

Linux-Firewalls mit iptables & Co.

open source library

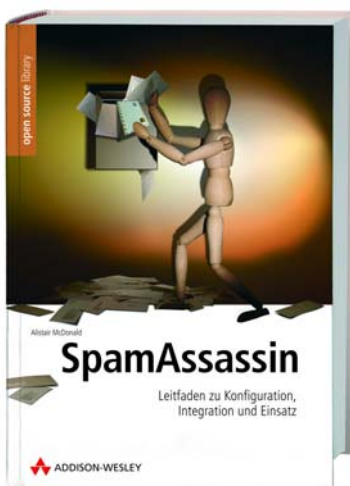
Open Source Software wird gegenüber kommerziellen Lösungen immer wichtiger. Addison-Wesley trägt dieser Entwicklung Rechnung mit den Büchern der **Open Source Library**. Administratoren, Entwickler und User erhalten hier professionelles Know-how, um freie Software effizient einzusetzen. Behandelt werden sowohl Themen wie Betriebssysteme, Netzwerke und Sicherheit als auch Programmierung.

Eine Auswahl aus unserem Programm:



Dieses Buch zeigt, wie mit den Bordmitteln jeder Linux-Distribution – z. B. Snort 2.0 – auf einem Linux-Server ein professionelles System zur Einbruchserkennung und -Verhinderung aufgesetzt wird. Der Autor erläutert die Anwendung von IDS auf komplexe Netzwerke, beschreibt die Arbeit mit den wichtigsten Tools (Tripwire und Snort) zur System- und Netzwerküberwachung, schildert ausführlich die Analyse der gewonnenen Daten sowie ihre Interpretation und gibt Richtlinien für die Prävention und die richtige Reaktion im Ernstfall. Er beschreibt außerdem die technischen und formalen Voraussetzungen für den Einsatz eines IDS, zeigt Grenzen auf und warnt vor juristischen Fallstricken.

Ralf Spennberg
Intrusion Detection und Prevention mit Snort 2 & Co
ISBN-13: 978-3-8273-2134-3
ISBN-10: 3-8273-2134-4
840 Seiten
Euro 59,95 (D), 61,70 (A)



Dieses Buch beschreibt fokussiert und übersichtlich, wie SpamAssassin auf- und eingesetzt wird, um Spam erfolgreich abzuwehren. Der Autor schafft mit der Beschreibung verschiedener Abwehr-Verfahren zunächst die theoretischen Grundlagen, bevor er detailliert deren Umsetzung mit SpamAssassin beschreibt. Von der Zusammenarbeit mit verschiedenen Mailservern wie sendmail, qmail, postfix und exim über die dynamische Optimierung der Filter bis hin zu Performancefragen werden alle Aspekte der SpamAssassin-Praxis behandelt.

Alistair McDonald
SpamAssassin
ISBN-13: 978-3-8273-2205-0
ISBN-10: 3-8273-2205-7
288 Seiten
Euro 39,95 (D), 41,10 (A)

Ralf Spenneberg

Linux-Firewalls mit iptables & Co.

Sicherheit mit Kernel 2.4 und 2.6
für Linux-Server und -Netzwerke



 ADDISON-WESLEY

An imprint of Pearson Education

München • Boston • San Francisco • Harlow, England
Don Mills, Ontario • Sydney • Mexico City
Madrid • Amsterdam

Die Deutsche Bibliothek – CIP-Einheitsaufnahme

Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.ddb.de> abrufbar.

Die Informationen in diesem Produkt werden ohne Rücksicht auf einen eventuellen Patentschutz veröffentlicht.

Warennamen werden ohne Gewährleistung der freien Verwendbarkeit benutzt.

Bei der Zusammenstellung von Texten und Abbildungen wurde mit größter Sorgfalt vorgegangen. Trotzdem können Fehler nicht ausgeschlossen werden.

Verlag, Herausgeber und Autoren können für fehlerhafte Angaben und deren Folgen weder eine juristische Verantwortung noch irgendeine Haftung übernehmen.

Für Verbesserungsvorschläge und Hinweise auf Fehler sind Verlag und Herausgeber dankbar.

Alle Rechte vorbehalten, auch die der fotomechanischen Wiedergabe und der Speicherung in elektronischen Medien.

Die gewerbliche Nutzung der in diesem Produkt gezeigten Modelle und Arbeiten ist nicht zulässig.

Fast alle Hardware- und Softwarebezeichnungen und weitere Stichworte und sonstige Angaben, die in diesem Buch verwendet werden, sind als eingetragene Marken geschützt.

Da es nicht möglich ist, in allen Fällen zeitnah zu ermitteln,

ob ein Markenschutz besteht, wird das ® Symbol in diesem Buch nicht verwendet.

Umwelthinweis:

Dieses Produkt wurde auf chlorfrei gebleichtem Papier gedruckt.

