

- .exrc*, 199
 - .rhosts*, 199–200
 - /boot/grub/menu.lst*, 124, 157–159
 - /dev/*, 197
 - /etc/*, 196
 - /etc/aliases*, 122
 - /etc/fstab*, 171–173
 - /etc/host.conf*, 256
 - /etc/hosts*, 256
 - /etc/hosts.allow*, 182
 - /etc/hosts.deny*, 182
 - /etc/hosts.equiv*, 199–200
 - /etc/hosts.lpd*, 199–200
 - /etc/inetd.conf*, 179
 - /etc/init.d/depend.boot*, 130
 - /etc/init.d/depend.start*, 130
 - /etc/init.d/depend.stop*, 130
 - /etc/inittab*, 125
 - /etc/lilo.conf*, 125, 159–161
 - /etc/modprobe.conf*, 162
 - /etc/modules.conf*, 162
 - /etc/named.conf*, 434–436
 - /etc/networks*, 256
 - /etc/nsswitch.conf*, 256
 - /etc/peers/<name>*, 227
 - /etc/ppp/chap-secrets*, 228, 234, 242, 248, 251
 - /etc/ppp/options*, 248–249
 - /etc/ppp/ip-down*, 228, 249, 252, 305–306, 349
 - /etc/ppp/ip-up*, 228, 249, 252, 305–306, 349
 - /etc/ppp/options*, 227–229
 - /etc/ppp/options.<ttyname>*, 227
 - /etc/ppp/pap-secrets*, 227, 234, 242, 248, 251
 - /etc/ppp/peers/*, 248, 250–251
 - /etc/ppp/peers/<name>*, 231–233, 240–242
 - /etc/protocols*, 180
 - /etc/resolv.conf*, 254
 - /etc/services*, 180, 527
 - /etc/sysconfig/security*, 194
 - /etc/sysconfig/syslog*, 208, 217
 - /etc/syslog-ng/syslog-ng.conf*, 208–214
 - /etc/syslog-ng/syslog-ng.conf.ini*, 208
 - /etc/syslog.conf*, 206–207
 - /procl/*, 166–171
 - /usr/src/linux/Makefile*, 152
 - ~/ppprc*, 227
 - 1TR6, 140, 143, 149, 246
- A**
- Abnahmetests, 441–451
 - accton, 145
 - ACK-Storm, 50
 - ActiveX-Controls, 59
 - Installation von Trojanern, 54
 - signierte, 60
 - Adresse
 - IP, *siehe* IP-Adresse
 - logische, 25
 - MAC, 20
 - Spoofing, 45–46
 - Advisories, 535–536

- agetty, 577
- AIDE, 468–474
- aide.conf*, 468
- Aktive Inhalte, 59–61, 534
- Angriffe
 - ARP Cache Poisoning, *siehe* ARP Cache Poisoning
 - ARP Spoofing, *siehe* ARP Cache Poisoning
 - auf Applikationen, *siehe* Applikationen, Fehler in
 - auf die Privatsphäre, *siehe* Privatsphäre
 - Cracking, *siehe* Cracking
 - Denial-of-Service, *siehe* DoS-Angriffe
 - DNS, *siehe* DNS, Angriffe, *siehe* DNS, Angriffe
 - Flooding, *siehe* Flooding
 - Fragmentierung, *siehe* Fragmentierung, als Angriff
 - ICMP, *siehe* ICMP, Angriffe, *siehe* ICMP, Angriffe
 - Insider-, 7
 - IP-Spoofing, *siehe* IP-Spoofing
 - Man-in-the-Middle-Attacks, *siehe* Man-in-the-Middle-Attacks
 - Phishing, *siehe* Phishing
 - Raten von TCP-Folgennummern, *siehe* TCP, Folgennummern, Raten von
 - Sniffing, *siehe* Sniffing
 - Social Engineering, *siehe* Social Engineering
 - Source Routing, *siehe* Source Routing, als Angriff
 - Telnet-Hijacking, *siehe* Telnet-Hijacking
 - Trojaner, *siehe* Trojaner
 - Würmer, *siehe* Würmer
- Applikationen
 - Fehler in, 36–37
- aptitude, 119–121
- ARP, 20–21
 - Cache, 48
 - Proxy-, *siehe* Proxy-ARP
- arp, 355
- ARP Cache Poisoning, 48–49
- ARP Spoofing, *siehe* ARP Cache Poisoning
- at, 179, 191
- atd, 179, 189
- awk, 194
- B**
- Backup, 109, 483–500
- Banner Grabbing, 33
- bash, 186
- batch, 179
- Beispielskripte
 - arpit, 355–357
 - checksummer, 460–463, 560–562
 - confcheck, 200–203, 453, 556–560
 - delcat, 583–584
 - dmz.ipchains, 364–375
 - dmz.iptables, 382–397
 - dsl, 243–245
 - echolot.sh
 - ipchains, 258–260
 - iptables, 263–266
 - ethdevs, 222–225
 - gpm
 - Debian, 133
 - SuSE, 127–132
 - isdn, 252–253
 - logarc, 502
 - logfilter.sh, 513–519
 - md5verify, 464–465, 560
 - modem, 235–236
 - modload, 164
 - pfilter.ipchains, 297–305
 - pfilter.iptables, 338–349
 - proconf, 169
 - pseudo, 36
 - siminternet, 443–444
- Benutzer
 - Schulung, 532–535
- Betriebssystemerkennung, 32–33
- bind, 430–440

