

Inhaltsverzeichnis

1	TCP/IP-Dienste konfigurieren	10
1.1	Ports, Sockets und die Datei <code>/etc/services</code>	10
1.2	Server mit eigenem Startskript	12
1.3	Der Internet-Dämon (x) <code>inetd</code> und der TCP-Wrapper	15
1.3.1	<code>xinetd</code> — der Internet-Super-Server	15
1.3.2	<code>inetd</code> – Der Internet Super-Server	17
1.3.3	Der TCP-Wrapper	19
1.4	Wissensfragen	21
1.5	Übungen	23
1.6	Lösungen	24
2	TCP/IP-Standardclients	27
2.1	<code>whois</code>	27
2.2	<code>telnet</code>	28
2.3	<code>ftp</code>	29
2.4	Die Berkeley r-Dienste	32
2.4.1	<code>rlogin</code>	34
2.4.2	<code>rcp</code>	34
2.4.3	<code>rsh</code>	35
2.5	Die Secure-Shell (<code>ssh</code>)	36
2.6	Übungen	39
3	NIS Network Information Service	41
3.1	NIS-Grundlagen	41
3.2	Konfiguration eines NIS-Master-Servers	43
3.3	Konfiguration eines NIS-Clients	46
3.3.1	Grundkonfiguration	46
3.3.2	Feinkonfiguration	49
3.4	Übungen	55
3.5	Lösungen	56

INHALTSVERZEICHNIS

4	Namensauflösung unter Linux	57
4.1	Funktionsweise des DNS	57
4.1.1	Domain-Struktur	57
4.1.2	Namensraum	58
4.1.3	Delegation und Zonen	59
4.2	Namensauflösung	60
4.2.1	Vorwärtsauflösung	60
4.2.2	Caching	62
4.2.3	Rückwärtsauflösung	63
4.2.4	Lastverteilung und Ausfallsicherheit	64
4.3	Konfiguration des Resolvers	65
4.3.1	/etc/resolv.conf	67
4.3.2	/etc/nsswitch.conf	68
4.3.3	/etc/host.conf	70
4.4	DNS-Konfiguration	71
4.4.1	Übersicht über die Konfigurationsdateien	71
4.4.2	Konfiguration eines caching-only-Nameservers	75
4.4.3	Konfiguration eines primären Nameservers ohne Unterzonen	79
4.4.4	Konfiguration eines primären Nameservers mit Unterzonen	82
4.4.5	Konfiguration eines sekundären Nameservers	85
4.4.6	Konfiguration eines eigenen Root-Nameservers	87
4.4.7	Testen einer Konfiguration	89
4.4.8	Nameserver fernsteuern mit rndc	96
4.5	Das Wichtigste in Kürze	98
4.6	Wissensfragen	102
4.7	Lösungen	104
4.8	Übungen	105
4.9	Lösungen	107
5	DHCP — Netzwerkkonfiguration zentral	111
5.1	Das DHCP-Protokoll und seine Einsatzmöglichkeiten	111
5.1.1	Einsatzmöglichkeiten	113

5.2	Server-Konfiguration	114
5.2.1	Ein paar Tipps zur Sicherheit	118
5.2.2	dhcpcd unter SuSE	118
5.3	Client-Konfiguration	120
5.4	Wissensfragen	122
5.5	Übungen	123
5.6	Lösungen	124
6	Samba — Datei- und Druckdienste im Windows-Netz	127
6.1	Grundbegriffe des Windows-Netzwerks	127
6.1.1	Überblick über das Samba-Paket	132
6.2	Server-Konfiguration	132
6.2.1	Grundeinstellungen vornehmen	133
6.2.2	Zugriff steuern	134
6.2.3	Verzeichnisse freigeben	135
6.2.4	Drucker freigeben	137
6.2.5	Konfiguration testen	137
6.2.6	Samba übers Web administrieren	138
6.3	Clients benutzen und konfigurieren	139
6.3.1	Dateisysteme einbinden	139
6.3.2	Drucker einbinden	139
6.3.3	Netzwerk-Backup zentral	140
6.3.4	Windows-Clients konfigurieren	141
6.4	Übungen	141
7	Apache — Der Web-Server-Standard	143
7.1	Einführung	143
7.2	Konfiguration	147
7.2.1	Globale Servereigenschaften	148
7.2.2	Zugriffsteuerung	149
7.2.3	Server-Ressourcen verwalten	152
7.3	Test der Konfiguration	155