10 9 8 7 6 5 4 3 2 1

08 07 06

ISBN-13: 978-3-8273-2136-7

ISBN-10: 3-8273-2136-0

© 2006 by Addison-Wesley Verlag,
ein Imprint der Pearson Education Deutschland GmbH,
Martin-Kollar-Straße 10–12, D-81829 München/Germany
Alle Rechte vorbehalten

Einbandgestaltung: Marco Lindenbeck, webwo GmbH (mlindenbeck@webwo.de)

Lektorat: Boris Karnikowski, bkarnikowski@pearson.de

Korrektorat: Friederike Daenecke, Zülpich

Fachkorrektorat: Wilhelm Dolle, Berlin

Herstellung: Monika Weiher, mweiher@pearson.de

Satz: LE-TeX Jelonek, Schmidt & Vöckler GbR, Leipzig

Druck und Verarbeitung: Kösel, Krugzell (www.KoeselBuch.de)

Printed in Germany

Für Claudia
Ich Dich auch ;-)

Inhaltsübersicht

Vorwort	31
Einleitung	33
Teil I Firewall-Grundlagen	35
1 Firewall-Geschichte	37
2 Firewall-Technologien	41
3 Firewall-Architekturen	45
4 Bedrohungen bei der Vernetzung von Systemen	51
Teil II Firewalls mit Iptables – Einführung	79
5 Eine einfache Firewall mit Iptables	81
6 Härtung eines Linux-Systems	143
7 Intrusion-Detection- und -Prevention-Systeme	165
Teil III Typische Firewall-Konfigurationen	169
8 Eine lokale Firewall	171
9 Aufbau einer DMZ	185
Teil IV Werkzeuge	213
10 Zentrale Protokollserver	215
11 Zentrale Zeitsynchronisation	241

12	Protokollanalyse	251
13	Administrationsoberflächen	273
14	Distributionswerkzeuge	297
15	Testmethoden und -werkzeuge	319
Teil V Fortgeschrittene Konfiguration		357
16	Die Iptables-Standardtests	359
17	Alle Standardziele	375
18	Patch-O-Matic	383
19	Connection Tracking	401
20	Die NAT-Tabelle	411
21	Die Mangle-Tabelle	421
22	Die Raw-Tabelle	425
23	Das /proc-Dateisystem	427
24	Fortgeschrittene Protokollierung	451
25	Ipset	461
26	Hochverfügbare Firewalls	469
27	Nfnetlink und Kernel 2.6.14	489
28	nf-HiPAC	493

Teil VI Transparente Firewalls	495
29 ProxyARP	497
30 Iptables auf einer Bridge	501
31 Ebttables	507
Teil VII Protokolle und Applikationen	519
32 Behandlung einzelner Protokolle	521
33 IPsec	559
34 ICMP	569
35 IPv6	587
A Postfix-E-Mail-Relay	591
B Firewall-Skript	595
C Netzwerkgrundlagen	599
Literaturverzeichnis	629
Stichwortverzeichnis	631
Über den Autor	643

Inhaltsverzeichnis

Vorwort	31
Einleitung	33
I Firewall-Grundlagen	35
1 Firewall-Geschichte	37
1.1 Der Anfang des Internets	37
1.2 Der Morris-Wurm	38
1.3 Die erste Firewall	38
1.4 Firewalls heute	39
2 Firewall-Technologien	41
2.1 Paketfilter	41
2.2 Zustandsorientierte Paketfilter	42
2.3 Circuit Relay	42
2.4 Application-Level-Gateway (Proxy)	43
2.5 Network Address Translation	43
3 Firewall-Architekturen	45
3.1 Screening-Router	45
3.2 DMZ	46
3.3 Multiple DMZ	48
3.4 Wahl der Architektur	48
4 Bedrohungen bei der Vernetzung von Systemen	51
4.1 Angreifer und Motivation	51
4.1.1 Der klassische Hacker	51
4.1.2 Script-Kiddies	52
4.1.3 Insider	52
4.1.4 Mitbewerber	53

4.1.5	Geheimdienste	53
4.1.6	Terroristen und organisierte Kriminalität	53
4.2	Tendenzen und Entwicklungen	54
4.3	Schutzziele	55
4.4	Angriffsmethoden	57
4.4.1	Denial-of-Service (DoS)	58
4.4.2	Spoofing	59
4.4.3	Session Hijacking	64
4.4.4	Bufferoverflow	66
4.4.5	Formatstring-Angriffe	70
4.4.6	Race-Condition	71
4.4.7	SQL-Injektion	75
4.4.8	Welchen Schutz bietet eine Firewall?	77
II Firewalls mit Iptables – Einführung		79
5	Eine einfache Firewall mit Iptables	81
5.1	Netfilter und Iptables	81
5.2	Der Iptables-Befehl und die Filter-Tabelle	82
5.3	Ihr erstes Firewall-Skript	89
5.3.1	Fehlersuche	98
5.4	Einbindung in den Boot-Prozess	100
5.5	Connection Tracking und Netzwerkverbindungen	102
5.5.1	Der zustandslose Paketfilter IPchains	102
5.5.2	IPchains und UDP	103
5.5.3	IPchains und TCP	105
5.5.4	IPchains und ICMP	109
5.5.5	IPchains und Masquerading	110
5.5.6	Iptables und Contrack	110
5.6	Filter-Regeln	119
5.7	Die NAT-Tabelle und -Regeln	121

