

Hacking Knoppix

COPYRIGHTED MATERIAL

Index

SYMBOLS & NUMERICS

\$ `ifconfig` command, 51
802.11b card, 48, 178

A

accessing Internet
 broadband connection, 47–48
 modem, connecting via, 45–47
 static address, setting, 51–52
 wirelessly, 48–51
Acrobat Reader (Adobe)
 printer, setting up, 13
 viewing PDFs with, 41–43
Adblock extension, 56
Add Acc window (KMail), 61
Add Account window (Gaim), 65
Add Transport window (KMail), 60
Add → AddPrinter/Class, 12
address book, auto-populating, 62–64
Ad-Hoc mode for card, 49
Adobe Acrobat Reader
 printer, setting up, 13
 viewing PDFs with, 41–43
Advanced options (Remote Desktop Connection), 69
All tab (KPackage), 4
AllMusic Website, 57
Alt+SysRq+B (reboot), 266
analyzing network traffic, 141–147
Apache Web server, 87–88
application fonts, changing, 8–11
application level rootkit, 128
APT information Website, 5
`apt-get` utility, 205, 216–217
Archix distro
 background, changing, 238–239
 boot screen, changing, 239, 241
 customizing look of, 238–241
 environment, preparing, 229
 installing software for, 235–238
 mastering CD, 241
 preparation for creating, 228
 reasons for creating, 227

 removing unneeded software, 230–235
 testing, 242
arrow keys, 36
ASCII file, 124
ASCII text output, generating, 125
Asterisk Logger (Helix), 194–196
Astronomy Picture of the Day Website, 238
Audacity, editing files with, 15, 17–18
Auditor distro
 Driftnet, 181–182
 Kismet, 182–184
 Mailsnarf, 179–180
 Nikto, 177–178
 overview of, 175–177
 reviews of, 184
 URLsnarf, 180–181
author, Website of, 56
Auto mode for card, 49
Autohide on/off control (Remote Desktop Connection), 69
auto-populating address book, 62–64
Azureus BT client, 55

B

B card, 48, 51
background, changing, 217, 238–239
backing up
 checking files after, 116
 MBR, 92–93
 partitions, 100–102
 XF86Config-4 file, 96
Beginner option, 273
Beginning Regular Expressions (Andrew Watt), 24
BioKnoppix, 173
BitTornado, downloading and installing, 54
BitTorrent (BT), 53–55
black hat hacker, 134
blank screen, troubleshooting, 264–265
Bluetooth device, setting up as modem, 51
Bookmarks → Add Bookmark, 72
boot command line limit, 261
boot disk, creating, 278–279

boot issues

- GRUB, fixing, 94
- LILO, fixing, 93–94
- restoring missing MBR, 92–93

boot screen, changing, 218, 239, 241

boot splash screen, 256

booting process

- bootloader phase, 258–259
- with different kernel
 - loop Linux Kernel Module, adding, 222
 - copying kernel, 225
 - installing pre-made kernel, 220
 - make-kpkg command, 221
 - overview of, 219–220
 - updating initial RAM disk, 223–225

graphics phase, 263

ideal, 255

Knoppix view, 256–258

shutdown phase, 263–264

text phase, 259–263

traditional view, 255–256

troubleshooting, 264–268

boot.ini file, accessing to resolve start issues, 111–114

bootloader phase of boot process, 258–259

broadband connection to Internet, 47–48

browser (Mozilla Firefox)

- extensions, installing, 55–56
- fonts, changing, 8–9
- Home Page, improving, 55
- searches, focusing, 56–58
- upgrading, 249–250

BT (BitTorrent), 53–55

Buddy List window (Gaim), 66

burning CD with K3b

- Advanced tab, 32–34
- Burn button, 34
- burn speed, setting, 28–29
- Filesystem tab, 30–32
- overview of, 25–27, 117–119
- settings, changing, 29–30
- Volume Desc tab, 30

Business Software Alliance, 227

C

captive-ntfs program, 111

Capture Options window (Ethereal), 142

CD

burning with K3b

- Advanced tab, 32–34
- for back up and recovery, 117–119
- Burn button, 26, 33
- burn speed, setting, 27–29
- Filesystem tab, 29–32
- overview of, 25–27, 117–119
- settings, changing, 29–30
- Volume Desc tab, 30
- mastering, 226, 241, 252–253
- playing, 267–268

