
6.2	Bösartigen Code aufspüren	196
6.3	Weitere Informationsquellen	212
6.4	Zusammenfassung	213
<b>Kapitel 7</b>	<b>Sniffer und elektronische Abhöreinrichtungen</b>	215
7.1	Die Arbeitsweise von Sniffern	216
7.2	Fallstudien: Durchführen ein paar einfacher Sniffer-Angriffe	218
7.3	Weitere Sniffer und Tools zur Netzwerk-Überwachung	232
7.4	Welche Gefahr stellen Sniffer dar?	235
7.5	Abwehr von Sniffer-Angriffen	237
7.6	Andere, allgemeinere Methoden zur Abwehr von Sniffern	240
7.7	Weitere Informationsquellen	241
7.8	Zusammenfassung	241

<b>Kapitel 8</b>	<b>Scanner</b>	243
8.1	Was ist ein Scanner?	244
8.2	Die Anatomie eines System-Scanners	245
8.3	Die Anatomie eines Netzwerk-Scanners	249
8.4	Scanner-Bausteine und die Weiterentwicklung der Scanner	253
8.5	SATAN (Security Administrator's Tool for Analyzing Networks)	255
8.6	Wie Scanner in Ihre Sicherheitsstrategie eingebunden werden können	264
8.7	Verschiedene Scanner-Tools	265
8.8	Sind Scanner legal?	283
8.9	Abwehr von Scanner-Angriffen	284
8.10	Weitere Informationsquellen	291
8.11	Zusammenfassung	292
<b>Kapitel 9</b>	<b>Spoofing</b>	293
9.1	Was ist Spoofing?	294
9.2	TCP- und IP-Spoofing	294
9.3	Fallstudie: Eine einfache Spoofing-Attacke	297
9.4	IP-Spoofing-Attacken abwehren	303
9.5	ARP-Spoofing	304
9.6	DNS-Spoofing	306
9.7	Andere ungewöhnliche Spoofing-Attacken	308
9.8	Weitere Informationsquellen	310
9.9	Zusammenfassung	311
<b>Kapitel 10</b>	<b>Schutz der Daten während der Übertragung</b>	313
10.1	Secure Shell (ssh)	314
10.2	Die grundlegenden ssh-Utilities	315
10.3	Schnelle Installation des ssh-Pakets	316
10.4	Nicht ganz so schnelle Installation: Festlegen der configure-Optionen	320
10.5	Konfiguration des ssh-Servers	322
10.6	ssh-Dienste in heterogenen Netzwerken anbieten	334
10.7	ssh-Sicherheitsprobleme	343
10.8	Weitere Informationsquellen	343
10.9	Zusammenfassung	344

<b>Kapitel 11</b>	<b>FTP-Sicherheit</b>	345
11.1	File Transfer Protocol	346
11.2	Die Sicherheitsvorgeschichte von FTP	346
11.3	Standard-Sicherheitsfunktionen von FTP	350
11.4	SSLftp	356
11.5	Sicherheit spezieller FTP-Anwendungen	358
11.6	Zusammenfassung	359
<b>Kapitel 12</b>	<b>Mail-Sicherheit</b>	361
12.1	SMTP-Server und -Clients	362
12.2	Grundlagen der sendmail-Sicherheit	368
12.3	sendmail durch Qmail ersetzen	384
<b>Kapitel 13</b>	<b>Telnet-Sicherheit</b>	391
13.1	Müssen Sie Telnet-Dienste anbieten?	392
13.2	Telnets Sicherheitsvorgeschichte	392
13.3	Sichere Telnetsysteme	394
13.4	Wichtige Dokumente	403
13.5	Zusammenfassung	404
<b>Kapitel 14</b>	<b>Sichere Webserver</b>	405
14.1	Entfernen nicht unbedingt notwendiger Dienste	406
14.2	Ihren Webserver sichern	416
14.3	Verzeichniszugriffskontrolle über Standard-HTTP-Authentifizierung hinzufügen	429
14.4	Eine chroot-Webumgebung einrichten	438
14.5	Akkreditierung und Zertifizierung	440
14.6	Zusammenfassung	442
<b>Kapitel 15</b>	<b>Sichere Protokolle</b>	443
15.1	Das Problem	444
15.2	Secure Sockets Layer Protocol (SSL) von Netscape Communications Corporation	444
15.3	Installation von Apache-SSL	449
15.4	Andere sichere Protokolle: IPSEC	469
15.5	Zusammenfassung	470