- 5.7.1 Source-NAT 122
- 5.7.2 Destination-NAT 126
- 5.7.3 NAT-Beispiel 127
- 5.8 Die Mangle-Tabelle 131
- 5.9 Die Raw-Tabelle 132
- 5.10 Einstellungen des Kernels 133
- 5.11 Protokollierung 136
- 5.12 Test der Firewall 139
- 6 Härtung eines Linux-Systems 143**
 - 6.1 Warum sollte eine Firewall gehärtet werden? 143
 - 6.2 Installation des Linux-Systems 144
 - 6.3 Updates 146
 - 6.3.1 Debian-Updates 147
 - 6.3.2 SUSE-Updates 147
 - 6.3.3 Red Hat-Updates 147
 - 6.3.4 Fedora Core-Updates 147
 - 6.4 Deaktivieren überflüssiger Dienste 147
 - 6.4.1 Startskripten 149
 - 6.4.2 Internet-Super-Server 149
 - 6.4.3 Cron-Daemon 150
 - 6.5 Entfernen überflüssiger Software 151
 - 6.6 Sicherheit auf Dateisystemebene 152
 - 6.7 Sicherheit beim Bootvorgang 154
 - 6.8 Bastille-Linux 155
 - 6.9 Mandatory-Access-Control-Systeme (MAC) 161
- 7 Intrusion-Detection- und -Prevention-Systeme 165**
 - 7.1 Intrusion-Detection-Systeme 165
 - 7.2 Intrusion-Prevention-Systeme 167

III	Typische Firewall-Konfigurationen	169
8	Eine lokale Firewall	171
8.1	Wieso eine lokale Firewall?	171
8.2	Die Ketten	173
8.3	Der Owner-Match	178
8.4	Kombination mit Gateway-Regeln	181
9	Aufbau einer DMZ	185
9.1	DMZ-Architekturen	185
9.2	Dreibeiniger Paketfilter mit DMZ	186
9.3	Optimierung mit benutzerdefinierten Ketten	195
9.3.1	Anwendung der benutzerdefinierten Ketten	199
9.4	DMZ mit zwei Paketfiltern	204
9.4.1	Der äußere Paketfilter	206
9.4.2	Der innere Paketfilter	209
IV	Werkzeuge	213
10	Zentrale Protokollserver	215
10.1	Einrichtung eines zentralen Protokollservers	215
10.2	Modular Syslog	219
10.2.1	Installation des Msyslogd	220
10.2.2	Konfiguration von <i>msyslogd</i>	220
10.3	Syslog-ng	228
11	Zentrale Zeitsynchronisation	241
11.1	Das Zeitsynchronisationsprotokoll NTP	241
11.2	Der ntpd-Zeitserver	242
11.2.1	Der Client	242
11.2.2	Der Server	245
11.3	Sicherheit	245
11.3.1	Symmetrische Authentifizierung	246
11.3.2	Asymmetrische Authentifizierung	247

- 12 Protokollanalyse 251**
 - 12.1 Fwlogwatch 251
 - 12.1.1 Installation von Fwlogwatch 251
 - 12.1.2 Konfiguration von Fwlogwatch 252
 - 12.2 IP Tables State (IPTState) 263
 - 12.3 Webfwlog Firewall Log Analyzer 265
 - 12.4 Scanulog und ulog-acctd 267
 - 12.5 Nulog 270
 - 12.6 EpyLog Log Analyzer 271

- 13 Administrationsoberflächen 273**
 - 13.1 Firewall Builder 273
 - 13.2 Firestarter 283
 - 13.3 Shorewall (Shoreline Firewall) 287
 - 13.3.1 Das Shorewall-Konzept 288
 - 13.3.2 Die Shorewall-Dateien 292
 - 13.3.3 Weitere Shorewall-Eigenschaften 295

- 14 Distributionswerkzeuge 297**
 - 14.1 Fedora Core 4 297
 - 14.2 SUSE Linux OSS 10 298
 - 14.3 Debian 306
 - 14.4 IPCop 307
 - 14.4.1 Das IPCop-Konzept 307
 - 14.4.2 IPCop-Installation 308
 - 14.4.3 IPCop-Web-Interface 312
 - 14.5 Smoothwall 317
 - 14.5.1 Smoothwall-Installation 318
 - 14.5.2 Smoothwall-Web-Interface 318

