

Index

Symbols

- (dash), 134, 142
- (hyphen), 493
- . (dots), 134
- . (period), 518
- / (forward slash), 134, 163, 299
- : (colon), 162, 293
- ; (semicolon), 230, 382
- \ (backslash), 134, 230, 369
- | (pipe), 231, 244
- + (plus sign), 474
- = (equal sign), 293
- # (pound sign; hash mark), 283, 337, 382
- \$ (dollar sign), 470
- \$? variable, 498
- \$\$ variable, 498
- \$* variable, 498
- \$@ variable, 498
- \$^ variable, 498
- \$< variable, 498
- * (asterisk), 233–235, 282
- ? (question mark), 233–235, 356
- [] (bracket), 234
- < (less-than sign), 232
- > (greater-than sign), 232

A

- absolute navigation, 140
- absolute paths, 518
- access logs, Apache server, 339–341
- access point (AP), 204–205
- AccessFileName directive, 338
- ACPI Shutdown function (VirtualBox), 50

- acpi=off boot option, 72
- action field, 256
- Activities overview area, GNOME, 91
- ad hoc mode, 201
- Add/Remove Applications program, 79
- address command, 214
- addlabel command, 214
- Adjust Window Size, 51
- Advanced Encryption Standard (AES), 202
- After line, 261–262
- alias command, 236, 475
- alias file, 395–396
- allowcdma boot option, 72
- Amarok, 128
- answer variable, 474
- Apache server
 - access logs, 339–341
 - basic setup, 337–339
 - configuring, 336–343
 - creating secure web server, 343–344
 - error logs, 339–341
 - features, 332
 - installing, 333–336
 - overview, 319, 331–332
 - user web hosting, 341
 - virtual web hosting, 341–343
 - vulnerabilities, 454
- Apache Software Foundation, 518
- apic boot option, 72
- appearance, customizing, 92
- applets
 - Cinnamon desktop, 106–107
 - MATE desktop, 110

- Xfce desktop, 113–114
- application gateway, 413
- Application Launcher, KDE Plasma, 95
- Application layer (TCP/IP), 186
- application-proxy gateway firewall, 441–442
- apropos command, 236
- apt tool, 380, 396
- AR variable, 498
- ARFLAGS variable, 498
- arguments, 58
- ARPANET, 187
- AS variable, 498
- ASCII-armored format, 429
- ASFLAGS variable, 498
- ash shell, 16
- assumptions, in this book, 2–3
- asterisk (*), 233–235, 282
- asymmetric DSL (ADSL), 177–178. *See also* DSL (Digital Subscriber Line)
- at command, 278–280
- atd daemon program, 278
- atrm command, 280
- audio
 - GNOME Sound options, 125
 - KDE Plasma multimedia settings, 126–127
 - listening to, 124–129
 - MP3 libraries, 127
 - players
 - Amarok, 128
 - Rhythmbox, 128
 - streaming versus downloading, 128
 - troubleshooting, 124
- authentication, 408, 413, 454

authorization, 409
AVI files, 129
awk language, 482–486

B

backdoor, 413
background, customizing, 92
background processes, running, 314–315
backing up files, administrator's duties, 250
backslash (\), 134, 230, 369
bandwidth throttling, 332
base station, 202
Bash shell
 built-in commands, 475–478
 commands
 combining, 231
 controlling input and output, 231–233
 for file management, 230
 format, 228–229
 syntax of, 228–230
 wildcards, 233–235
 controlling flow of execution, 471–474
 defined, 228
 defining variables, 469–470
 described, 16
 programming features, 469–470
 starting, 56–57
 using, 228–235
 .bash_history file listing, 138
bastion host, 413
Berkeley Internet Name Domain (BIND) software, 328
bg command, 238, 475
/bin directory, 229, 300
binary files, 237
BIND (Berkeley Internet Name Domain) software, 328
BIND DNS, 454

binmail program, 324
bit bucket, 233
black hat, 460
black-box testing, 460–461
BogoMIPS, 271
/boot directory
 defined, 300
 /grub/menu.lst file, 456
boot disk, creating, 28–30
boot messages, 54
boot process
 Systemd method, 259–263
 SysVinit method, 252–259
bootable DVD
 booting from, 31
 creating, 28–29
bootable USB stick, creating, 29–30
booting, 53
Bourne, Stephen, 16
Bourne shell, 16
bracket ([]), 233–235
breadcrumbs, 150
break command, 475
break NUM command, 504
bt command, 504
buffer, 165
buffer overflow, 413

C

C compiler, 489
C programming language, 490
C++ programming language, 490, 492–493
cable modem connections
 compared to DSL, 175
 data transfer speeds, 182
 general discussion, 175
 LAN connections, 197–198
 overview of function, 180–182
 typical setup, 182–184
Cable Modem Termination System (CMTS), 182
cal command, 243
Carrier-Sense Multiple Access/ Collision Detection (CSMA/CD), 191
case statement, 473
cat command, 155, 230, 237, 245
CC variable, 498
cd command, 236, 475, 519
CD-ROMs, managing, 76–77
CentOS, 67
CERT Software Engineering Institute of Carnegie Mellon University, 418
certificate authorities (CAs), 414
certificates, 414
certification. *See* Linux certification
certified engineer, 536
certified IT associate, 536
certified system administrator, 536
CFLAGS variable, 498
CGI (Common Gateway Interface), 332
chage command, 417
charset command, 357
check digit, 482
chgrp command, 295
chkconfig command, 258
chmod command, 236, 423
chown command, 143, 295
CIFS (Common Internet File System), 379
Cinnamon desktop
 applets, 106–107
 desklets, 106–107
 features, 104–105
 general discussion, 103–104
 history of, 104–105
 menu, 105
 spices, 106–107
 system settings, 105–106

- clear command, 356
- clear *FILENAME: NUM* command, 504
- clients, 314
 - listening for, 316–318
- client-server network, 325
- CQ variable, 498
- COFLAGS variable, 498
- colon (:), 162, 229, 293
- command interpreter, 56
- command line, 58, 228
- command-line interface (CLI), 15–16, 136–137
- command-line options, 228
- Common Gateway Interface (CGI), 332
- Common Internet File System (CIFS), 379
- Common Unix Printing System (CUPS), 326
- Common Vulnerabilities and Exposures (CVE), 453
- compiler, 488, 489
- compress command, 238
- CompTIA Linux+ exams
 - overview, 530
 - Scripting, Containers, and Automation domain, 533
 - Security domain, 532
 - System Management domain, 531–532
 - Troubleshooting domain, 533–534
- computer program, defined, 488
- computer security
 - audits
 - benefits of, 450
 - methodology, 452–460
 - network-security review, 458–460
 - nontechnical aspects of, 450–451
 - overview, 449–450
 - security testing tools, 461–463
 - technical aspects of, 451
 - vulnerability testing types, 460–461
 - authentication, 413
 - backdoor, 413
 - bastion host, 413
 - buffer overflow, 413
 - certificate authorities (CAs), 414
 - certificates, 414
 - chage command, 417
 - common vulnerabilities, 453–454
 - confidentiality, 414
 - cracker, 414
 - decryption, 414
 - denial of service (DoS) attack, 414
 - digital signature, 414
 - distributed denial of service (DDoS) attack, 414
 - DMZ, 414
 - dual-homed host, 414
 - encryption, 414
 - exploit tools, 414
 - firewalls, 414
 - hash, 414
 - host, 415
 - host-security review, 454–458
 - integrity, 415
 - IP spoofing, 415
 - logic bomb, 415
 - lsuf utility, 417
 - netstat utility, 417
 - nmap tool, 417, 461–463
 - nonrepudiation, 415
 - packet, 415
 - packet filtering, 415
 - passwd utility, 417
 - perimeter network, 415
 - port scanning, 415
 - proxy servers, 415
 - public key cryptography, 415
 - public key infrastructure (PKI), 415
 - screening router, 415
 - setuid program, 416
 - sniffer, 416
 - spyware, 416
 - sudo command, 417
 - symmetric key encryption, 416
 - threat, 416
 - Trojan horse, 416
 - ulimit command, 417
 - usermod command, 417
 - virus, 416
 - vulnerabilities, 416
 - war-dialing, 416
 - war-driving, 416
 - worms, 416
- Computing Technology Industry Association (CompTIA), 529
- concatenation, of
 - commands, 230
- Concurrent Version System (CVS), 454, 490
- confidentiality, 414
- configtest command, 336
- Conflicts line, 262
- connect command, 356
- continue command, 475, 504
- Control Center, MATE, 109–110
- copyleft, 518
- core Linux distributions, 17–18
- coreutils package, 12
- cp command, 230, 236
- cpio command, 238
- CPP variable, 499
- CPPFLAGS variable, 499
- cracker, 414
- cron jobs, 281–283
- cron.service unit configuration file, 261
- crontab command, 281–282
- CUPS (Common Unix Printing System), 326