chroot-Umgebung, 430–434

BIOS, 123

BIOS-Paßwort, 123

Bootloader, 123–125

Bootreihenfolge, 123

Bootvorgang, 123–134

Meldungen, 173

Botnet, 52, 63

busybox, 466–467, 545

C

cat, 490

cdrecord, 493–494

CGI-Skripte, 36

chage, 192

Chain, 307

CHAP, 228, 234, 242, 251

chat, 233–234, 241

checkproc, 132

Checksummer, 42, 453–483

md5sum, *siehe* md5sum

chfn, 192

chmod, 193

chroot, 500

chsh, 192

Cluster

verlorene, 455

comm, 561–562

cons.saver, 193

Cookies, 56

Coroner's Toolkit

Kompilation, 554–555

crack, 535

Cracking, 31–52

Cron, 175

cron, 187

Cronjob, 175

crontab, 191

Crontabs, 175

Cryptographic Handshake Authentication Protocol, *siehe* CHAP

D

date, 544

Dateianhänge, 54

Dateien

versteckte, 200

Dateirechte

Entfernung unsicherer, 189–197

dd, 553

DDoS-Angriffe, *siehe* DoS-Angriffe, ver-
teilte

debugfs, 579–584

Demilitarisierte Zone, *siehe* DMZ

Denial-of-Service-Angriffe, *siehe* DoS-
Angriffe

depmod, 154

Devices, 161–163

Block-, 162

Character-, 162

Finden unsicherer, 197–198

Major-Nummer, 162

Minor-Nummer, 162

df, 540

Dialer, 53

automatische Installation, 54

Dienste

Aufspüren überflüssiger, 184–187

Entfernen überflüssiger, 187–188

dig, 440, 523

disable-paste, 192

Diskettenlinuxe, 75–102

Coyote Linux, 78–89

fli4l, 90–102

dmesg, 173

DMZ, 7, 72

Einrichtung, 351–397

Paketfilter, 359–397

ipchains, 360–375

iptables, 375–397

Reverse Proxy, 357–359

DNS, 25–26

Angriffe, 32, 51–52

Zone Transfer, 32

Domänen, 25

Filterung

ipchains, 284–285

iptables, 324–325

Port Scans, 525

rekursive Anfrage, 26

Resource Record, *siehe* RR

- Root-Server, 25
- Top Level Domain, 25
- Zone Transfer Request, 26
- Zonen, 25
- DNS-Server
 - Benutzung eines, 254
 - einrichten, *siehe* bind
- Dokumentation, 530–532
- DoS-Angriffe, 27–30
 - Flooding, *siehe* Flooding
 - ICMP, *siehe* ICMP, Angriffe, Destination Unreachable, *siehe* ICMP, Angriffe, Manipulation des Routing
 - Reflektor-, 28–29
 - verteilte, 28–29, 43
 - DDoS-Zombies, 53
- DoubleClick, 57
- DSL
 - Konfiguration, 227–245
- DSS1, 140, 143, 149, 246
- du, 37, 540
- dump, 106
- E**
- EAZ, *siehe* MSN
- egrep, 508
- eject, 191
- elvis, 600
- Endgeräte-Auswahlziffer, *siehe* MSN
- Ethernet-Protokoll, 17, 20
- Euro-ISDN, *siehe* DSS1, *siehe* DSS1, *siehe* DSS1
- Exim
 - Mailversand an root, 121–122
- exim, 118, 189, 193
- expiry, 192
- F**
- fdisk, 484, 496–497, 552
- Feld-Separator, 41
- Fernwartung, 36
- Filesharing