15 Testmethoden und -werkzeuge	319
15.1 Test der Regeln	319
15.2 Nmap	324
15.2.1 Nmap-Installation	324
15.2.2 Einfache Scans	325
15.2.3 Fortgeschrittene Anwendung	333
15.3 Nmap-Hilfswerkzeuge	343
15.3.1 Nmap-Audit	343
15.3.2 NDiff	345
15.3.3 Nmap-Parser	347
15.3.4 nmaplr	348
15.3.5 Fe3d	349
15.4 Nessus	350
V Fortgeschrittene Konfiguration	357
16 Die Iptables-Standardtests	359
16.1 Eingebaute Tests	359
16.1.1 -p, --protocol	359
16.1.2 -s, --source	359
16.1.3 -d, --destination	359
16.1.4 -i, --in-interface	360
16.1.5 -o, --out-interface	360
16.1.6 -f, --fragment	360
16.2 TCP-Tests	360
16.2.1 sourceport	360
16.2.2 destinationport	361
16.2.3 tcp-flags	361
16.2.4 syn	361
16.2.5 tcp-options	361

- 16.3 UDP-Tests 361
 - 16.3.1 sourceport 362
 - 16.3.2 destinationport 362
- 16.4 ICMP-Tests 362
- 16.5 addrtype 363
- 16.6 ah 363
- 16.7 comment 364
- 16.8 connbytes 364
- 16.9 connmark 365
- 16.10 conntrack 365
- 16.11 dccp 365
- 16.12 dscp 365
- 16.13 ecn 366
- 16.14 esp 366
- 16.15 hashlimit 366
- 16.16 helper 367
- 16.17 iprange 368
- 16.18 length 368
- 16.19 limit 368
- 16.20 mac 369
- 16.21 mark 369
- 16.22 multiport 370
- 16.23 owner 370
- 16.24 physdev 370
- 16.25 pkttype 370
- 16.26 realm 371
- 16.27 recent 371
- 16.28 sctp 372
- 16.29 state 373
- 16.30 string 373
- 16.31 tcpmss 373

16.32	tos	374
16.33	ttl	374
17	Alle Standardziele	375
17.1	ACCEPT	375
17.2	CLASSIFY	375
17.3	CLUSTERIP	375
17.4	CONNMARK	377
17.5	DNAT	377
17.6	DROP	377
17.7	DSCP	377
17.8	ECN	377
17.9	LOG	377
17.10	MARK	378
17.11	MASQUERADE	378
17.12	NETMAP	378
17.13	NFQUEUE	379
17.14	NOTRACK	379
17.15	QUEUE	379
17.16	REDIRECT	379
17.17	REJECT	379
17.18	RETURN	380
17.19	SAME	380
17.20	SNAT	380
17.21	TCPMSS	380
17.22	TOS	382
17.23	TTL	382
17.24	ULOG	382
18	Patch-O-Matic	383
18.1	Was ist Patch-O-Matic?	383
18.2	Wie bekomme ich Patch-O-Matic, und wie wende ich es an?	383

18.3	Base-Patches	386
18.3.1	IPV4OPTSSTRIP	386
18.3.2	connlimit	386
18.3.3	expire	387
18.3.4	NETMAP	387
18.3.5	fuzzy	387
18.3.6	ipv4options	388
18.3.7	nth	388
18.3.8	osf	388
18.3.9	psd	389
18.3.10	quota	390
18.3.11	random	390
18.3.12	set	390
18.3.13	time	390
18.3.14	u32	390
18.4	Extra-Patches	392
18.4.1	ACCOUNT	393
18.4.2	IPMARK	393
18.4.3	ROUTE	394
18.4.4	TARPIT	394
18.4.5	TRACE	395
18.4.6	XOR	395
18.4.7	account	395
18.4.8	condition	396
18.4.9	connrate	396
18.4.10	geoip	396
18.4.11	goto	396
18.4.12	h323-contrack-nat	396
18.4.13	ip_queue_vwmark	397
18.4.14	ipp2p	397
18.4.15	policy und IPsec-Patches	397