`cut` command, 237, 520
CVE (Common Vulnerabilities and Exposures), 453
CVS (Concurrent Version System), 454
`CXX` variable, 499
`CXXFLAGS` variable, 499

D

daemon, 314
dash (-), 134, 142
dash, GNOME 3, 91
Data Over Cable Service Interface Specification (DOCSIS), 182
data protection, 409
database objects, creating, 370–372
database projects, creating, 360–363
database servers
 MariaDB server, 321, 349–363
 MongoDB server, 321–322
 MySQL server, 321
 PostgreSQL server, 320, 363–372
databases
 creating, 361–362
 vulnerabilities, 454
`date` command, 242
`dbgts` program, 507
`dd` command, 237
Debian. *See also* Linux distributions
 configuring Internet super server, 435
 distributions based on, 18–19
 inetd server, 435
 installing *mailutil* package, 397
 installing Postfix, 396
 installing Samba, 380
 mounting DVD or CD-ROM, 303
 network configuration files, 208
 popularity, 17
 root password, 60
 run levels, 254
 Systemd method in, 259
 text mode installation, 64
 turning off stand-alone servers, 435
 update-rc.d command, 435
debugger
 defined, 488, 490
 finding bugs, 505–508
 fixing bugs, 508–509
 gdb commands, 504–505
 overview, 502
 preparing to debug, 502
 running *gdb*, 502–503
`declare` command, 476
decryption, 414, 432–433
`default` command, 263, 264
`delimiter` command, 356
denial of service (DoS) attack, 216, 404, 407, 414
`depmod` command, 277
derived work, 510
desklets, 106–107
desktop
 Cinnamon, 103–107
 GNOME, 87–92
 KDE Plasma, 93–101
 MATE, 107–110
 Xfce, 111–114
detection, 452, 455, 458
`/dev` directory, 229, 231, 300
device drivers, 273
device files
 block devices, 274
 character devices, 275
 network devices, 275
 udev program, 275
Devices menu (VirtualBox), 51–52
`df` command, 268–269
dhclient package, 327
DHCP (Dynamic Host Configuration Protocol), 188, 189, 209, 317, 327
dhcpcd package, 327
DHCPd server, 327
`diff` command, 237
digital signature, 414, 428–429
Digital Subscriber Line. *See* DSL (Digital Subscriber Line)
directories. *See also* files
 base, 135
 creating, 140, 147
 defined, 133–134
 deleting, 148
 opening directories, 146–147
 protecting, 422–425
 removing, 140
`DirectoryIndex` directive, 338
`dirs` command, 476
`disable` command, 263
disclosure, 407
disk performance and usage, 267–270
`display EXPR` command, 504
`display=IP_address:0 boot` option, 72
displays, settings for, 92
distributed denial of service (DDoS) attack, 404, 414
DistroWatch.com (website), 19
DivX files, 129
`dmesg` command, 65
DMZ, 414
`dnf` tool, 381, 397
DNS (Domain Name System), 317, 342
DNS Security Extensions (DNSSEC) protocol, 328
DOCSIS (Data Over Cable Service Interface Specification), 182
`DocumentRoot` directive, 338, 341
dollar sign (\$), 470
Dolphin file manager, KDE Plasma

- clicking icons, 151
- location bar, 150
- opening, 149
- Places panel, 150
- status bar, 150
- toolbar, 150
- Domain Name System (DNS), 188, 189
- DOS disk partition, mounting, 308–309
- /dos directory
 - /dos, 308–309
 - /windows, 308
- dots (.), 134
- dotted decimal notation, 188
- dotted quad notation, 188
- downloading
 - music, 127, 129
 - vs. streaming, 128
- downstream data, 181
- Drag and Drop function (VirtualBox), 52
- driver modules
 - /etc/modprob.d files, 277–278
 - loading and unloading, 276–277
 - overview, 276–278
- driverdisk boot option, 72
- DSL (Digital Subscriber Line)
 - asymmetric, 177–178
 - compared to cable, 175
 - data transfer speeds, 178
 - defined, 175
 - general discussion, 175
 - high-bit-rate, 178
 - IDSL, 178
 - LAN connections, 197–198
 - local loop, 175
 - overview of function, 176–177
 - rate-adaptive, 178
 - selecting providers and plans, 179–180
 - symmetric, 178

- typical setup, 179–180
- very-high bit-rate, 178
- very-high bit-rate DSL version 2, 178
- du command, 270
- dual booting
 - about, 23
 - installing a second hard drive for, 24
 - partitioning an existing drive for, 24–27
- dual-homed host, 414
- DVDs, managing, 76–77
- Dynamic Host Configuration Protocol (DHCP), 188, 189, 209, 317, 327
- dynamic linking, 511

E

- echo command, 471, 476
- ed text editor
 - command mode, 162
 - commands, 162–164
 - defined, 161
 - deleting text, 163–164
 - editing text, 162–163
 - inserting text, 164
 - overview, 161–162
 - replacing text, 164
 - saving changes, 164
 - text input mode, 162
- edit command, 356
- edit-compile-debug cycle, 488
- ego command, 356
- egrep utility, 520
- email
 - addresses, 118
 - encrypted, 119–120
 - Evolution software, 120–121
 - hostname, 118
 - as Internet service, 174
 - KMail, 121–123
 - server, 118
 - Thunderbird, 123–124
- enable command, 263, 476
- encryption, 414, 432–433
- enforcing=0 boot option, 72
- enp0s3 network interface, 215
- env command, 292
- environmental variables, 292–294
- equal sign (=), 293
- error logs, 339–341
- error messages, saving, 233
- ErrorDocument directive, 338, 339
- ErrorLog directive, 338
- /etc directory
 - /at.allow file, 278
 - /cron.allow file, 281, 456
 - /cron.deny file, 281, 456
 - /crontab file, 283, 456
 - defined, 300
 - /at.deny file, 279
 - /exports file, 306–307, 375–377
 - /fstab file, 303–304
 - /hostname file, 210
 - /hosts file, 210
 - /hosts.allow file, 436, 448, 456
 - /hosts.deny file, 436, 448, 456
 - /inetd.conf file, 435
 - /init.d file, 448
 - /init.d/rcS file, 257
 - /inittab file, 254–256, 448
 - /logrotate.conf file, 456
 - /mail/access file, 394
 - /mail/access.db file, 394
 - /mail/certs file, 394
 - /mail/helpfile file, 394
 - /mail/local-host-names file, 394
 - /mail/mailertable file, 394
 - /mail/relay-domains file, 394
 - /mail/sendmail.cf file, 389–390
 - /mail/userdb.db file, 394

/etc directory (continued)

- /mail/trusted-users* file, 394
- /mail/virtusertable* file, 394
- /modprob.d* files, 277–278
- /nologin* file, 448
- /pam.d* file, 456
- /passwd* file, 420, 448, 456, 523
- /postfix/main.cf* configuration file, 398
- /rc.d* file, 456
- /resolv.conf* file, 210
- /rsyslog.conf* file, 434
- /samba/smb.conf* file, 379, 382
- /samba/smbusers* file, 379
- /securetty* file, 456
- /security* file, 456
- /services* file, 318
- /shadow* file, 421–422, 448, 456, 523
- /shutdown.allow* file, 456
- /ssh* file, 456
- /ssh/sshd_config* file, 437
- /ssh/ssh_config* file, 437
- /sysconfig* file, 456
- /sysctl.conf* file, 456
- /syslog.conf* file, 434, 456
- /udev/udev.config* file, 457
- /udev/vsftpd* file, 457
- /udev/vsftpd.ftputers* file, 457
- /X11/xorg.conf* file, 439
- /xinetd.conf* file, 435, 448, 457
- /xinetd.d* file, 435, 448, 457