 - dauernde Verbindungsanfragen, 526
 - eDonkey2000, 527
 - eMule, 527
 - Kazaa, 526
- find, 187, 188, 194, 195, 197, 458
- Finger
 - Port Scans, 525
- Fingerprinting, 33
- Firewall
 - allgemeine Erklärung, 5–9
 - Einsatzszenarien, 9–14
 - Konzepte, 65–73
 - Schwachstellen, 7–9
- Flooding, 27–30
 - SYN-, 27
 - Gegenmaßnahmen, *siehe* Syn-cookies
- fold, 584
- Fragmentierung, 19
 - als Angriff, 37–39
- fsck, 172, 455
- FTP
 - aktives, 292, 330
 - Filterung
 - ipchains, 292–295
 - iptables, 330–331
 - passives, 292, 330
 - Port Scans, 525
- ftp, 117
- ftp-proxy, 189, 418–430
 - chroot-Umgebung, 420–424
- G**
- Gopher
 - Filterung
 - ipchains, 289
 - iptables, 328–329
- gpg, 191
- gpm, 127, 132, 134
- grave-robber, 569
- grep, 185, 187, 508–510
- growisofs, 494–496
- Grub
 - Konfiguration, 157–159
 - Sicherheit, 124–125
- gunzip, 499
- gzip, 465, 490

H

halt, 127, 132
Hardware-Anforderungen, 108–109
Header, 17
hex, 589
host, 523
HTTP
 Anfrage, 58
 Filterung
 ipchains, 286–287
 iptables, 326
 Header
 Filterung, 58
 Host, 58
 Referer, 57
 User-Agent, 58
HTTPS
 Filterung
 ipchains, 289–290
 iptables, 329–330
Hub, 45

I

icat, 579, 583–584
ICMP, 21
 Angriffe, 30, 49–50
 Destination Unreachable, 30
 Manipulation des Routing, 30, 49–50
 Redirect, 30, 49
 Router Discovery Protocol, 30, 50
 Destination Unreachable, 21, 279, 321
 Echo Reply, 21, 32, 279, 321
 Echo Request, 21, 32, 280, 321
 Filterung
 ipchains, 279–281
 iptables, 320–322
 Nachrichtentypen, 279–281, 320
 Parameter Problem, 21, 281, 321
 Redirect, 21, 280, 321
 Router Advertisement, 21, 280, 321
 Router Discovery Protocol, 21

 Router Solicitation, 21, 280, 321
 Source Quench, 21, 280, 321
 Time Exceeded, 21, 280, 321
Ident, 528
 Filterung
 ipchains, 285–286
 iptables, 317–318
IDS, 33, 49, 593
ifconfig, 220, 248
ils, 569, 583–584
ils2mac, 555, 569
IMAP
 Filterung
 ipchains, 288
 iptables, 327–328
 Port Scans, 526
IMAPS
 Filterung
 ipchains, 289–290
 iptables, 329–330
imond, 94
in.telnetd, 577
inetd, 179–184
inetd, 189, 546, 571
init, 124–134, 186, 577
Inodes, 568–586
 Erklärung, 568
 gelöschte, 578–586
insserv, 129, 166, 171, 355
Installation
 Paketauswahl
 Debian, 119–121
 SuSE, 116
 Vorgehen, 109–110
Intrusion Detection System, *siehe* IDS
IP, 18–20
 Header, 38
 Time to Live, *siehe* IP, TTL-Feld
 TTL-Feld, 19, 21, 522
 Type-of-Service-Feld, 274
IP-Adresse, 19
 Adressen für private Subnetze, 20
 Broadcast, 20
 Netzwerk-Adresse, 20
 unspezifizierte, 20