18.4.16	mms-contrack-nat	397
18.4.17	mport	397
18.4.18	owner-socketlookup	397
18.4.19	pptp-contrack-nat	398
18.4.20	quake3-contrack-nat	398
18.4.21	rpc	398
18.4.22	rsh	398
18.4.23	sip	399
18.4.24	talk-contrack-nat	399
18.4.25	tproxy	399
18.4.26	unclean	399
19	Connection Tracking	401
19.1	Connection Tracking – Überblick	401
19.1.1	Das TCP-Connection Tracking	402
19.1.2	Das UDP-Connection Tracking	403
19.1.3	Das ICMP-Connection Tracking	403
19.1.4	Das Connection Tracking für alle weiteren Protokolle	404
19.2	Das ip_contrack-Kernelmodul	404
19.3	TCP-Window-Tracking	406
19.4	/proc-Variablen	406
19.4.1	ip_contrack_buckets	407
19.4.2	ip_contrack_count	407
19.4.3	ip_contrack_generic_timeout	407
19.4.4	ip_contrack_icmp_timeout	407
19.4.5	ip_contrack_log_invalid	407
19.4.6	ip_contrack_max	408
19.4.7	ip_contrack_tcp_be_liberal	408
19.4.8	ip_contrack_tcp_loose	408
19.4.9	ip_contrack_tcp_max_retrans	408
19.4.10	ip_contrack_tcp_timeout_close	408
19.4.11	ip_contrack_tcp_timeout_close_wait	408

- 19.4.12 ip_contrack_tcp_timeout_established 409
- 19.4.13 ip_contrack_tcp_timeout_fin_wait 409
- 19.4.14 TCP-Zustände 410
- 20 Die NAT-Tabelle 411**
 - 20.1 Die NAT-Tabelle und ihre Ketten 411
 - 20.2 Source-NAT 413
 - 20.3 Destination-NAT 415
 - 20.4 MASQUERADE 415
 - 20.5 NETMAP 416
 - 20.6 SNAT 417
 - 20.7 SAME 417
 - 20.8 DNAT 418
 - 20.9 REDIRECT 418
 - 20.10 TPROXY 419
 - 20.11 NAT-Helfermodule 419
 - 20.12 CONNMARK-Target 420
- 21 Die Mangle-Tabelle 421**
 - 21.1 Die Ketten der Mangle-Tabelle 421
 - 21.2 Aktionen der Mangle-Tabelle 421
 - 21.2.1 CLASSIFY 421
 - 21.2.2 CONNMARK 422
 - 21.2.3 DSCP 422
 - 21.2.4 ECN 422
 - 21.2.5 IPMARK 422
 - 21.2.6 IPV4OPTSSTRIP 423
 - 21.2.7 MARK 423
 - 21.2.8 ROUTE 423
 - 21.2.9 TOS 423
 - 21.2.10 TTL 424
 - 21.2.11 XOR 424

22 Die Raw-Tabelle	425
22.1 Die Raw-Tabelle	425
23 Das /proc-Dateisystem	427
23.1 Einführung in /proc	427
23.2 /proc/net/	429
23.2.1 ip_conntrack	430
23.2.2 ip_conntrack_expect	430
23.2.3 ip_tables_*	430
23.3 /proc/sys/net/ipv4	430
23.3.1 icmp_*	430
23.3.2 igmp_*	432
23.3.3 inet_peer_*	433
23.3.4 ip_*	433
23.3.5 ipfrag_*	435
23.3.6 tcp_*	435
23.4 /proc/sys/net/ipv4/conf	445
23.4.1 accept_redirects	446
23.4.2 accept_source_route	446
23.4.3 arp_announce	446
23.4.4 arp_filter	446
23.4.5 arp_ignore	446
23.4.6 bootp_relay	447
23.4.7 disable_policy	447
23.4.8 disable_xfrm	447
23.4.9 force_igmp_version	447
23.4.10 forwarding	447
23.4.11 log_martians	447
23.4.12 mc_forwarding	447
23.4.13 medium_id	447
23.4.14 promote_secondaries	448

- 23.4.15 proxy_arp 448
- 23.4.16 rp_filter 448
- 23.4.17 secure_redirects 448
- 23.4.18 send_redirects 448
- 23.4.19 shared_media 448
- 23.4.20 tag 449
- 23.5 /proc/sys/net/ipv4/neigh 449
- 23.6 /proc/sys/net/ipv4/netfilter 449
- 23.7 /proc/sys/net/ipv4/route 449
- 23.8 /proc/sys/net/ipv6 449
- 24 Fortgeschrittene Protokollierung 451**
 - 24.1 Das ULOG-Target 451
 - 24.2 Das ipt_ULOG-Kernelmodul 452
 - 24.3 Der Ulogd-Daemon 452
 - 24.3.1 [OPRINT] 456
 - 24.3.2 [LOGEMU] 456
 - 24.3.3 [MYSQL] 456
 - 24.3.4 [PGSQL] 457
 - 24.3.5 [PCAP] 457
 - 24.3.6 [SQLITE3] 458
 - 24.3.7 [SYSLOG] 458
 - 24.4 Der Specter-Daemon 458
- 25 Ipset 461**
 - 25.1 ipset und iptables 461
 - 25.2 Die Ipset-Typen 462
 - 25.2.1 ipmap 463
 - 25.2.2 portmap 463
 - 25.2.3 macipmap 464
 - 25.2.4 iphash 465
 - 25.2.5 nethash 465