Ethernet

- cables, 192–193
- invention of, 192
- overview of function, 191–192
- switch, 193–194

eval command, 476

Evolution email software, 120–121

exec command, 476

executable files, 237

executable permission, 139

execute permission, 143

Exim MTA package, 324

exit command, 357, 476, 521

exit status, 471

expand command, 237

expert boot option, 72

exploit tools, 414

export command, 476

expr command, 473

expressions, 488

extended partitions, 25

F

fast boot, 28

fc command, 476

FC variable, 499

FEATURE macro file, 391

Fedora. *See also* Linux distributions

- configuring Internet super server, 435

- configuring Samba, 382

- described, 18

- enabling packet filtering, 443

- installing *postgresql-server* package, 364

- iptables.rules* file, 447

- log files, 67

- mail server, 385, 386, 388–389, 393

- MATE desktop, 107–110

- run levels, 254

- systemctl* command, 435

- text mode installation, 64

- turning on/off stand-alone servers, 435

- /var/log/messages* file, 67

- xinetd* server, 435

FFLAGS variable, 499

fg command, 238, 476

fgrep utility, 520

FHS (Filesystem Hierarchy Standard), 134, 301

file command, 139, 237

file FILE command, 504

file managers

- defined, 144

- Dolphin, 149–151

- Files, 145–149

- Thunar, 151–152

File Searcher, GNOME, 152–153

file servers, 325

file sharing

- with NFS

- exporting file system with, 375–376

- installing, 374–375

- mounting, 378

- overview, 374–375

- with Samba

- configuring, 382–383

- installing, 380–381

- overview, 378–380

- resources, 384

file systems

- commands

- for file listing information, 137–139

- for viewing information about files, 137

- defined, 133–134, 297

- exporting with NFS, 306–307

- file managers, 144–152

- file types, 139

- file-system hierarchy

- FHS, 301

- overview, 298–299

- standard directories, 300

- /usr* directory, 300

- /var* directory, 301

- mounting

- DOS disk partition, 308–309

- /etc/fstab* file, 303–304

- mount* command, 302

- mount point, 302, 307
 - NFS, 307–308
 - NTFS partition, 309–310
 - overview, 299
 - unmount command, 303
 - USB sticks, 302
 - Windows disk partition, 308–309
 - navigating, 140
 - overview, 297–298
 - paper filing system analogy, 298
 - permissions, 141–144
 - root directory, 134–136
 - searching for files and folders, 152–153
 - File Transfer Protocol (FTP), 186, 189
 - file types, 139
 - FileManager function (VirtualBox), 50
 - filenames, 134
 - files. *See also* directories
 - changing user and group ownership of, 295
 - copying, 147–148, 230
 - deleting, 140–141, 148, 230
 - getting command output from, 231–232
 - moving, 147–148, 230
 - opening files, 146, 147
 - ownerships, 423
 - permissions
 - assigning, 455–457
 - changing, 423–424
 - codes, 424
 - description of, 456–457
 - set user ID, 426
 - setting default, 424–425
 - protecting, 422–425
 - reading, 59
 - renaming, 140, 230
 - saving command output in, 232–233
 - saving error messages in, 233
 - searching for, 152–153
 - signing, 431–432
 - splitting into several smaller files, 245–246
 - substituting or deleting characters from, 245
 - Files file manager, GNOME
 - context areas, 146
 - copying and moving files, 147–148
 - creating new directories, 147
 - deleting files and directories, 148
 - opening directories, 146–147
 - opening files, 146
 - opening files and running programs, 147
 - sidebar, 145
 - starting, 145
 - status bar, 146
 - toolbar, 145
 - viewing and changing permissions, 148–149
 - Filesystem Hierarchy Standard (FHS), 134, 301
 - find command, 236, 417, 521
 - fingerprint, 421, 428
 - Firefox browser
 - configuring, 117–118
 - general discussion, 117
 - settings categories, 118
 - firewalld program, 306
 - firewalls
 - application-proxy gateway firewall, 441–442
 - characteristics, 440
 - defined, 404, 405, 414, 439
 - network address translation (NAT), 442–443
 - overview, 439–440
 - packet filter firewall, 440–441
 - programs, 306
 - setting up, 439–447
 - stateful inspection firewall, 441
 - ufw, 443–444
 - flash drives, managing, 76–77
 - flow-control statements, 488
 - fold command, 237
 - folders, searching for, 152–153
 - for loop, 473
 - .forward file, 395
 - forward slash (/), 134, 163, 299
 - Free and Open Source Software (FOSS), 518
 - free command, 238
 - Free Software Foundation (FSF), 518
 - FTP (File Transfer Protocol), 317
 - Fullscreen Mode function (VirtualBox), 51
 - fullstatus command, 335, 336
 - functions, 488
- ## G
- g++ command, 493
 - GCC (GNU C and C++ compilers)
 - compiling C++ programs, 492–493
 - options, 493, 494–495
 - overview, 490
 - using, 490–492
 - gcc command, 493–494
 - gdb program
 - commands, 504–505
 - finding bugs, 505–508
 - fixing bugs, 508–509
 - overview, 502
 - preparing to debug, 502
 - running, 502–503
 - gedit text editor, 157–158
 - General Public License (GPL), 510
 - Gentoo, 17
 - get-default command, 263
 - GIAC Certifications, 536–537
 - GIMP, 130–131

- globbing, 518
- GNOME (GNU Network Object Model Environment)
 - Activities overview area, 91
 - application menu, 89
 - customizing, 92
 - dash, 91
 - desktop, 90
 - Evolution email, 120–121
 - File Searcher, 152–153
 - Files file manager, 145–149
 - general discussion, 14–15
 - history of, 87–88
 - logging out from, 61
 - menus, 88–89
 - Settings tool, 92
 - sound options, 125
 - Terminal, 57, 226–227
 - Windows overview area, 91
 - workspace selector, 91
- GNOME Shell, 88
- GNOME Videos, 130
- GNU dbm (gdbm) database library, 510
- GNU debugger
 - finding bugs, 505–508
 - fixing bugs, 508–509
 - gdb commands, 504–505
 - overview, 502
 - preparing to debug, 502
 - running gdb, 502–503
- GNU licenses
 - General Public License, 509–510
 - Library General Public License, 511
 - overview, 509
- GNU make utility
 - makefile, 495–497, 499–500
 - options for, 501–502
 - overview, 489–490, 493–495
 - running make command, 500–501
 - variables, 497–499

- GNU Project, 12
- GNU utilities, 11–12
- GNUmakefile, 495
- GnuPG (GNU Privacy Guard)
 - encrypting and decrypting documents, 432–433
 - exchanging keys, 429–430
 - generating key pair, 429–430
 - overview, 427
 - signing files, 431–432
- go command, 357
- GParted partition editor tool, 26–27
- GPL (General Public License), 510
- graceful command, 336
- graceful-stop command, 336
- Grand Unified Bootloader (GRUB), 53–54
- graphical display, 13
- graphical user interfaces.
 - See GUIs (graphical user interfaces)
- graphics cards, 13, 68
- gray-box testing, 461
- greater-than sign (>), 232
- grep command, 58, 229, 237, 243–244
- grep utility, 520
- Group directive, 338
- group role, 361
- groupadd utility, 291, 523
- groupdel command, 292
- groups
 - adding users to, 292
 - changing file ownership, 295
 - creating, 291
 - defined, 291
 - finding, 281
 - ownership, 423
 - permissions, 142, 143–144
 - removing, 292
- guest account, 55

- Guest Additions CD, 52
- GUIs (graphical user interfaces)
 - Cinnamon, 103–107
 - GNOME, 87–92
 - KDE Plasma desktop, 93–101
 - Mate, 107–110
 - overview, 56
 - tools
 - managing user accounts with, 288–290
 - system administration, 284–286
 - Xfce, 111–114
- gunzip command, 238
- gzip command, 238, 521

H

- halt command, 238
- hard limits, 289
- hard link, 523
- hard mount, 378
- hardware management, 11
- hash, 414, 428
- hash command, 476
- hash mark (#), 382
- hdparm program, 267–268
- help command, 336, 357, 475–478, 476
- help NAME command, 504
- hexadecimal digits, 204
- hidden files, viewing, 137
- high-bit-rate (HDSL), 178. *See also* DSL (Digital Subscriber Line)
- history command, 476
- /home directory, 300
- HOME environmental variable, 294
- host, 415, 419
- host security
 - file permissions, 455–457
 - incident response, 458
 - operating system updates, 455