INHALTSVERZEICHNIS

7.4	Einrichten von passwortgeschützten Web-Seiten	156
7.5	Virtuelle Hosts	159
7.5.1	IP-basierte virtuelle Hosts	160
7.5.2	Namensbasierte virtuelle Hosts	161
7.5.3	Portbasierte virtuelle Hosts	162
7.6	Apache MPM-Module und Tuning	163
7.6.1	Das Apache-Modul <code>prefork</code>	163
7.6.2	Das <code>worker</code> -Modul	168
7.6.3	Das <code>perchild</code> -Modul	168
7.6.4	Tuning-Tipps und Benchmarking	171
7.7	Übungen	175
7.8	Lösungen	176
7.9	Querverweise	179
8	Grundlagen E-Mail	181
8.1	Übertragung von E-Mails	181
8.2	Das Simple Mail Transfer Protocol (SMTP)	183
8.3	Aufbau einer Nachricht	184
8.4	Adressen	185
8.5	Zusammenspiel von Mail-Übertragung und DNS	186
8.6	Postfächer zentral verwalten	187
8.7	Wissensfragen	189
8.8	Lösungen	190
9	sendmail - der Dinosaurier unter den Mailservern	191
9.1	Einleitung, Historie	191
9.2	Kurzübersicht sendmail -Administration	192
9.3	Konfigurationsdatei <code>sendmail.cf</code>	192
9.4	Veränderung der mitgelieferten <code>sendmail.cf</code>	192
9.5	Konfiguration mit m4 -Makrodateien	194
9.6	Routing von E-Mails	195
9.7	Adressmanipulationen	198

9.7.1	Absenderadressen ausgehender Mails umschreiben	198
9.7.2	Empfängeradressen eingehender Mails umschreiben	200
9.8	Zugriffskontrolle	205
9.9	Sonstige Optionen	207
9.10	Beispielkonfigurationen	208
9.10.1	Konfigurations eines einfachen Mail-HUB	208
9.10.2	Standalone Rechner mit vollem Internetzugang	209
9.10.3	Arbeitsplatzrechner in einem Firmennetz	210
9.10.4	Zentraler Mailserver in einem Firmennetz	211
9.10.5	Mailserver mit Dialup-Verbindung	213
9.11	Testen / Fehlersuche	214
9.12	Wissensfragen	216
9.13	Lösungen	218
9.14	Übungen	221
9.15	Lösungen	222
9.16	Querverweise	226
10	postfix - schnell, sicher, robust	227
10.1	Einleitung	227
10.2	Kurzübersicht postfix -Administration	228
10.3	Konfigurationsdatei <code>main.cf</code>	228
10.4	Konfigurationstabellen	228
10.5	Grundlegende Konfigurationsparameter	229
10.6	Routing von E-Mails	230
10.7	Adressmanipulationen	232
10.8	Zugriffskontrolle	238
10.9	Beispielkonfigurationen	244
10.10	Testen / Fehlersuche	249
10.11	Wissensfragen	250
10.12	Lösungen	252
10.13	Übungen	255
10.14	Lösungen	256