25.2.6	ipporthash	466
25.2.7	iptree	466
25.3	Das Kommando ipset	466
26	Hochverfügbare Firewalls	469
26.1	Was ist Hochverfügbarkeit, und wo ist das Problem?	469
26.2	Einfache Hochverfügbarkeit	470
26.3	Hochverfügbarkeit bei zustandsorientierten Firewalls	471
26.4	Praktische Implementierung mit KeepAlived	473
26.5	Hochverfügbarkeit und Masquerading/NAT	476
26.6	Zustandssynchronisation mit ct_sync	477
26.6.1	Installation	478
26.6.2	Funktion von ct_sync	480
26.6.3	Aufbau des ct_sync-Clusters	483
27	Nfnetlink und Kernel 2.6.14	489
27.1	Der conntrack-Befehl	489
28	nf-HiPAC	493
28.1	Was ist nf-HiPAC?	493
VI	Transparente Firewalls	495
29	ProxyARP	497
29.1	Wie funktioniert ProxyARP?	497
29.2	ProxyARP-Konfiguration	498
29.3	Filterung mit Iptables	500
29.4	Fazit	500
30	Iptables auf einer Bridge	501
30.1	Wie funktioniert die Bridge?	501
30.2	Bau einer Bridge mit Linux	502
30.3	Filtern auf der Bridge mit iptables	504

- 30.4 Filtern auf der Bridge mit arptables 505
- 30.5 Fazit 506
- 31 Etables 507**
 - 31.1 Etables-Installation 507
 - 31.1.1 Konfiguration des Linux-Kernels 507
 - 31.1.2 Installation des Userspace-Werkzeugs 508
 - 31.2 Die Etables-Tabellen 508
 - 31.2.1 Der Rahmen erreicht über ein Bridge-Interface das System . 510
 - 31.2.2 Der Rahmen erreicht über ein Nicht-Bridge-Interface
das System 510
 - 31.2.3 Ein lokal erzeugtes Paket verlässt das System
über die Bridge 510
 - 31.3 Die broute-Tabelle 510
 - 31.4 Die etables-Syntax 513
 - 31.5 Start einer Bridge auf Fedora Core 517
- VII Protokolle und Applikationen 519**
 - 32 Behandlung einzelner Protokolle 521**
 - 32.1 DHCP 521
 - 32.1.1 Das DHCP-Protokoll 522
 - 32.1.2 Iptables-Regeln 522
 - 32.2 DNS 523
 - 32.2.1 Das DNS-Protokoll 523
 - 32.2.2 Iptables-Regeln 524
 - 32.3 HTTP/HTTPS/Proxy 526
 - 32.3.1 Iptables-Regeln 528
 - 32.4 ELSTER 529
 - 32.4.1 Iptables-Regeln 529
 - 32.5 Telnet 530
 - 32.5.1 Iptables-Regeln 530

32.6	SSH	531
32.6.1	Iptables-Regeln	531
32.7	P2P: Edonkey	532
32.7.1	Iptables-Regeln	532
32.8	P2P: KaZaA	534
32.8.1	Iptables-Regeln	534
32.9	P2P: BitTorrent	535
32.9.1	Iptables-Regeln	536
32.10	FTP	537
32.10.1	Das FTP-Protokoll	537
32.10.2	Die Stateful Inspection des FTP-Protokolls	539
32.10.3	Iptables-Regeln	540
32.11	SNMP	542
32.11.1	Iptables-Regeln	542
32.12	Amanda	543
32.12.1	Das Amanda-Protokoll	543
32.12.2	Iptables-Regeln	543
32.13	PPTP	544
32.13.1	Iptables-Regeln	545
32.14	SMTP	546
32.14.1	Das SMTP-Protokoll	546
32.14.2	Iptables-Regeln	547
32.15	IRC	548
32.15.1	Iptables-Regeln	549
32.16	TFTP	549
32.16.1	Iptables-Regeln	550
32.17	IMAP	551
32.17.1	Iptables-Regeln	552
32.18	POP3	552
32.18.1	Iptables-Regeln	553