- passwords, 457
- review, 454–458
- hostname, 118
- HOSTNAME environmental variable, 294
- host-security tools, 462
- Hypertext Transfer Protocol (HTTP), 186, 189, 317, 343–344
- Hypertext Transfer Protocol Secure (HTTPS), 318
- hyphen (-), 493

I

- ICMP (Internet Control Message Protocol) packets, 216
- icons, used in this book, 3
- id field, 256
- ide=nodma boot option, 72
- ISDL, 178. *See also* DSL (Digital Subscriber Line)
- IETF (Internet Engineering Task Force), 317
- if command, 472
- ifconfig utility, 521
- IMAP (Internet Message Access Protocol), 189
- IMAP email servers, 118
- incident handling, 409
- incident response, 458
- Include directive, 338
- independent testing, 450
- independent verification, 450
- inetd application, 316
- inetd server, 435, 458–459
- info break command, 504
- info command, 236, 519
- info files command, 504
- info func command, 504
- info local command, 504
- info prog command, 504
- info var command, 504
- infrastructure mode, 201
- init 0 command, 61
- init process, 10
- init program, 252
- input and output (I/O) redirection, 231–232
- Input menu (VirtualBox), 50–51
- insmod command, 277
- integrity, 415
- International Standard Book Number (ISBN), 482–485
- Internet access, 409
- Internet connections
 - connection options
 - cable model, 175
 - cable modem, 180–184
 - dial-up, 174, 176
 - Digital Subscriber Line (DSL), 175, 176–180
 - fiber-optic Internet, 175
 - satellite, 175–176
 - wireless hot spot, 175
 - general discussion, 173
 - Internet overview, 174
 - local area networks
 - wired (Ethernet), 185–198
 - wireless network, 199–206
 - network management
 - configuring network features, 207–216
 - editing network configuration files, 208–216
 - troubleshooting TCP/IP networks, 216–221
- Internet Control Message Protocol (ICMP) packets, 216
- Internet Engineering Task Force (IETF), 317
- Internet Message Access Protocol (IMAP), 189
- Internet Printing Protocol (IPP), 326
- Internet Protocol (IP), 209
- Internet Protocol version 6 (IPv6), 209
- Internet services,
 - defined, 313
 - Linux server
 - general discussion, 313–314
 - launching services, 314–316
 - listening for clients, 316–318
 - running background processes, 314–315
 - super-server program, 316
 - mail services
 - general discussion, 323
 - mail delivery agent, 323–324
 - mail transfer agent, 323–324
 - port number, 318
 - securing
 - configuring Internet super server, 435–436
 - configuring TCP wrapper security, 436
 - firewalls, 439–447
 - OpenSSH, 437–439
 - turning off stand-alone services, 434–435
 - security policy, 409
 - service names, 189–190
 - Web services
 - Apache server, 319
 - defined, 316
 - lighttpd package, 319–320
 - NGINX server, 316
- Internet super server, 435–436
- Internet Systems Consortium (ISC), 327
- internetworking, 174, 187
- intrusion detection, 462
- invoke-rc.d command, 435
- IP addresses, 118, 187–188, 327
- IP packet, 417
- IP spoofing, 415
- IPP (Internet Printing Protocol), 326
- iproute2 utilities, 214–216
- IPSec (IP Security Protocol), 415

`iptables` command, 444–447
ISBN (International Standard Book Number), 482–485
ISC (Internet Systems Consortium), 327
ISO image, 67
`isolate` command, 263
ISOLINUX, 54

J

JavaScript Object Notation (JSON), 322

jobs

- cron, 281–283
- one-time, 278–280
- recurring, 281–283
- scheduling, 278–283

`jobs` command, 476

`join` command, 520

`journalct` command, 67–68

`journal` program, 67, 328

JSON (JavaScript Object Notation), 322

K

Kate text editor, 160–161

KDE (K Desktop Environment)
Plasma desktop

- Application Launcher, 95
- desktop, 96–98
- desktop settings, 100–101
- Dolphin file manager, 149–151
- general discussion, 13–14, 93–94
- Kate text editor, 160–161
- KFind utility, 152–153
- KMail, 121–123
- Konsole, 226–227
- KWrite text editor, 159–160
- logging out from, 61
- multimedia settings, 126–127
- panel, 96

system settings, 99–100

terminal window, 57

widgets, 98–99

KDE Dragon, 130

kernel modules, 11

kernel ring buffer, 65–66

key pairs, generating, 429–430

KFind utility, KDE Plasma,
152–153

kickstart file, 72

`kill` command, 238, 242, 476, 504

KMail, 121–123

KNOPPIX

- boot commands, 68–70
- partitioning tool, 26–27
- text mode installation, 64

Konsole, opening, 226–227

korn shell, 16

`ks` boot option, 72

`ks=kickstartfile` boot option, 72

`ksyms` command, 277

KVM, 40

KWrite text editor, 159–160

L

`l2tp` command, 214

LANs (local area networks)

- connecting to Internet,
196–198
- setting up with cable, 197–198
- setting up with DSL, 197–198
- sharing files in, 325
- wired (Ethernet)
 - cables, 192–193
 - overview of function,
191–192
 - setting up, 190–195
 - switch, 192–193
 - TCP/IP, 185–190, 185–198
- wireless network
 - ad hoc mode, 201
 - configuring, 205–206

configuring access points,
204–205

connection diagram and
notes, 203–204

infrastructure mode, 201

security specifications,
201–202

setting up hardware,
203–204

standards for, 199–201

LDAP (Lightweight Directory
Access Protocol), port
number, 318

`ldd` command, 238

`LDFLAGS` variable, 499

`less` command, 237

less-than sign (<), 232

`let arg` command, 476

LGPL (Library General Public
License), 511

`/lib` directory, 300

`libcrc32c` module, 277

Library General Public License
(LGPL), 511

LibreOffice, 115–116, 518

`lighttpd` package, 319–320

`link` command, 214

Linux

general discussion, 7–8

installing

- approaches for, 21–22
- creating boot disk, 28–30
- disabling secure boot
feature, 27–28
- first boot after, 36–37
- keyboard, selecting, 32
- language, selecting, 31
- minimal installation, 32
- normal installation, 32
- options in, 33–34
- by partitioning an existing
drive, 24–26, 34–35
- by replacing an existing
operating system, 21–22

- reporting installation experience, 36
- on a second hard drive, 22, 24
- software to install, selecting, 32
- steps in, 30–35
- troubleshooting, 65–71
- as a virtual Linux machine, 23
- on virtual machine, 45–52
- securing
 - encryption and digital signature, 427–433
 - file and directories, 422–425
 - Internet services, 434–436
 - key security files, 448
 - passwords, 420–423
 - system security, 433–434
- shutting down, 60–61
- starting, 53–55
- user interfaces, 12–13
- Linux Assigned Names And Numbers Authority (LANANA), 274
- Linux certification
 - CompTIA Linux+ exams
 - overview, 530
 - Scripting, Containers, and Automation domain, 533
 - Security domain, 532
 - System Management domain, 531–532
 - Troubleshooting domain, 533–534
- Linux Essentials Certificate of Achievement
 - domains, 516
 - “Finding Your Way on a Linux System” topic, 518–519
- Linux Community and a Career in Open Source” topic, 516–517
- “Linux Community and a Career in Open Source” topic, 521–522
- “Power of the Command Line” topic, 520–521
- “Security and File Permissions” topic, 522–524
- Linux Foundation, 535–536
- Linux kernel
 - boot options, 71–74
 - defined, 8, 54
 - functions of
 - described, 9
 - hardware management, 11
 - software program management, 10–11
 - system memory management, 9–10
 - modules, 11
 - version numbers, 59
 - vulnerabilities, 454
- Linux Mint, Cinnamon desktop, 104
- Linux Professional Institute (LPI), 511
- Linux Professionals
 - LPIC-1 level of certification exams, 524–527
 - LPIC-2 level of certification exams, 527–528
 - LPIC-3 level of certification exams, 528
- “Power of the Command Line” topic, 520–521
- “Security and File Permissions” topic, 522–524
- Linux Professionals
 - LPIC-1 level of certification exams, 524–527
 - LPIC-2 level of certification exams, 527–528
 - LPIC-3 level of certification exams, 528
- overview, 515–516
- vendor-neutral certifications
 - GIAC Certifications, 536–537
 - Linux Foundation, 535–536
- vendor-specific certifications, 537
- Linux commands
 - for archiving and compressing files, 238
 - defined, 235
 - for displaying dates and times, 239
 - for finding files, 236–237
 - for finding help and abbreviations, 236
 - for managing files, 238
 - for managing files and directories, 236
 - for managing the file system, 239
 - for managing users, 239
 - for processing files, 237–238
- Linux distributions
 - categories, 17
 - core, 17–18
 - Debian, 17
 - defined, 16
 - Fedora, 18
 - Gentoo, 17
 - LiveDVD, 19
 - Mint, 18
 - MX Linux, 18
 - openSuse, 17
- Puppy Linux, 18
- Slackware, 17
- specialized, 18–19
- text mode installation, 64
- Ubuntu, 18

