
Inhalt

Einleitung	XIII
1 Wer braucht eine Firewall?	1
2 Was ist eine Firewall?	5
Was eine Firewall kann	5
Was eine Firewall nicht kann	7
Typische Einsatzszenarien für Firewalls	9
Der Privathaushalt	9
Das Studentenwohnheim	11
Die Firma	12
3 Netzwerkgrundlagen	15
TCP/IP im Überblick	16
IP	18
ARP	20
ICMP	21
TCP	21
UDP	24
DNS	25
4 Welche Angriffe gibt es?	27
Denial-of-Service-Angriffe	27
Flooding	27
Angriffe mittels ICMP	30

Cracking	31
Auswahl eines Ziels	31
Informationsbeschaffung	31
Einbruch in den Rechner	34
Rootrechte erlangen	40
Sicherungsmaßnahmen	42
Lokale Aktivität	43
Den nächsten Angriff vorbereiten	43
Würmer	52
Trojaner	52
Angriffe auf die Privatsphäre	56
Aktive Inhalte von HTML-Seiten	59
Social Engineering und Phishing	62
5 Firewall-Architekturen	65
Paketfilter	65
Proxies	67
Network Address Translation	68
Masquerading	69
Redirection	70
Kombinierte Konzepte	71
Screened Host	71
Screened Subnet	72
6 Eine Firewall auf einer Floppy	75
Vorüberlegungen	76
Coyote Linux	78
Installation	78
Ein erster Rundgang	83
Die Konfiguration anpassen	87
fli4l	90
Konfiguration	90
Ein erster Rundgang	99

7	Planung einer normalen Installation	103
	Policies	103
	Eine Policy für ein Studentenwohnheim	104
	Eine Policy für eine Firma	105
	Richtlinien und Spezifikationen	106
	Hardware	108
	Vorgehen bei der Implementation	109
	Rechnerdaten	110
	Partitionen und ihre Mountpoints festlegen	112
8	Installation der Software	115
	Installation der benötigten Software	116
	SuSE	116
	Debian	119
	Konfiguration des Mailservers Exim	121
	SuSE 9.3	121
	Debian 3.1	121
	Testen der geänderten Konfiguration	122
	Der Bootvorgang	123
	Das BIOS	123
	Der Bootloader	123
	Init	125
	Hardware-Integration durch Kompilation	135
	Grundlagen: Modularer vs. monolithischer Kernel	136
	Konfiguration eines Kernels der Serie 2.2	137
	Konfiguration eines Kernels der Serie 2.4	140
	Konfiguration eines Kernels der Serie 2.6	144
	Kernelkompilation	150
	Kompilation und Installation der Module	153
	Installation des Kernels	154
	Eintrag in die modules.conf bzw. modprobe.conf	161
	Laden der Module durch ein Runlevel-Skript	164
	Konfiguration des /proc-Dateisystems	166

Konfiguration der /etc/fstab	171
Neustart	173
9 Das System sicher konfigurieren	175
Cron	175
Der inetd	179
Entfernen unnötiger Programme, Dienste, Dateirechte und Dateien	184
Automatisch gestartete Programme	184
Dateirechte	189
Spezielle Dateien	197
Automatisieren der Suche	200
Das Systemprotokoll	205
syslog	206
syslog-ng	208
10 Das Netzwerk einrichten	219
Vorbereitung	219
Konfiguration der Netzwerkkarte	219
Einrichten von Modem oder DSL	227
Der PPP-Daemon	227
Modemkonfiguration	229
DSL	237
Einrichten der ISDN-Karte	245
Eintrag des DNS-Servers	254
Eintragen der lokalen Rechnernamen	256
Verbindungstests	257
Mit ipchains (Kernel 2.2.x)	258
Mit iptables (Kernel 2.4.x)	263
11 Konfiguration der Paketfilter mit ipchains	269
Die Idee	269
Policy	271
Regeln	271
Muster	272

Aktionen	273
Optionen	273
Verwaltung von Chains	274
Besondere Masquerading-Befehle	274
Testen von Chains	274
Sichern und Wiederherstellen der Firewall-Konfiguration	275
Einige Beispiele	275
Die absolut sichere Firewall	277
Schutz vor Spoofing	277
Das Loopback-Interface	278
NetBIOS	278
ICMP	279
Eigene Chains	282
Blockieren des Zugriffs auf lokale Serverdienste	283
DNS	284
Ident (Auth)	285
Einfache Anwendungsprotokolle über TCP	286
Proxies auf der Firewall	290
Transparente Proxies	291
FTP	292
Logging ungewöhnlicher Pakete	296
Eintragen der Regeln in die Systemdateien	296
12 Konfiguration der Paketfilter mit iptables	307
Die Idee	307
Policies	308
Regeln	309
Tables	309
Muster	310
Aktionen	311
Verwalten von Chains	313
Einige Beispiele	314
Die absolut sichere Firewall	316

Schutz vor Spoofing	316
Ident (Auth)	317
Unerwünschter Aufbau von Verbindungen	318
Das Loopback-Interface	320
NetBIOS	320
ICMP	320
Eigene Chains	322
Blockieren des Zugriffs auf lokale Serverdienste	323
DNS	324
Einfache TCP-basierte Protokolle	325
FTP	330
Proxies auf der Firewall	331
Transparente Proxies	333
Logging ungewöhnlicher Pakete	335
Masquerading	336
Regeln in Systemdateien eintragen	337
13 Eine DMZ – Demilitarized Zone	351
Das Netzwerk planen	351
Proxy-ARP	353
Reverse Proxies	357
Paketfilter	359
Paketfilterung mit ipchains	360
Paketfilterung mit iptables	375
14 Proxies	399
Einrichten eines Web- oder FTP-Proxys	399
squid	400
Privoxy	405
ftp-proxy aus der SuSE Proxy-Suite	418
Einrichten eines DNS-Servers	430
Einrichtung eines chroot-Käfigs	430
Konfiguration des Systemprotokollendienstes	432

Grundkonfiguration	434
Konfiguration des Dienstaufrufs	438
Start und Test	439
15 Abnahmetests	441
Vorarbeiten	441
Testaufbau	441
Simulation einer Einwahl	442
Die Konfiguration der Testrechner	444
Funktionstests	444
Port Scans	446
Grundlagen	446
Die Tests	449
16 Wie Sorge ich dafür, daß meine Firewall sicher bleibt?	453
Checksummer	453
Planung	454
md5sum	456
AIDE	468
Tripwire	474
Backups	483
Sicherung der Partitionierungsdaten	484
Archive erzeugen mit tar	485
Direktes Schreiben des Backups auf Magnetband	488
Brennen eines Backups auf CD oder DVD	489
Das Zurückspielen des Backups	496
Auswerten der Systemprotokolle	501
Logrotation	501
Filterung	506
Bewertung der Meldungen	520
Dokumentation	530
Schulung der Benutzer	532
Updates	535

17	Vorfallsbehandlung	539
	Warnsignale	540
	Dokumentation	542
	Bestandsaufnahme	544
	Die Kontrolle wiedererlangen	549
	Spurensicherung	550
	Autopsie	554
	Kompilieren des Coroner's Toolkit	554
	Veränderte Programme und Dateien	555
	MAC-Zeiten	568
	Gelöschte Dateien	578
	Autopsiebericht	591
	Wiederherstellen des Systems	592
	Nachlese	592
A	Internet-by-Call ohne Anmeldung	595
B	Der vi	597
C	Linux-Firewalls Copyright-Informationen	601
	Literaturverzeichnis	617
	Index	623