

Inhaltsverzeichnis

Einführung	17
E.1 Übersicht	18
E.2 Was dieses Buch nicht beschreibt	19
E.3 Einbruchsversuche: Dimension eines Problems	20
E.4 Was hat der Eindringling davon?	20
E.5 Was steht für Sie auf dem Spiel?	21
E.6 Firewalls und Black Hats in einer idealen Welt	22
 Teil 1 Vorüberlegungen	 23
 Kapitel 1 Grundlegende Konzepte für Paketfilter-Firewalls	 25
1.1 Das OSI-Referenzmodell	27
1.2 Ports: Tore zu den Programmen auf Ihrem Computer	30
1.3 Pakete: Botschaften im IP-Netz	32
1.3.1 IP-Nachrichtentypen: ICMP	33
1.3.2 IP-Nachrichtentypen: UDP	34
1.3.3 IP-Nachrichtentypen: TCP	35
1.4 Zusammenfassung	39
 Teil 2 Paketfilter und grundlegende Sicherheitsmaßnahmen	 41
 Kapitel 2 Konzepte für Paketfilter	 43
2.1 Eine Paketfilter-Firewall	45
2.2 Auswahl der Voreinstellung für den Umgang mit Paketen	47
2.3 REJECT und DENY: Pakete ablehnen oder verwerfen?	50
2.4 Filtern ankommender Pakete	51
2.4.1 Filtern nach Absender-IP	51
2.4.2 Filtern nach Empfänger-IP	54
2.4.3 Filtern nach Absender-Port	54

2.4.4	Filtern nach Empfänger-Port	55
2.4.5	Filtern nach TCP-Status-Flags	55
2.4.6	Abtastversuche und Scans	55
2.4.7	Denial-of-Service-Angriffe	59
2.4.8	Weitere Überlegungen zum Filtern von Paketen	63
2.5	Filtern abgehender Pakete	64
2.5.1	Filtern nach Absender-IP	65
2.5.2	Filtern nach Empfänger-IP	65
2.5.3	Filtern nach Absender-Port	66
2.5.4	Filtern nach Empfänger-Port	66
2.5.5	Filtern nach TCP-Status-Flags	66
2.6	Private und öffentliche Dienste im Netz	67
2.6.1	Unsichere lokale Dienste schützen	68
2.6.2	Auswahl der Dienste	68
2.7	Zusammenfassung	86
Kapitel 3	Gestaltung und Installation einer Firewall	87
3.1	ipchains: Firewall-Verwaltung unter Linux	88
3.1.1	Im Firewall-Skript eingesetzte ipchains-Optionen	90
3.1.2	IP-Adressen von Absender und Empfänger	91
3.2	Initialisierung der Firewall	93
3.2.1	Symbolische Konstanten für die Beispiele	94
3.2.2	Löschen alter Firewall-Regeln	94
3.2.3	Festlegung der voreingestellten Policy	95
3.2.4	Einschalten des Loopback-Interfaces	95
3.2.5	Gefälschte Absender und andere fehlerhafte Adressen	96
3.3	ICMP-Nachrichten filtern	103
3.3.1	Fehler- und Kontrollnachrichten	103
3.3.2	Kontrollnachrichten für ping: echo-request (Typ 8) und echo-reply (Typ 0)	106
3.4	Dienste auf festen, unprivilegierten Ports schützen	108
3.4.1	Häufige TCP-Dienste auf unprivilegierten Ports	109
3.4.2	Lokale UDP-Dienste auf unprivilegierten Ports	111

3.5	Zwingend benötigte Dienste erlauben	114
3.5.1	DNS (UDP- und TCP-Port 53)	114
3.5.2	Der auth-Service (TCP-Port 113)	120
3.6	Häufige TCP-Dienste	121
3.6.1	E-Mail (TCP: SMTP – Port 25; POP – Port 110; IMAP – Port 143)	122
3.6.2	Usenet News (NNTP: TCP-Port 119)	129
3.6.3	telnet (TCP-Port 23)	131
3.6.4	ssh (TCP-Port 22)	133
3.6.5	ftp (TCP-Ports 20 und 21)	135
3.6.6	World Wide Web	139
3.6.7	finger (TCP-Port 79)	142
3.6.8	whois (TCP-Port 43)	143
3.6.9	gopher (TCP-Port 70)	144
3.6.10	WAIS (TCP-Port 210)	145
3.7	Häufige UDP-Dienste	145
3.7.1	traceroute (UDP-Port 33434)	145
3.7.2	Zugriff auf den DHCP-Server Ihres Internet-Providers (UDP-Ports 67 und 68)	147
3.7.3	Network-Time-Server abfragen (UDP-Port 123)	150
3.8	Abgewiesene Pakete protokollieren	151
3.9	Zugriff für problematische Sites pauschal sperren	153
3.10	LAN-Zugang	154
3.10.1	LAN-Zugang zum internen Netzwerkinterface der Firewall	154
3.10.2	LAN-Zugriffe auf das Internet: IP-Forwarding und -Masquerading	155
3.11	Die Firewall installieren	156
3.11.1	Installation einer Firewall mit einer statischen IP-Adresse	156
3.11.2	Installation einer Firewall für PPP	157
3.11.3	Installation einer Firewall für DHCP	158
3.12	Zusammenfassung	160