- Linux server
 - general discussion, 313–314
 - launching services, 314–316
 - listening for clients, 316–318
 - running background processes, 314–315
 - super-server program, 316
- Linux Standard Base, 301
- Linux system memory map, 10
- `list` command, 504, 507
- `Listen` directive, 338
- `list-units` command, 263
- LiveDVD, 19, 23, 31
- LivePatch feature (Ubuntu), 36
- `ln` command, 236
- `lo` network interface, 215
- load averages, 265
- load balancing, 332
- loadable kernel modules, 276
- `LoadModule` directive, 338
- local area networks. *See* LANs (local area networks)
- `local` command, 476
- local loop, 175
- `locate` command, 236
- location services, selecting, 36
- log analysis and monitoring tools, 462
- log files, 66–67, 327–328
- `LogFormat` directive, 338
- `logger` command, 522
- logging in, 56
- logging out, 60–61
- logging server, 327–328
- logic bomb, 415
- logical partitions, 25
- login ID, creating, 35
- login roles, 361
- login window, 55
- `LOGNAME` environmental variable, 294
- `logout` command, 476
- `logrotate` command, 522

- `lowres` boot option, 72
- `lpr` command, 237
- `ls` command, 137, 229, 236, 519
- `ls -l` command, 137–138
- `lsmmod` command, 277
- `lsot` utility, 417

M

- Machine menu (VirtualBox), 50
- macro expansion, 387
- macro processor, 387
- macros, 387, 497–499
- `maddress` command, 214
- `mail` command, 399–400
- mail delivery agent (MDA), 324
- `MAIL` environmental variable, 294
- mail servers
 - mail-delivery test, 398–400
 - Postfix, 396–398
 - sendmail
 - alias file, 395–396
 - configuration file, 386
 - files, 393–395
 - `.forward` file, 395
 - general discussion, 385–386
 - `m4` macro processor, 386–388
 - macro file, 388–391
 - `sendmail.cf` file, 391–393
- mail services
 - general discussion, 323
 - mail delivery agent, 324
 - mail transfer agent, 322–324
 - mail user agent (MUA), 322
- mail transfer agent (MTA), 322–324
- mail transport agent (MTA), 385
- mail user agent (MUA), 322
- `MAILER` macro file, 391
- `MAILTO` environment variable, 283

- `mailutil` package, 398–399
- major device numbers, 274
- `make` command, 497, 500–501, 505
- `makefile`, 495–497, 499–500
- Makefile, 495
- `man` command, 236, 519
- managed mode, 201
- MariaDB server
 - command prompt, 353–356
 - creating database projects, 360–363
 - creating user accounts, 362–363
 - history, 350
 - installing, 350–353
 - `mysql` command-line parameters, 354–355
 - `mysql` commands, 356–360
 - overview, 321
 - using, 349–363
- `mariadb` daemon program, 315
- `MASQUERADE_AS` macro file, 391
- `MASQUERADE_DOMAIN` macro file, 391
- MATE desktop
 - applets, 110
 - Control Center, 109–110
 - GNOME 2 desktop layout in, 107
 - history of, 107–109
 - icons, 109
 - menu, 108–109
 - workspace switcher, 109
- `MaxClients` directive, 338
- `MaxSpareServers` directive, 338
- MD5 (Message Digest algorithm 5), 67, 414, 421
- `/media` directory, 136, 300
- `mediacheck` boot option, 72
- `mem=xxxM` boot option, 72
- minimal installation, 32
- minor device numbers, 274

MinSpareServers directive, 338
Mint, 18
mitigation approach, 409–410
mkdir command, 140, 236
MMDDhhmmYYYY date and time, 242–243
/mnt directory, 300
modinfo command, 277
modprobe command, 277
MongoDB server, 321–322
monitor command, 214
monolithic program, 276
more command, 59, 237, 243–244
mount command, 302
Mount Optical Drives function (VirtualBox), 51
mount point, 302, 307
mounting, 136
 DOS disk partition, 308–309
 /etc/fstab file, 303–304
 mount command, 302
 mount point, 302, 307
 NFS, 307–308
 NFS (Network File System), 378
 NTFS partition, 309–310
 overview, 299
 unmount command, 303
 USB sticks, 302
 Windows disk partition, 308–309
mouse, settings for, 92
MOV files, 129
movies
 formats, 129
 players, 129
Mozilla, 117
Mozilla Firefox browser, 518
MP3 files, 127
MPG files, 129
mroute command, 214
mrule command, 214
mtr program, 217–218

mv command, 140, 230, 236, 519
MX Linux, 18, 111–114
MySQL server, 321, 350

N

name servers, 328
named server daemon, 328
nano editor, 156–157
NAT router, 197
Nautilus, 145
neighbor command, 214
NetBIOS, 190
netfilter, 443
netns command, 214
Netplan tool, 209
netstat utility, 218–221, 417, 521
net-tools package, 218
network adapters, 52
network address translation (NAT)
 defined, 442–443
 hiding, 442
 implementation, 442–443
 overview, 442
 port address translation, 443
 router, 197, 203–204
 static, 442
network configuration files, 208–210
Network Information Service (NIS), 454
Network layer (TCP/IP), 187
network management, 328–329
Network News Transfer Protocol (NNTP), 190
network resource servers, 326
network security
 inetd server, 458–459
 overview, 458
 penetration test, 460
 stand-alone services, 459
 xinetd server, 458–459

Network Time Protocol (NTP), 329
network utilities, 462
networking and Internet connections
 connection options
 cable model, 175
 cable modem, 180–184
 dial-up, 174, 176
 Digital Subscriber Line (DSL), 175, 176–180
 fiber-optic Internet, 175
 satellite, 175–176
 wireless hot spot, 175
 general discussion, troubleshooting TCP/IP networks, 173
Internet overview, 174
local area networks
 wired (Ethernet), 185–198
 wireless network, 199–206
monitoring status of, 251
network management
 configuring network features, 207–216
 editing network configuration files, 208–216
 troubleshooting TCP/IP networks, 216–221
NetworkManager tool
 editing network connection settings, 210–212
 network settings, 209
 nmcli command-line tool, 212–214
 nmtui command-line tool, 212–213
 overview, 205–206
next command, 505
NFS (Network File System)
 database services
 MariaDB server, 321
 MongoDB server, 321–322
 MySQL server, 321
 PostgreSQL server, 320

NFS (*continued*)
defined, 190
exporting file system with, 306–307, 375–376
file sharing with, 304–305, 325
installing, 305–306, 374–375
mounting, 307–308, 378
port number, 318
sharing files with, 373–378
vulnerabilities, 454
nfs-kernel-server package, 305–306
nfs-utils package, 306
NGINX server
configuring, 346–347
default web page, 345
installing, 344–345
overview, 316, 333
nice command, 238
NIS (Network Information Service), 454
nl command, 237
nmap tool, 417, 461–463
nmbd NetBIOS name server, 379
nmblookup command, 379
nmcli command-line tool, 212–214
nmi_watchdog=1 boot option, 72
nmtui command-line tool, 212–213
noapic boot option, 72
nofirewire boot option, 72
noht boot option, 73
nomce boot option, 73
nomount boot option, 73
Non-Maskable Interrupt (NMI), 72
nonrepudiation, 415
nonzero exit status, 472
nopager command, 357
nopass boot option, 73
nopecmca boot option, 73

noprobe boot option, 73
normal installation, 32
noshell boot option, 73
NoSQL, 321
nousb boot option, 73
nousbstorage boot option, 73
nowarning command, 357
ntable command, 214
NTFS (NT File System) partition, mounting, 309–310
NTP (Network Time Protocol), 329
nv module, 68