- 32.19 NTP 554
 - 32.19.1 Iptables-Regeln 554
- 32.20 NNTP 554
 - 32.20.1 Iptables-Regeln 554
- 32.21 H.323 555
 - 32.21.1 Iptables-Regeln 555
- 32.22 SIP 556
 - 32.22.1 Iptables-Regeln 557
- 33 IPsec 559**
 - 33.1 IPsec 559
 - 33.2 Iptables-Regeln zum Durchleiten von IPsec 560
 - 33.3 KLIPS 561
 - 33.4 26sec 562
 - 33.4.1 Transport-Modus 563
 - 33.4.2 Tunnel-Modus 563
 - 33.4.3 Filterung mit Firewall-Markierung 566
 - 33.4.4 Filterung mit dem policy-Match 567
- 34 ICMP 569**
 - 34.1 ICMP 569
 - 34.2 ICMP destination-unreachable 570
 - 34.3 ICMP fragmentation-needed 572
 - 34.4 ICMP source-quench 576
 - 34.5 ICMP redirect 577
 - 34.6 ICMP time-exceeded 577
 - 34.7 ICMP parameter-problem 578
 - 34.8 ICMP router-advertisement/router-solicitation 578
 - 34.9 ICMP timestamp-request/timestamp-reply 579
 - 34.10 ICMP address-mask-request/address-mask-reply 580
 - 34.11 ICMP echo-request/echo-reply (Ping) 580

34.12 Traceroute	582
34.13 Optimierung der ICMP-Regeln	584
35 IPv6	587
35.1 Filterung mit ip6tables	587
35.2 Neue IPv6-Targets	588
35.2.1 HL	588
35.3 Neue IPv6-Matches	589
35.3.1 dst	589
35.3.2 eui64	589
35.3.3 hbh	589
35.3.4 hl	589
35.3.5 ipv6header	589
35.4 rt	590
A Postfix-E-Mail-Relay	591
A.1 Postfix als E-Mail-Relay	591
A.2 Adressverifizierung	592
A.3 Amavisd-New	593
B Firewall-Skript	595
B.1 Stopp der Firewall	595
C Netzwerkgrundlagen	599
C.1 TCP/IP	599
C.2 IP	600
C.2.1 Version	601
C.2.2 Header-Länge	601
C.2.3 Type-of-Service	602
C.2.4 Gesamtpaketlänge	602
C.2.5 Identifikationsnummer	602
C.2.6 Flaggen	602
C.2.7 Fragment-Offset	603

- C.2.8 Time To Live (TTL) 603
- C.2.9 Protokoll 604
- C.2.10 Prüfsumme 604
- C.2.11 Quell-IP-Adresse 604
- C.2.12 Ziel-IP-Adresse 604
- C.2.13 IP-Optionen 604
- C.3 UDP 606
- C.4 TCP 608
 - C.4.1 Auf- und Abbau einer TCP-Verbindung 609
 - C.4.2 TCP-Header 611
 - C.4.3 Fortgeschrittene Eigenschaften von TCP 616
- C.5 Explicit Congestion Notification 619
- C.6 ICMP 621
 - C.6.1 Destination Unreachable 622
 - C.6.2 Source Quench 623
 - C.6.3 Time Exceeded 623
 - C.6.4 Redirect 624
 - C.6.5 Parameter Problem 624
 - C.6.6 Echo-Request und Reply 624
 - C.6.7 Address Mask Request und Reply 625
 - C.6.8 Timestamp Request und Reply 625
 - C.6.9 Router Solicitation und Advertisement 626
- C.7 ARP 626

- Literaturverzeichnis 629**
- Stichwortverzeichnis 631**
- Über den Autor 643**



Vorwort

Dieses Buch widmet sich dem Paketfilter *Netfilter/Iptables* der Linux-Kernel 2.4 und 2.6. Obwohl bereits einiges an Literatur zu diesem Thema existiert, hat mir persönlich kein Buch richtig gut gefallen. Daher habe ich bereits seit einigen Jahren überlegt, ein eigenes Buch zu diesem Thema zu schreiben, das auch die fortgeschrittenen Themen und neue Eigenschaften behandelt, die in den letzten Jahren hinzugekommen sind.

Während ich an diesem Buch geschrieben habe, hat das Netfilter-Team (das das Framework im Kernel entwickelt, das mit Iptables gesteuert wird) große Teile, die im Kernel verborgen sind, ausgetauscht. Das hat zu einem Wettlauf zwischen mir und den Release-Zyklen der Kernel geführt. Natürlich wollte ich diese Funktionen auch in dieses Buch einarbeiten. Da ich selbst noch nicht sämtliche Auswirkungen auf alle Bereiche absehen kann und sich einige auch noch im Fluss befinden, habe ich diese Neuerungen in ein eigenes Kapitel (siehe Kapitel 27) verschoben. Jedoch wird der typische Endanwender diese Modifikationen entweder gar nicht wahrnehmen oder aber in einigen Bereichen auch begrüßen.

Ansonsten habe ich versucht, sowohl den Einsteiger zu berücksichtigen und ihn in einzelnen Kapiteln behutsam mit der Materie des Paketfilters vertraut zu machen als auch dem fortgeschrittenen Benutzer die Mittel an die Hand zu geben, die er für eine mächtige Firewall benötigt.