Kapitel 4	LANs, mehrfache Firewalls und Perimeter-Netze	161
4.1	Sicherheit im LAN	163
4.2	Konfigurationsmöglichkeiten für ein privates LAN mit vertrauenswürdigen Benutzern	164
4.2.1	LAN-Zugriffe auf die Bastion-Firewall	166
4.2.2	LAN-Zugriffe auf andere LANs: Lokale Pakete zwischen mehreren lokalen Netzen weiterleiten	166
4.2.3	LAN-Zugriffe aufs Internet: Forwarding und Masquerading	167
4.3	Konfigurationsmöglichkeiten für ein größeres oder weniger vertrauenswürdiges LAN	169
4.3.1	Bildung mehrerer Subnetze	169
4.3.2	Selektiver interner Zugang nach Host, Adressbereich oder Port	170
4.3.3	Masquerading zwischen LAN und Internet	178
4.3.4	Portumleitung und transparente Proxies	181
4.3.5	Aus dem Internet ankommende Verbindungen zu internen Servern umleiten	181
4.4	Eine formale Firewall mit abgeschirmtem Subnetz	183
4.4.1	Symbolische Konstanten für die Firewall-Beispiele	185
4.4.2	Löschen alter Firewall-Regeln	187
4.4.3	Festlegung der voreingestellten Policy für die Choke	187
4.4.4	Einschalten des Loopback-Interfaces auf der Choke	187
4.4.5	Gefälschte Absender und andere fehlerhafte Adressen (Klassen A bis C)	188
4.4.6	ICMP-Nachrichten filtern	189
4.4.7	DNS (UDP- und TCP-Port 53)	194
4.4.8	Der auth-Service (TCP-Port 113)	200
4.4.9	E-Mail (SMTP: TCP-Port 25; POP: TCP-Port 110; IMAP: TCP-Port 143)	203
4.4.10	Usenet News (TCP: NNTP-Port 119)	214
4.4.11	telnet (TCP-Port 23)	216
4.4.12	ssh (TCP-Port 22)	218
4.4.13	ftp (TCP-Ports 21 und 22)	222

4.4.14	WWW	232
4.4.15	finger (TCP-Port 79)	243
4.4.16	whois (TCP-Port 43)	245
4.4.17	gopher (TCP-Port 70)	246
4.4.18	WAIS (TCP-Port 210)	247
4.4.19	RealAudio und QuickTime (Ports 554 u.a.)	249
4.4.20	Internet Relay Chat IRC (TCP-Port 6667)	253
4.4.21	CU-SeeMe (UDP-Port 7648, 7649 und 24032; TCP-Ports 7648 und 7649)	258
4.4.22	Quake (UDP-Ports 26000 sowie 1025 bis 1200)	262
4.4.23	Der Network Time Service NTP (UDP-Port 123)	266
4.4.24	Protokolle an einen anderen Computer schicken (UDP-Port 514)	269
4.4.25	Die Choke als lokaler DHCP-Server (UDP-Ports 67 und 68)	271
4.4.26	LAN-Zugriff auf die Choke	272
4.4.27	IP-Masquerading	272
4.4.28	Protokollierung	273
4.5	Zusammenfassung	273
Kapitel 5	Fehlersuche	275
5.1	Ein paar allgemeine Tipps für die Firewall-Entwicklung	276
5.2	Anzeigen der Firewall-Regeln	278
5.2.1	ipchains -L input	278
5.2.2	ipchains -L input -n	279
5.2.3	ipchains -L input -v	281
5.2.4	ipchains -L input -nv	283
5.3	Die Regeln für die input-, output- und forward-Chains	284
5.3.1	Die input-Chain	284
5.3.2	Die output-Chain	286
5.3.3	Die forward-Chain	289
5.4	Die Firewall-Regeln mit Einzelpaketen testen	290