O

object code, 488
Objective C, 490
one-time jobs, 278–280
Open Secure Sockets Layer (OpenSSL), 454
Open Source Initiative (OSI), 518
OpenOffice.org, 518
open-source software (OSS), 12
OpenSSH (Open Secure Shell), 437–439
openSUSE. *See also* Linux distributions
adding applications in, 81
adding packages in, 82–83
described, 17
network configuration files, 208
Systemd method in, 259
updating, 78–79
Yet another Setup Tool version 2, 82–83
operating system updates, 77–79, 455
/opt directory, 300
Oracle Certified Associate (OCA) certification, 537
Oracle Certified Professional (OCP) certification, 537
OSTYPE macro file, 391
others, 142
owners, 142, 143

P

pack command, 521
package managers, 81–83
packet, 415
packet filter firewall, 440–441
packet filtering
defined, 415
enabling, 443–447
iptables command, 444–447
security level configuration tool, 443–444
packet sniffer, 417, 461–462
pages, 9
panel, KDE Plasma, 96
Parallels, 40
partitioning
during Linux installation, 34–35
using Linux tools, 26–27
using Windows tools, 25–26
partitions
defined, 25
shrinking, 22
types of, 25
passwd command, 290, 523
passwd utility, 417
password-checking tools, 462
passwords
permissions, 457
pluggable authentication modules, 421–422
root, 55
searching for name, 229
securing, 420–423
shadow, 420–421
paste command, 237, 520
patch command, 237
PATH environmental variable, 293–294, 294

- pathname, 299
- Pause function (VirtualBox), 50
- pci=biosirq boot option, 73
- pci=noacpi boot option, 73
- peer-to-peer network, 325
- PEM (Privacy Enhanced Mail), 394
- penetration testing, 460
- perimeter network, 415
- period (.), 518
- permissions
 - changing, 423–424
 - codes, 424
 - defined, 138, 141
 - execute permission, 143
 - groups, 143–144
 - owners, 143
 - read permission, 143
 - set user ID, 426
 - setting default, 424–425
 - triplets, 141–143
 - write permission, 143
 - viewing and changing, 148–149
- Physical layer (TCP/IP), 187
- ping command, 216–217
- ping utility, 521
- ping6 command, 216–217
- pipe (|), 231, 244
- pluggable authentication
 - modules (PAMs), 421–422
- plus sign (+), 474
- Point-to-Point Protocol (PPP)
 - connections, 275
- POP email servers, 118
- popd command, 476
- port numbers, 186, 189–190, 317–318, 460
- port scanners, 461–462
- port scanning, 415, 460
- Post Office Protocol (POP), 186, 189, 318
- Postfix, 524
 - /etc/postfix/main.cf configuration file, 398
- installing
 - on Rocky Linux, 397
 - on Ubuntu, 396–397
- mail-delivery test, 398–399
- PostgreSQL server
 - command interface, 366–369
 - connecting to server, 367–368
 - creating database, 370–371
 - creating database objects, 370–372
 - creating user accounts, 371–372
 - installing, 364–366
 - overview, 320
 - psql commands, 368–369
 - using, 363–372
- pound sign (#), 283, 337, 382
- prevention, 452, 455, 458
- primary partitions, 25
- print command, 357
- print EXPR command, 505
- print servers, 326
- printenv command, 238, 292
- printers, setting up, 74–76
- printing system, managing, 250
- Privacy Enhanced Mail (PEM), 394
- /proc file system
 - /acpi file, 272
 - /bus file, 272
 - /cmdline file, 272
 - /cpuinfo file, 271, 272
 - defined, 270
 - /devices file, 272
 - /dma file, 272
 - /driver/rtc file, 272
 - /filesystems file, 272
 - /ide file, 272
 - /interrupts file, 272
 - /ioports file, 272
 - /kcore file, 270, 272
 - /kmsg file, 272
 - /loadavg file, 272
 - /locks file, 272
 - /meminfo file, 272
 - /misc file, 272
 - /modules file, 273
 - /mounts file, 273
 - /net file, 273
 - /partitions file, 273
 - /pci file, 273
 - /scsi file, 273
 - /stat file, 273
 - /swaps file, 273
 - /sys file, 273
 - /uptime file, 273
 - /version file, 273
- process field, 256
- process file system. *See* /proc file system
- process ID (PID), 241–242
- programming
 - bash built-in commands, 475–478
 - basics of, 469–478
 - calling shell functions, 471
 - controlling flow of execution, 471–474
 - defining variables, 470–471
 - edit-compile-debug cycle, 488
- GNU licenses
 - General Public License, 510
 - Library General Public License, 511
- overview, 467–469, 488–489
- sed stream editor
 - awk language and, 482–486
 - overview, 479–481
- simple shell scripts, 468–469
- software-development tools
 - GNU C and C++ compilers, 490–493
 - GNU debugger, 502–509
 - GNU make utility, 493–501
 - overview, 489–490
 - steps in, 488

programs, list of running, 59–60
prompt command, 357
protocols, 186
proxy servers, 415
ps ax command, 241, 244
ps command, 59–60, 238
pstree command, 238
public key cryptography, 415
public key infrastructure (PKI), 415
pump package, 327
Puppy Linux, 18
pushd command, 476
pwd command, 236, 476

Q

QT files, 129
question mark (?), 233–235, 356
quit command, 357, 505

R

RADIUS (Remote Authentication Dial-In User Service), 202
rate adaptive DSL, 178. *See also* DSL (Digital Subscriber Line)
read command, 470, 477
read permission, 143
readonly command, 477
Ready to Go window (Ubuntu), 36
reboot command, 238
reboot=b boot option, 73
rebooting, 60–61, 71
Recording function (VirtualBox), 51
recurring jobs, 281–283
Red Hat
 certifications, 537
 network configuration files, 208, 209
 Systemd method in, 259
Red Hat Security Center, 418
regular expressions, 518
rehash command, 357
relative navigation, 140
relative path, 518
reload command, 263
remote access, 174
remote logins, 437–439
removable media, 136
Rendezvous Directory Service, 190
Request for Comments (RFC) documents, 317
Requires line, 262
rescue boot option, 73
Reset function (VirtualBox), 50
resolution=*HHHxVVV* boot option, 73
response, 452, 458
response metrics, 455
responsibilities, 409
restart command, 263, 336
Restart line, 261
return command, 477
reverse proxy, 332
Revision Control System (RCS), 490
risk analysis
 defined, 406
 mitigation approach, 409–410
 performing, 406–408
 probability and effect, 408
 security policy, 408–409
 threats, 407
 vulnerabilities, 407
rm command, 140–141, 230, 236, 519
RM files, 129
RM variable, 499
rmdir command, 140, 236
rmmod command, 277
Rocky Linux
 dnf tool, 381, 397
 firewall, 306

installing Postfix, 396
installing postgresql-server package, 364
installing Samba in, 381
libcrc32c and xfx modules, 277
nfs-utils package, 306
System Monitor utility, 284–286
systemd program, 253
/root directory, 300
root user and account (superuser), 55, 60, 240–241, 251–252, 302
route command, 214
route utility, 521
routers, 197, 203–204
routines, 488
rsyslogd configuration file, 434
rsyslogd service, 328
Rufus, 29–30
rule command, 214
run command, 505
run levels, 253–254
runlevels field, 256
run-parts shell script, 283

S

Samba
 components of, 379–380
 configuring, 382–383
 defined, 325–326
 installing, 380–381
 resources, 384
 setting up Windows server using, 378–379
 systemctl command, 435
sandbox, 40
 naming, 42
 working with, 49–52
SANS Institute, 453
/sbin directory
 defined, 300