INHALTSVERZEICHNIS

10.15	Querverweise	260
11	Troubleshooting	261
11.1	Befehle für die Diagnose von Hardwareproblemen	261
11.2	Befehle für die Diagnose von Netzwerkproblemen	266
11.3	Probleme mit Anwendungen	267
11.4	Erstellen einer Rettungsdiskette	269
11.5	Reparieren des Bootloaders LILO	269
11.6	Reparieren von GRUB	270
11.7	Fehlerhafte Konfigurationsdateien reparieren	271
11.8	Einen Dateisystem-Check durchführen	272
11.9	Root-Passwort vergessen	273
11.10	Wissensfragen	275
11.11	Lösungen	276
12	PAM — austauschbare Authentifizierungsverfahren	277
12.1	Überblick	277
12.2	Konfiguration des PAM-Systems	279
12.2.1	Konfiguration der PAM-fähigen Anwendungen	279
12.2.2	Austausch des Authentifizierungsverfahrens	284
12.3	Wissensfragen	287
12.4	Übungen	289
12.5	Lösungen	290
13	SSH: Sicherer Zugriff auf entfernte Rechner	293
13.1	Das SSH-Protokoll	294
13.2	Den SSH-Client verwenden	297
13.2.1	ssh	297
13.2.2	scp	299
13.2.3	sftp	300
13.3	Den SSH-Server sshd administrieren	302
13.3.1	Wichtige Dateien	302

13.3.2	Die Konfiguration von sshd	304
13.3.3	Die Konfiguration von ssh	308
13.4	Weitergehende Anwendungen für SSH	308
13.4.1	Varianten zur Authentifizierung	309
13.4.2	Tunneln von TCP/IP-Protokollen	313
13.4.3	Tunneln des X-Server Protokolls	314
13.5	Fehlersuche	314
13.6	SSH-Clients für Windows und MacOS	315
13.7	Das Wichtigste in Kürze	316
13.8	Wissensfragen	318
13.9	Lösungen	320
13.10	Übungen	321
13.11	Lösungen	322
14	Host-Security	325
14.1	Buffer Overflow	326
14.2	Die <i>tmp-race</i> -Problematik	327
14.3	Gegenmaßnahmen	327
14.3.1	<i>SUID</i> -Programme entschärfen	328
14.3.2	Sonderfall Dateirechte bei der SuSE-Distribution	329
14.4	Dämonen	330
14.4.1	Der [x]inetd	330
14.4.2	Startskripte	332
14.5	Physikalischer Zugriff	333
14.5.1	Sicherheitsloch Bootmanager	333
15	Iptables (Netfilter)	337
15.1	Grundlagen	337
15.2	Regeln erstellen und bearbeiten	340
15.3	Erweiterungen	344
15.3.1	Negieren von Merkmalen	344
15.3.2	Flags im TCP-Header	344

INHALTSVERZEICHNIS

15.3.3	ICMP-Pakete	345
15.3.4	Eigene Regellisten	347
15.3.5	Filtern nach der MAC-Adresse	348
15.3.6	Limits setzen	348
15.4	Stateful Inspection	349
15.5	Network Address Translation	349
15.6	Masquerading als spezielle Form des NAT	351
15.7	Skripte, Konfigurationstools	353
15.7.1	Ein Beispielskript	353
15.7.2	Weitere Befehle	354
15.8	Wissensfragen	356
15.9	Lösungen	359
16	Intrusion Detection Systeme	361
16.1	IDS: Alarmanlagen im Netz	361
16.2	Spurensuche im Dateisystem: tripwire	361
16.2.1	Installation	362
16.3	Einfaches IDS mit ipchains/iptables	367
16.4	IDS mit snort	367
16.4.1	Installation	368
16.4.2	Falscher Alarm	369
16.4.3	Alte Bekannte: Angriffe aus der Trickkiste	371
16.4.4	Fallensteller	372
16.4.5	Analyse mittels snortsnarf.pl	373
16.5	Übungen	375
16.6	Querverweise	376
I	Anhang	377
A	Besonderheiten von Fedora/RedHat	378
A.1	Übersicht	378
A.2	Die Fedora/RedHat-spezifischen Konfigurationsdateien	379

A.3	Netzwerkkonfiguration	379
A.4	Konfiguration des Init-Systems	381
A.5	Wissensfragen	384
A.6	Übungen	385
A.7	Lösungen	386
B	Besonderheiten der Debian-Distribution	387
B.1	Übersicht	387
B.2	Netzwerkkonfiguration	387
B.3	Konfiguration des Init-Systems	389
B.4	Wissensfragen	392
B.5	Übungen	393
B.6	Lösungen	394
C	Literaturhinweise	395
D	Stichwortverzeichnis	399