- IP-Spoofing, 46–48
- ipchains, 269–306
 - DMZ, 360–375
- ipchains-restore, 275
- ipchains-save, 275
- ipconfig, 167, 262, 267
- ippod, 248–252, 443
- iptables, 306–349
 - DMZ, 375–397
- ISDN
 - Modems, 246
 - 1TR6, *siehe* 1TR6, *siehe* 1TR6, *siehe* 1TR6
 - analoges Modem über, 246
 - Asynchrones PPP, *siehe* PPP, asynchrones
 - DSS1, *siehe* DSS1, *siehe* DSS1, *siehe* DSS1
 - Euro-, *siehe* DSS1, *siehe* DSS1, *siehe* DSS1
 - Konfiguration, 245–254
 - Raw IP, *siehe* Raw IP
 - Synchrones PPP, *siehe* PPP, synchrones
- isdnctrl, 247
- J**
- Java-Applets, 59, 60
- JavaScript, 59
- JScript, 59
- K**
- Kernel, 135
 - Bootoptionen, 155–157
 - Erstellung eines, 135–173
 - Installation, 154–161
 - Kompilation, 150–153
 - Serie 2.6, 152–153
 - Serien 2.2 und 2.4, 150–152
 - Konfiguration
 - Kernel 2.2, 137–140
 - Kernel 2.4, 140–143
 - Kernel 2.6, 144–150
 - modularer, 136
 - monolithischer, 136
- kill, 181
- killall, 182
- killproc, 132, 133
- klogd, 187
- L**
- lophtcrack, 535
- lastcomm, 145
- lazarus, 554, 586–591
- less, 200, 507, 513, 558
- LiLo, 112
 - Konfiguration, 159–161
 - Sicherheit, 125
- lilo, 500
- logger, 215
- Logical Block Addressing, 160
- login, 186, 577–578
- logrotate, 503–506
- ls, 41, 42, 200
- lsmold, 154
- lsodf, 545–548
- M**
- MAC-Zeiten, 568–578
- mactime, 570
- mail, 122
- man, 191, 474, 483
- Man-in-the-Middle-Attacks, 48
 - ARP, *siehe* ARP Cache Poisoning
 - DNS, *siehe* DNS, Angriffe, Spoofing
 - ICMP, *siehe* ICMP, Angriffe, Manipulation des Routing
 - TCP, *siehe* Telnet-Hijacking
- mandb, 191
- Masquerading, 69–70
 - iptables, 336–337
- mcopu, 204
- md5sum, 56, 456–468, 560–562
- mingetty, 186
- minicom, 229
 - Test des Modems mit, 229–231
- mkdir, 216
- mke2fs, 497
- mkisofs, 493–494
- mkswap, 497
- Modem

- Konfiguration, 227–245
- modeprobe, 164
- modprobe, 136, 154, 161, 162
- Module, 136
 - als Angriffswerkzeug, 136
 - Kompilation u. Installation, 153–154
 - Konfiguration, 161–164
 - Laden beim Systemstart, 164–166
- more, 558
- mount, 172, 191
 - noatime, 578
 - nodev, 204, 466, 555
 - noexec, 204, 466, 555
 - ro, 204, 466, 555
- MSN, 246
- mt, 489
- Multiple Subscriber Number, *siehe* MSN

N

- NetBIOS
 - Filterung
 - ipchains, 278–279
 - iptables, 320
 - Port Scans, 526
- netcat, 444–445
- netstat, 184–185
 - trojanisiert, 546
- Network Address Translation, 68–70
 - Masquerading, *siehe* Masquerading
 - Redirection, *siehe* Redirection
- Netzwerk
 - einrichten, 219–256
 - Tests, 257–268
- Netzwerkkarte
 - Konfiguration, 219–227
- nice, 460
- NIS, 35
- nmap, 446–449
- NNTP
 - Filterung
 - ipchains, 288–289
 - iptables, 328