Ich hoffe, dass es mir mit diesem Buch gelungen ist, Ihren Geschmack zu treffen und Ihnen wertvolle Informationen zu liefern. Nach meinen Büchern »VPN mit Linux (ISBN 3-8273-2114-X)« und »Intrusion Detection und Prevention mit Snort 2 & Co. (ISBN 3-8273-2134-4)« rundet dieses Buch das Thema Netzwerksicherheit mit Open Source ab.

Sollten Sie Fragen oder Kritik zu diesem Buch haben, zusätzliche Ideen haben oder Informationen vermissen, würde ich mich über Ihre E-Mail an ralf@spenneberg.net freuen.

Ich wünsche Ihnen viel Spaß beim Lesen und viel Erfolg bei der Konfiguration und Administration Ihrer Linux-Firewall.



Einleitung

Angesichts täglicher Meldungen über neue Viren, Hackerangriffe und Sicherheitslücken ist eine Firewall ein wesentlicher Bestandteil eines sicheren Netzwerks. Eine Firewall ist besonders wichtig, wenn Sie Ihr Netzwerk mit anderen unbekanntem und nicht vertrauten Netzwerken wie dem Internet verbinden. Dann sollten Sie diese Verbindung mit einer Firewall überwachen. Die Firewall beschränkt den Netzwerkverkehr auf den von Ihnen gewünschten Verkehr und weist alle anderen Anfragen ab. Natürlich müssen Sie sicherstellen, dass es keine Möglichkeit gibt, die Firewall mit Hilfe eines Modems oder anderer Hilfsmittel zu umgehen, denn dann ist die Firewall fast nichts mehr wert. Es bleibt Ihnen dann nur noch der Wert der Hardware.

Aber selbst wenn Sie Ihr Netzwerk nicht mit einem anderen Netz verbinden oder hierzu eine kommerzielle Firewall verwenden, kann es sinnvoll sein, über interne Linux-Firewalls nachzudenken. Kennen Sie Ihre Benutzer und Anwender wirklich? Vertrauen Sie ihnen? Gibt es in Ihrem Netz Systeme, die Sie schützen möchten oder müssen? Dann ist es sinnvoll, auch innerhalb eines Netzes mit Firewalls den Schutz dieser Systeme zu implementieren.

Dieses Buch hilft Ihnen dabei, diese Funktionen mit Hilfe von Linux und Iptables zu realisieren.

Das Buch beginnt mit den Firewall-Grundlagen. Hier lernen Sie wichtige Begriffe, Architekturen und die Unterschiede der verschiedenen Firewall-Technologien kennen. Außerdem erhalten Sie einen kurzen Überblick, wie Firewalls entstanden sind.

Der zweite Teil beschäftigt sich mit einer Einführung in Iptables und zeigt Ihnen, wie Sie eine einfache Firewall auf einem Gateway mit Iptables realisieren. Außerdem erfahren Sie in diesem Kapitel, wie Sie eine Linux-Distribution härten und wie Ihnen Intrusion-Detection-Systeme helfen können, Angriffe zu erkennen, die Ihre Firewall nicht abgewehrt hat.

Der dritte Teil beschäftigt sich mit typischen Firewall-Architekturen und stellt Ihnen eine lokale Firewall und eine Firewall mit DMZ inklusive der Realisierung und möglicher Probleme vor.

Im vierten Teil werden verschiedene zusätzliche Werkzeuge vorgestellt, die Sie benötigen oder verwenden können, um erfolgreich eine Firewall aufzubauen und zu warten. Dies sind Protokollserver, Zeitserver, Protokollanalysewerkzeuge, Oberflächen für die Administration, eine Betrachtung der von den Distributionen mitgelieferten Werkzeuge und Werkzeuge für den Test Ihrer Firewall.

Der fünfte Teil ist für die fortgeschrittenen Anwender gedacht und beginnt mit einer kompletten Referenz aller Iptables-Funktionen (Tests und Ziele), den in Patch-O-Matic verfügbaren zusätzlichen Funktionen, einer Beschreibung des Connection-Tracking-Mechanismus und dessen Tuning und der Beschreibung der NAT-, Mangle- und Raw-Tabellen. Weiterhin finden Sie hier die Erklärung der Variablen im `/proc`-Verzeichnis. Sie lernen, wie Sie in Datenbanken protokollieren, IP-Adressen mit `ipset` gruppieren, hochverfügbare Firewalls aufbauen und welche Funktionen in der nächsten Zukunft in Iptables zu erwarten sind.

Der sechste Teil ist komplett transparenten Firewalls gewidmet. Dies sind Firewalls, die auf der IP-Ebene unsichtbar sind und wie auf einer Bridge arbeiten.

Der siebte Teil beschäftigt sich mit den Besonderheiten einzelner Protokolle und zeigt Ihnen, wie Sie DHCP, IPv6 oder IPsec filtern. Diese Kapitel sollten alle Fragen rund um eine Iptables-Firewall beantworten.