- /hdparm program, 267–268
- /hotplug program, 275
- /udev program, 276
- Scaled Mode function (VirtualBox), 51
- scheduling jobs
 - one-time jobs, 278–280
 - recurring jobs, 281–283
 - tasks, 278
- screening router, 415
- scripting
 - bash built-in commands, 475–478
 - basics of, 469–478
 - calling shell functions, 471
 - controlling flow of execution, 471–474
 - defining variables, 470–471
 - edit-compile-debug cycle, 488
 - GNU licenses
 - General Public License, 510
 - Library General Public License, 511
 - overview, 467–469, 488–489
 - sed stream editor
 - awk language and, 482–486
 - overview, 479–481
 - simple shell scripts, 468–469
 - software-development tools
 - GNU C and C++ compilers, 490–493
 - GNU debugger, 502–509
 - GNU make utility, 493–501
 - overview, 489–490
 - steps in, 488
- SCSI card, 68
- Seamless Mode function (VirtualBox), 51
- Secure Shell (SSH), 190, 317
- security
 - business requirements, 406
 - establishing security framework, 404–406
 - business requirements, 406
 - risk analysis, 406–408
 - host security
 - defined, 410
 - overview, 411
 - importance of, 404
 - managing, 410
 - mitigation approach, 409–410
 - monitoring, 251
 - network security
 - defined, 410, 411
 - overview, 412–413
 - news and updates, 417
 - overview, 403
 - setting up, 251
 - terminology, 413–416
 - tools, 417
- security audits, 409
- Security Enhanced Linux (SELinux) mandatory access control, 72
- security policy, 404–405, 408–409
- sed command, 237
- sed stream editor
 - awk language and, 482–486
 - overview, 479–481
- segment violation, 71
- selinux=0 boot option, 73
- semicolon (;), 230, 382
- sendmail
 - alias file, 395–396
 - configuration file, 386
 - files, 393–395
 - .forward file, 395
 - general discussion, 385–386
 - m4 macro processor, 386–388
 - macro file, 388–391
 - MTA package, 323
 - sendmail.cf file, 391–393
 - vulnerabilities, 454
- sendmail.cf file, 391–393
- serial boot option, 73
- ServerAdmin directive, 338
- ServerName directive, 338
- ServerRoot directive, 338
- servers
 - automatically starting at system startup, 258–259
 - hardening, 412
 - manually starting and stopping, 257–258
- service program, 315
- services, 314
- Session Information function (VirtualBox), 50
- set command, 477
- set user ID, 426
- set variable VAR=VALUE command, 505
- setuid program, 416
- SHA-1 (Secure Hash Algorithm-1), 414
- shadow passwords, 420–421
- Shared Clipboard, function (VirtualBox), 52
- Shared Folders function (VirtualBox), 52
- shell
 - about, 15, 56, 225
 - call shell functions, 471
 - defined, 56, 228, 517
- shell CMD command, 505
- shell commands, 58
- SHELL environmental variable, 294
- shell scripts, 15, 57, 155
 - writing, 246–247
- shelving inventory system, 56
- shift command, 477
- shutdown command, 238
- shutting down, 60–61
- signal 11 error, 71
- SIGSEGV (Segment Violation Signal), 71

- Simple Mail Transfer Protocol (SMTP), 186, 189, 317, 400
- Simple Network Management Protocol (SNMP), 190, 454
- Simultaneous Authentication of Equals (SAE), 202
- skipddc boot option, 73
- SMB (Server Message Block), port number, 318
- smbadduser program, 379
- smbcacs program, 379
- smbclient Windows client, 379
- smbcontrol program, 379
- smbd SMB server, 379
- smbmount program, 379
- smbpasswd program, 379, 382
- smbprint script, 379
- smbstatus command, 379
- smbtar program, 379
- smbumount program, 38
- SMTP (Simple Mail Transfer Protocol), 186, 189, 317, 400
- snapshot, VirtualBox, 50
- sniffer, 416, 461–462
- SNMP (Simple Network Management Protocol), 328–329
- soft limits, 289
- soft mount, 378
- software, installing, 79–83
- software-development tools
 - GNU C and C++ compilers, 490–493
 - GNU debugger, 502–509
 - GNU make utility, 493–501
 - overview, 489–490
- sort command, 237, 245
- source code, 488
- source command, 357
- source file, 488
- specialized Linux distributions, 18–19
- spices, 106–107
- split command, 237, 245
- spoofing, 440
- spyware, 416
- SQL (Structured Query Language), 320
- /srv directory, 300
- stand-alone servers, 434–435, 459
- standard error, 231, 520
- standard input, 231, 520
- standard output, 231, 520
- start command, 263, 336
- starting Linux, 53–55
- StartServers directive, 338
- startup scripts, 256–257
- state table, 441
- stateful inspection firewall, 441
- statements, 488
- status bar command, 263
- status command, 335, 336, 357
- step command, 505
- stop command, 263, 336
- stream editor, 480
- stream-based macro processor, 387
- streaming
 - audio, 128
 - defined, 174
- Structured Query Language (SQL), 320
- su command, 240, 417, 524
- subroutines, 488
- Subversion, 490
- sudo command, 55, 240, 252, 417, 524
- super-server program, 316
- superuser, 55, 143
- SUSE. *See also* Linux distributions
 - certifications, 537
 - configuring Samba, 382
 - enabling packet filtering, 443
 - run levels, 254
 - text mode installation, 64
 - turning on/off stand-alone servers, 435
- xinetd server, 435–436
- YaST Control Center, 284
- swap space, 9
- swapping out, 10, 267
- symmetric DSL, 178. *See also* DSL (Digital Subscriber Line)
- symmetric key encryption, 416
- Synaptic Package Manager (Ubuntu), 81–82
- sysfs file system, 275
- syslogd configuration file, 434
- system administration
 - administrators, 249
 - backups, 250
 - boot process
 - /etc/inittab file, 254–255
 - automatically starting servers at system startup, 258–259
 - init program, 255–256
 - manually starting and stopping servers, 257–258
 - run levels, 253–254
 - setting default target, 262
 - startup scripts, 256–257
 - systemctl program, 262–264
 - units and targets, 259–260
 - booting process
 - Systemd method, 259–264
 - SysVinit method, 253–259
 - defined, 249
 - device files
 - block devices, 274
 - character devices, 275
 - network devices, 275
 - overview, 274
 - udev program, 275
 - driver modules
 - /etc/modprobe.d files, 277–278
 - loading and unloading, 276–277
 - overview, 276–278
 - GUI tools, 284–286
 - hardware management, 250

- network status
 - monitoring, 251
- printing system
 - management, 250
- scheduling jobs
 - one-time jobs, 278–280
 - recurring jobs, 281–283
 - tasks, 278
- security monitoring, 251
- software installation, 250
- system performance
 - monitoring, 250
 - disk performance and usage, 267–270
 - top utility, 264–266
 - uptime command, 266
 - viewing system information, 270–273
 - vmstat utility, 264–266
- task automation, 250
- tasks, 250–252
- user account
 - management, 250
- system command, 357
- system information, viewing, 270–273
- system memory
 - management, 9–10
- System Monitor utility, 284–286
- system performance
 - monitoring, 250
- system security, monitoring, 433–434
- system startup and
 - shutdown, 250
- systemctl command, 306, 352, 365, 435
- systemctl program, 262–264, 315
- Systemd method
 - general discussion, 253
 - overview, 11
 - setting default target, 262
 - systemctl program, 262–264
 - units and targets, 259–260

- Systemd startup method, 67
- systemd timer unit files, 283
- SysVinit initialization method
 - /etc/inittab file, 254–255
 - automatically starting servers
 - at system startup, 258–259
 - defined, 10–11
 - general discussion, 252
 - init program, 255–256
 - manually starting and stopping servers, 257–258
 - run levels, 253–254
 - service program, 315
 - startup scripts, 256–257
 - systemctl program, 315

T

- tac command, 237
- tail command, 237
- tar command, 238, 521
- targets, 259–260
- TCP wrapper, 436
- TCP/IP (Transmission Control Protocol/Internet Protocol)
 - configuring, 195–196
 - four-layer model of, 185–187
 - general discussion, 185
 - Internet services, 189–190
 - IP addresses, 187–188
 - port numbers, 189–190
 - troubleshooting networks
 - advanced, 218–221
 - basic, 216–217
- TCP/IP packet, 417
- tcpmetrics command, 214
- tcsh shell, 16
- tee command, 357
- Telnet, 190, 317
- Temporal Key Integrity Protocol (TKIP), 202
- TERM environmental variable, 294
- Terminal program, 137, 226–227
- terminal window, 57, 225–227
- test command, 472, 521
- testparm program, 38
- text editors
 - defined, 152
 - ed text editor, 161–164
 - gedit text editor, 157–158
 - Kate editor, 160–161
 - KWrite editor, 159–160
 - nano editor, 156–157
 - overview, 489
 - using, 488
- text files
 - counting words and lines in, 244
 - editing, 156–169
 - sorting, 245
 - viewing text, 155–156
- text mode installation, 64
- threats
 - defined, 406, 416
 - disclosure of information to the public, 407
 - DOS attack, ' 407
 - unauthorized access, 407
- Thunderbird, 123–124, 518
- times command, 477
- /tmp directory, 300
- Token command, 214
- top command, 238
- top utility, 264–266
- Torvalds, Linus, 1
- touch command, 236
- touchpad, settings for, 92
- tr command, 237, 245
- traceroute command, 217
- Transmission Control Protocol (TCP), 186, 317
- Transport layer (TCP/IP), 186
- trap command, 477
- triplets, 141–143
- Tripwire, 433–434, 455