<b>Kapitel 16</b>	<b>Sichere Webentwicklung</b>	471
16.1	Risikofaktoren in der Webentwicklung: Ein kurzer Überblick	472
16.2	Shells aufrufen	472
16.3	Pufferüberläufe	482
16.4	Pfade, Verzeichnisse und Dateien	486
16.5	Andere interessante Sicherheitsprogrammier- und -Testtools	489
16.6	Andere Online-Informationsquellen	491
16.7	Zusammenfassung	491
<b>Kapitel 17</b>	<b>Denial-of-Service-Angriffe</b>	493
17.1	Was ist ein Denial-of-Service-Angriff?	495
17.2	Risiken durch Denial-of-Service-Angriffe	496
17.3	Aufbau dieses Kapitels	497
17.4	DoS-Angriffe gegen Hardware	497
17.5	Angriffe auf Linux-Netzwerke	502
17.6	Angriffe auf Linux-Applikationen	517
17.7	Andere DoS-Angriffe	520
17.8	Verteidigung gegen Denial-of-Service-Angriffe	523
17.9	Online-Informationsquellen	524
17.10	Zusammenfassung	525
<b>Kapitel 18</b>	<b>Linux und Firewalls</b>	527
18.1	Was ist eine Firewall?	528
18.2	Brauchen Sie wirklich eine Firewall?	532
18.3	tcpd: TCP Wrappers	533
18.4	ipfwadm	540
18.5	ipchains	544
18.6	Freie Firewall-Tools und Zusatzprogramme für Linux	546
18.7	Kommerzielle Firewalls	547
18.8	Zusätzliche Informationsquellen	550
18.9	Zusammenfassung	551
<b>Kapitel 19</b>	<b>Logs und Audit-Trails</b>	553
19.1	Was genau ist Logging?	554
19.2	Logging unter Linux	555
19.3	Andere interessante Logging- und Audit-Tools	575
19.4	Zusammenfassung	579

<b>Kapitel 20</b>	<b>Einbruchserkennung</b>	581
20.1	Was ist Einbruchserkennung?	582
20.2	Grundlegende Einbruchserkennungskonzepte	583
20.3	Einige interessante Einbruchserkennungssysteme	585
20.4	Dokumente über Einbruchserkennung	595
<b>Kapitel 21</b>	<b>Disaster Recovery – Wiederherstellung nach Katastrophen</b>	597
21.1	Was ist Disaster Recovery?	598
21.2	Dinge, die Sie vor dem Aufbau Ihres Linux-Netzwerks beachten sollten	598
21.3	Ihre Backup-Tools wählen	602
21.4	Einfache Archivierung Ihrer Dateien und Verzeichnisse über tar und gzip	603
21.5	Arten von Backups und Backup-Strategien	607
21.6	Backup-Pakete	611
21.7	Sonstiges	614
21.8	Zusammenfassung	615
	<b>Anhang A</b>	617
A.1	Sicherheitsrelevante Linux-Befehle	618
	<b>Anhang B</b>	651
B.1	Linux-Sicherheitsindex – ältere Linux-Sicherheitsprobleme	652
B.2	Zusammenfassung	668
	<b>Anhang C</b>	669
C.1	Andere nützliche Linux-Sicherheitstools	670
	<b>Anhang D</b>	695
D.1	Informationsquellen	696
	<b>Anhang E</b>	729
	<b>Stichwortverzeichnis</b>	785