5.5	Suche nach offenen Ports	292
5.5.1	netstat -a [-n -p -A inet]	292
5.5.2	strobe	295
5.5.3	nmap	296
5.6	Fehlersuche für ssh – ein Beispiel aus der Praxis	296
5.7	Zusammenfassung	299
Teil 3	Systemsicherheit und Systemüberwachung	301
Kapitel 6	Läuft das System wie erwartet?	303
6.1	Überprüfen der Netzwerkschnittstellen mit ifconfig	304
6.2	Überprüfen der Netzwerkverbindung mit ping	305
6.3	Überprüfen der Netzwerkprozesse mit netstat	307
6.4	Überprüfen aller laufenden Prozesse mit ps ax	308
6.5	Die Protokolldateien Ihres Systems	311
6.5.1	Was wird wohin geschrieben?	311
6.5.2	Konfiguration des syslogs	312
6.5.3	Was bedeuten die Meldungen der Firewall?	314
6.5.4	Häufig gescannte Ports	316
6.5.5	Pakete zur automatisierten Protokollanalyse	321
6.6	Zusammenfassung	322
Kapitel 7	Ergänzende Maßnahmen durch die Unix-Systemadministration	323
7.1	Authentifizierung: Prüfung der Identität	324
7.1.1	Shadow-Passwörter	324
7.1.2	MD5-Hashes für Passwörter	325
7.1.3	Die rhost-Authentifizierung von Berkeley: hosts.equiv und .rhosts	326
7.1.4	Gemeinsamer Zugang zu zentralen Authentifizierungsdatenbanken: der Network Information Service (NIS)	326
7.2	Autorisation: Festlegung von Zugriffsrechten	327
7.2.1	Zugriff auf den root-Account	327
7.2.2	Verwendung von su einschränken	328

7.2.3	Die tcp_wrapper	328
7.2.4	Zugriffsrechte für Dateien und Verzeichnisse	332
7.3	Serverspezifische Konfiguration	334
7.3.1	telnet-Konfiguration	334
7.3.2	ssh-Konfiguration	334
7.3.3	SMTP-Konfiguration	335
7.3.4	DNS-Konfiguration	337
7.3.5	ftp-Konfiguration	359
7.3.6	Konfiguration eines POP-Servers	365
7.3.7	Konfiguration eines DHCP-Servers	366
7.3.8	NTP-Konfiguration	368
7.3.9	Konfiguration von CGI-Skripten	370
7.4	SOCKS: eine Proxy-Firewall auf Anwendungsebene	371
7.5	Diverse Systemaccounts in /etc/passwd und /etc/group	372
7.6	Die PATH-Variable	373
7.7	/etc/issue.net	374
7.8	Protokollierung auf andere Rechner	375
7.9	Halten Sie Ihre Software auf dem Laufenden!	376
7.9.1	Updates von Red Hat	376
7.9.2	Beispiel: Sicherheitslücke in mountd	376
7.10	Zusammenfassung	377
Kapitel 8	Entdecken von Eindringlingen und Melden der Vorfälle	379
8.1	Prüfung der Systemintegrität	381
8.1.1	COPS	381
8.1.2	crack	381
8.1.3	ifstatus	382
8.1.4	MD5	382
8.1.5	SATAN	382
8.1.6	tiger	383
8.1.7	tripwire	383
8.2	Welche Symptome deuten auf einen Eindringling hin?	383
8.2.1	Hinweise aus dem syslog	384
8.2.2	Änderungen der Systemkonfiguration	385

8.2.3	Änderungen am Dateisystem	385
8.2.4	Änderungen an Benutzer-Accounts	386
8.2.5	Hinweise der Überwachungswerkzeuge	386
8.2.6	Geschwindigkeitseinbußen	387
8.3	Reaktion auf einen Einbruch	387
8.4	Meldung eines Vorfalls	389
8.4.1	Warum sollten Sie Vorfälle melden?	389
8.4.2	Welche Vorfälle sollten Sie melden?	390
8.4.3	Wem melden Sie?	392
8.4.4	Was melden Sie?	393
8.5	Wo finden Sie nähere Informationen?	394
8.6	Zusammenfassung	395
Teil 4	Anhänge	397
Anhang A	Ressourcen rund um das Thema Sicherheit	399
A.1	Informationsquellen	400
A.2	Softwaresammlungen	401
A.3	Sicherheitstools	401
A.4	Firewall-Tools	404
A.5	Nachschlagewerke und FAQ-Listen	404
A.5.1	Sicherheit unter Unix	404
A.5.2	Rund um Firewalls	405
A.5.3	Web-Server	406
A.6	Online-Dokumentation	406
A.7	Web-Sites zu allgemeinen Themen	407
A.8	Bücher	408
Anhang B	Firewall-Beispiele und hilfreiche Skripten	409
B.1	Die rc.firewall für ipchains für ein Einzelplatzsystem oder ein Privat-LAN aus Kapitel 3	410
B.2	Die rc.firewall für ipfwadm für ein Einzelplatzsystem oder ein Privat-LAN aus Kapitel 3	431

B.3	Optimierung der Firewall-Regeln	451
B.3.1	Optimierung der Reihenfolge der ipfwadm-Regeln	462
B.3.2	Optimierung der ipchains-Regeln mit benutzerdefinierten Chains	471
B.4	Spezialskripten	485
B.4.1	Alles erlauben	485
B.4.2	Alles sperren	485
B.4.3	Eine IP-Adresse blockieren	486
B.4.4	Eine blockierte IP-Adresse wieder zulassen	487
Anhang C	Glossar	489
	Der Autor	511
	Stichwortverzeichnis	513