- nscd, 545

P

- Paketfilter, 65–66
 - Konfiguration
 - ipchains, 269–306
 - iptables, 306–349
- pam_auth, 193
- PAP, 227, 234, 242, 251
- Partitionierung, 112–114
- passwd, 192
- Password Authentication Protocol, *siehe* PAP
- PATH-Variable, 41
- Paßwortdatei
 - Knacken, 40
 - Shadow, 41
- Paßwörter
 - lokal gespeicherte, 44
 - schlechte, 39, 251
 - Standard-, 36
 - unsichere, 534–535
- pcAnyware
 - Port Scans, 527
- Phishing, 63–64
- PID, 181
- ping, 139, 191, 257
- ping6, 191
- Policy, 7, 103–108
- POP2
 - Port Scans, 525
- POP3
 - Filterung
 - ipchains, 287–288
 - iptables, 327
 - Port Scans, 526
- POP3S
 - Filterung
 - ipchains, 289–290
 - iptables, 329–330
- Port Scanning, 33–34, 446–451
 - FIN-, 446
 - SYN-, 446
 - UDP-, 448
- Portnummer, 22

- postfix, 118
 - PPP
 - synchrones, 245
 - Konfiguration, 247–254
 - PPP over Ethernet, *siehe* PPPoE
 - pppd, 227–245, 443
 - PPPoE, 237
 - Verbindungsaufbau, 239
 - pppoe, 237, 241
 - Verbindungstest mit, 238–239
 - Privatsphäre, 56–58
 - Privoxy
 - Action Files, 414
 - Filter, 414
 - privoxy, 189, 405–418
 - chroot-Umgebung, 406–409
 - Promiscuous Mode, 21
 - Protokoll, 17
 - Arp, *siehe* ARP
 - DNS, *siehe* DNS
 - Ethernet, *siehe* Ethernet
 - ICMP, *siehe* ICMP
 - Ident, *siehe* Ident
 - IP, *siehe* IP
 - NetBIOS, CIFS, SMB, *siehe*
 - Windows-Netzwerk
 - NIS, *siehe* NIS
 - SOCKS, *siehe* SOCKS
 - SSH, *siehe* SSH
 - TCP, *siehe* TCP
 - Telnet, *siehe* Telnet
 - TFTP, *siehe* TFTP
 - UDP, *siehe* UDP
 - Whois, *siehe* Whois
 - X, *siehe* X
 - Protokolle
 - Store and Forward-, 333
 - syslog, *siehe* Systemprotokoll, Protokollierung über das Netzwerk
 - Proxies, 67–68
 - DNS
 - bind, *siehe* bind
 - Einrichtung, 399–440
 - Filterregeln für
 - ipchains, 290–291, 294–295
 - iptables, 331–333
 - FTP
 - ftp-gw, *siehe* ftp-gw
 - transparente, 70
 - ipchains, 291–292
 - iptables, 333–335
 - squid, 405
 - Web-
 - http-gw, *siehe* http-gw
 - Internet Junkbuster, *siehe* junkbuster
 - squid, *siehe* squid
 - Proxy
 - cachender, 6
 - Proxy-ARP, 353–357
 - Prozessnummer, *siehe* PID
 - ps, 42, 136, 181, 185
 - trojanisiert, 545–546
 - pt_chown, 193
- ## R
- R-Dienste, 35, 42
 - Raw IP, 245
 - rcp, 191
 - reboot, 127, 132, 173
 - Rechnerdaten, 110–111
 - Redirection, 70
 - Reguläre Ausdrücke, 508–510
 - Remote Shell, 53
 - resmgrd, 186
 - Resource Record, *siehe* RR
 - Rettungssystem, 42, 203, 496
 - Reverse Proxy, 357–359, 419
 - DMZ Einrichtung für, *siehe* DMZ, Reverse Proxy
 - Richtlinien, 105–108
 - Anwender-, 106
 - Betriebs-, 107
 - Vorfallsbehandlung, 539–540
 - rlogin, 191
 - rmmod, 154
 - Rootkit, 42, 136, 203, 453
 - Anzeichen für ein, 540
 - Rootrechte

- Erlangung, 40
- route, 220–222, 248, 262, 267
- Router, 18
- Routing
 - Manipulation, 30, 49–50
- rpm, 191
- RR, 436–437
 - A, 437
 - CNAME, 437
 - HINFO, 437
 - MX, 437
 - NS, 437
 - PTR, 438
 - SOA, 436–437
 - TXT, 437
- rsh, 191
- Runlevel, 125
 - Debian, 132–133
 - SuSE, 126–127