Trivial File Transfer Protocol (TFTP), 190

Trojan horse, 416

troubleshooting

audio, 124

TCP/IP networks, 216–221

troubleshooting installations

fatal signal 11 error, 68–70

PC reboot problem, 71

using kernel ring buffer, 65–66

using KNOPPIX boot commands, 68–70

using log files, 66–67

using the journal, 67–68

Tunnel command, 214

Tuntap command, 214

type command, 236, 477

U

Ubuntu

adding applications in, 80

adding packages in, 81–82

apt tool, 380

boot screen, 54

configuring Internet super server, 435

defined, 18

first boot, 36–37

inetd server, 435

installing, 30–35

installing Postfix, 396–397

installing Samba, 380

LiveDVD image, 30–31

LivePatch feature, 36

login window, 55

Synaptic Package Manager, 81–82

terminal window, 57

turning off stand-alone servers, 435

update-rc.d command, 435

updating, 77–78

/var/log/syslog file, 67

ufw (Uncomplicated Firewall), 306, 443–444

ulimit command, 417, 477

umask command, 424–425, 477

unalias command, 236, 477

uname command, 58, 238

unauthorized access, 407

uncompress command, 238

underscore (_), 134

Unified Extensible Firmware Interface (UEFI) boot method, 27–28

uniq command, 237

units

configuring, 261–262

Systemd, 259–260

Unix System V operating system, 252

unmount command, 303

unset command, 477

update-rc.d command, 258, 435

updating, operating system, 455

upstream data, 181

uptime command, 266

U.S. Computer Emergency Readiness Team (US-CERT), 418

USB drives

bootable, creating, 29–30

booting from, 31

US-CERT National Cyber Alert System, 418

uscertkey.asc file, 429

use command, 357

user account management

adding user accounts, 250, 288–291

logging in as root user, 251–252

removing user accounts, 250

su - command, 251–252

using commands, 288–290

using GUI tools, 288–290

User and Group Management tool, 289

User Datagram Protocol (UDP), 186, 317

User directive, 338

user file-creation mask, 424

user interfaces

command-line interface (CLI), 15–16

GNOME desktop, 14–15

KDE Plasma desktop, 13–14

overview, 12–13

X Window system, 13

user web hosting, 341

useradd command, 290

userdel command, 291

usermod command, 291–292, 417

users

changing file ownership, 295
environmental variables, 293–294

managing user accounts

adding user accounts, 250, 288–291

logging in as root user, 251–252

removing user accounts, 250

su - command, 251–252

using commands, 288–290

using GUI tools, 288–290

Using Samba (Carter et al), 384

/usr directory

/bin, 300

/bin/scp component, 437

/bin/slogin component, 437

/bin/ssh component, 437

/bin/ssh-keygen component, 437

/games, 300

/include, 300

/lib, 300

/libexec, 300

- /local, 300
- /sbin, 300
- /sbin/cron, 261
- /sbin/sshd component, 437
- /share, 300
- /share/ sendmail-cf directory, 389–390
- /src, 300

V

/var directory

- /cache, 301
- /crash, 301
- /lib, 301
- /lock, 301
- /log, 66, 301, 327, 457
- /log/lastlog, 457
- /log/messages, 67, 457
- /log/wtmp, 457
- /mail, 301
- /opt, 301
- /run, 301
- /spool, 301
- /syslog, 66–67
- /tmp, 301
- /yp, 301

variables, 488, 497–499

vendor-neutral certifications

- GIAC Certifications, 536–537
- Linux Foundation, 535–536

version control system, 490

VERSIONID macro file, 390

very-high bit-rate DSL (VDSL/
VHDSL), 178

vi text editor

- colon command mode, 166
- command mode, 166
- commands, 167–169
- defined, 161
- deleting text, 167
- navigating within, 166–167
- saving changes, 167

- starting, 165
- text-input mode, 166
- video cards, 13, 68
- View menu (VirtualBox), 50–51
- virtual consoles, opening, 225–227
- virtual hard disks, creating, 43
- virtual hosting, 332
- virtual machines (VMs)
 - audio, 46, 52
 - CPU and memory allocation, 46
 - creating, 42–44
 - defined, 23, 40
 - installing Linux on, 45–52
 - network, 47
 - network adapters, 52
 - serial ports, 47
 - shared folders, 47, 52
 - storage, 46
 - USB device access, 47, 52
 - user interface, 47
 - video memory and virtual display allocation for, 46
- virtual memory, 9
- virtual screens, 51
- virtual servers
 - amount of memory for, selecting, 43
 - creating, 42–44
 - hard disk emulation, selecting, 43
 - installing Linux with, 23
 - selecting operating system to install, 42–43
 - software packages, 23, 40
 - storage file creation, selecting method for, 44
 - storage type, selecting, 44
- virtual web hosting, 341–343
- VirtualBox
 - creating virtual machine, 42–44
- Devices menu, 51–52

- downloading, 41
- Input menu, 51
- installing, 40–42
- installing Linux on virtual machine
 - loading the operating system, 47–49
 - settings, changing, 45–46
- Machine menu, 50
- main window, 42
- overview, 23, 40
- Settings dialog box, 45–47
- View menu, 50–51
- VirtualBox Disk Image (VDI), 44
- <VirtualHost> directive, 342, 344
- virus, 416
- VLC player, 130
- vmstat utility, 264–266
- VMware, 23, 40
- vnc boot option, 73
- vsftpd SFTP server, 434
- vulnerabilities
 - common, 407, 453–454
 - defined, 416
 - online resources, 453
 - testing types, 460–461
- vulnerability scanners, 460, 461–462

W

- wait command, 477
- WantedBy line, 261
- Wants line, 262
- war-dialing, 416
- war-driving, 416
- warnings command, 357
- watch VAR command, 505
- Wayland, 13
- wc command, 238, 244, 520
- Web, 174
- web browsers, 518
- web caching, 332

- web proxy, 332
- web servers
 - Apache, 331–332
 - NGINX, 333, 344–347
- Web services
 - Apache server, 319
 - defined, 316
 - lighttpd package, 319–320
 - NGINX server, 316
- whatis command, 236, 519
- where command, 505, 507
- whereis command, 237
- which command, 237
- Whisker menu, Xfce desktop, 112–113
- white hat, 460
- white-box testing, 460–461
- widgets, KDE Plasma, 98–99
- Wi-Fi (Wireless Fidelity), 199
- Wi-Fi Alliance, 202
- Wi-Fi Protected Access (WPA), 202
- wildcards, 233–235
- WIMP (windows, icons, mouse, and pointer), 56
- winbindd server, 38
- Windows Disc Image Burner, 28–29
- Windows Disk Management tool, 25–26

- Windows disk partition, mounting, 308–309
- Windows operating system, installing as a virtual machine, 23
- Windows overview area, GNOME, 91
- Wired Equivalent Privacy (WEP), 202
- wireless access point (WAP), 204–205
- WLANS (wireless local area networks)
 - ad hoc mode, 201
 - configuring, 205–206
 - configuring access points, 204–205
 - connection diagram and notes, 203–204
 - infrastructure mode, 201
 - security specifications, 201–202
 - setting up hardware, 203–204
 - standards for, 199–201
- WMV files, 129
- word processor, 488
- workspace selector, GNOME, 91
- workspace switcher, MATE, 109
- worms, 416
- write permission, 143

X

- X Window system
 - defined, 13
 - Wayland, 13
 - X.org, 13
- x/F ADDR command, 505
- Xfce desktop
 - applets, 113–114
 - general discussion, 111
 - history of, 111–112
 - settings manager, 113
 - Thunar file manager, 151–152
 - Whisker menu, 112–113
- xfrm command, 214
- xfs module, 277
- xinetd server, 316, 434–436, 458–459
- X.org, 13

Y

- YaST Control Center, 284, 386
- Yet another Setup Tool (YaST), 82–83

Z

- zcat command, 238
- zless command, 238
- zmore command, 238
- zsh shell, 16