S

- Screened Host Firewall, 71–72
- Screened Subnet Firewall, 72–73
- script, 543
- Script Kiddies, 1, 31
- sed, 507, 573
- Sendmail, 36
- SGID-Bit, 190
 - Entfernung, 190–195
- sh, 37
- Signale, 181–182
 - SIGHUP, 181
 - SIGINT, 181
 - SIGKILL, 181
 - SIGTERM, 181
- Skriptsprachen, 59, 61
- SMB over TCP
 - Port Scans, 526
- SMTP
 - Filterung
 - ipchains, 287
 - iptables, 326–327
 - Port Scans, 525
- Sniffer, 21
- Sniffing, 44, 47

- SNMP
 - Port Scans, 526
- Social Engineering, 32, 62–64
- SOCKS, 68
- sort, 507
- Source Routing, 19
 - als Angriff, 47
- Speicherüberläufe, 36
- split, 490
- Spyware, 55
- squid, 189, 193, 400–405
- SSH, 108
- ssh, 192
- sshd, 186–189, 559
- start-stop-daemon, 133, 218
- startproc, 131–133
- Stateful Packet Filtering, 66
- strace, 562
- strings, 563–567
- su, 192, 521
- SUID-Bit, 42, 190
 - Entfernung, 190–195
- SUID-Programme, 40
 - Shellskripte, 41
- SuSE Proxy-Suite, *siehe* ftp-proxy
- SuSEconfig, 194, 195, 208
- Swap-Partition, 113
- Switch, 45
 - als Schutz, 45, 51
- sync, 127, 132
- Syncookies, 29
 - Aktivierung, 167
- syslog-ng, 187, 208–218
- syslogd, 168, 206–208, 501
- sysstat, 184
- Systemprotokoll, 205–218, 501–530
 - Filterung, 506–520
 - Konfiguration für chroot, 423–424
 - Meldungen bewerten, 520–530
 - Protokollierung über das Netzwerk, 25
 - Rotation, 501–506

T

- Table, 307

tar, 485–487
TAR-Archiv
 Aufbau, 590
TCP, 21–24
 Flags, 23
 Folgenummern, 23
 Raten von, 47
 Verbindungsaufbau, 24
TCP/IP Stack Fingerprinting, *siehe* Fingerprinting
tcpd, 182–184, 577
Technische Spezifikation, 106
Telnet, 108
 Port Scans, 525
telnet, 576
Telnet-Hijacking, 50–51
Temporäre Dateien, 41
TFTP, 35
tomsrtbt, 496
Topologie, *siehe* Verkabelung
tr, 584
Traceroute, 528–530
traceroute, 281, 529, 530
tracert, 281
Tripwire, 474–483
Trojaner, 52–56, 108, 527, 533–534
 Bubbleboy, 61
 Christmas.Exec, 533
 Dialer, *siehe* Dialer
 Happy99, 533
 Kettenbrief-, 53
 Remote Shell,
 see Remote Shell53
 Spyware, *siehe* Spyware
tune2fs, 484
twadmin, 476

U

udev, 186, 198
UDP, 24–25
umount, 191
uniq, 507
unix2_chkpwd, 192
unix_chkpwd, 192
unrm, 586

Updates, 535–537

V

VB-Script, 59
Verkabelung
 Bus-, 45
 Stern-, 45, 51
vi, 596–600
vim, 600
Virus, 108
Vorfallsbehandlung, 539–594

W

Wahlsperre, 232
WAIS
 Filterung
 ipchains, 289
 iptables, 328–329
wall, 192
Warnmeldungen, *siehe* Advisories
Web Bugs, 57
Werbebanner, 57
which, 483
Whois, 523–525
Windows Scripting Host, 59
Windows-Netzwerk, 35
write, 192
Würmer, 52
 E-Mail-, *siehe* Trojaner, Kettenbrief, 61, 533

X

X, 35
xxd, 589

Y

yast, 139, 141, 146, 194
ypcat passwd, 35

Z

Zertifikat, 60