CD-Recordable FAQ (Andy McFadden), 34

CD-R/RW device, confirming K3b sees, 26

CD-Writing HOWTO Website, 33

cell phone, setting up as modem, 51

changing

- application fonts, 8–11
- background, 217, 238–239
- boot screen, 218, 239, 241
- desktop environment, 219
- desktop manager, 266
- fonts
 - application, 8–11, 244
 - system, 4–8, 244

Knoppix without remastering, 207–211

printer driver, 13

runlevel, 262–263

username, 274–275

Windows Administrator password, 200

cheatcodes

- defining default, 218
- description of, 258
- finding undocumented, 268
- graphics phase, 263
- keyboard shortcuts for viewing, 257
- shutdown phase, 264
- text phase and, 260

checking for dangerous weaknesses, 134–140

chkrootkit program, 128–130

chntpw program, 115

chroot command, 229

ClamAV (INSERT), 197–199

loop command-line utilities, 215, 228

loop driver, 222

cluster, definition of, 159

clustering

- ClusterKnoppix and, 167–172
- concepts of, 160

- ParallelKnoppix and, 161–167
- system administrator and, 159–160
- ClusterKnoppix
 - description of, 167
 - John the Ripper, 169–172
 - POV-Ray, 169
 - setting up, 167–169
- Clusty toolbar, 56
- command-line controls for FreeNX server, 71
- command-line programs
 - chkrootkit program, 128–130
 - ImageMagick, 22–24
 - SCP (secure copy), 75–76
 - SFTP, 74
 - vim, 35–36
- commands
 - boot, optimizing, 264
 - chroot, 229
 - cp, 229
 - dd, 93, 100, 154–155
 - dd_rescue, 100–101
 - deborphan, 250
 - df -h, 28
 - du, 230, 233
 - grep, 152
 - \$ ifconfig, 51
 - lazarus, 152–153
 - mactime, 150–151
 - make-kpkg, 221
 - NFS, 86
 - pdf2ps, 41
 - pdftotext, 41
 - ps2pdf, 41
 - regedit, 114
 - rm, 98
 - sign-key, 124–125
 - smbclient, 77–78
 - split, 102
 - ssh, 101–102
 - submount, 80, 84–85
 - sudo ifconfig eth1 down, 50
 - tar, 101–102
 - tiff2pdf, 41
 - traceroute, 201
 - unrm, 151–152
 - wipe, 155–156
- Common Unix Printing System (CUPS), 11–12
- configuration files, saving, 207, 208–209
- Configuration window (KPPP), 46
- Configure window (Konqueror), 6–7
- Configure → Configure printer(s), 11
- configuring
 - DNS (Domain Name Server), 52
 - installation of Knoppix to hard drive, 273–277
 - KMail, 59–62
 - prior to creating Myppix, 244–245
 - Samba, 76–77
- connecting
 - to Internet
 - via broadband, 47–48
 - via modem, 45–47
 - wirelessly, 48–51
 - to Samba share on another machine, 78–80
- console window, opening, 270
- contextual menu (Kuickshow), 19
- controlling another computer with remote desktop
 - connection
 - FreeNX and, 69–71
 - VNC and, 67–69
- converting
 - MP3 to WAV, 15–16
 - PostScript document to PDF, 42
- copying
 - all free disk space, 151
 - data over network, 120
 - file using SSH, 75–76
 - kernel, 225
 - saved configurations, 252
- The Coroner's Toolkit (TCT)
 - grave-robber, 148–150
 - lazarus, 152–153
 - mactime, 150–151
 - overview of, 147
 - unrm, 151–152
- corpse, 148
- cp command, 229
- cracking and rootkits, 128
- Create Knoppix Configuration Archive window, 245–246
- Create Partition dialog box (QTParted), 108–109
- cron job, setting up, 129–130
- CUPS (Common Unix Printing System), 11–12
- Current Projects (K3b), 27
- cursor, positioning, 36

- customizing
 - application fonts, changing, 8–11
 - look of Myppix, 251
 - saving changes, 3
 - system fonts, replacing, 4–8
- D**
- “dartboard” technique, 163
- data
 - encrypting
 - GnuPG and, 121–127
 - protecting against Ethereal and, 147
 - SSH and, 75
 - recovering
 - CD or DVD, burning data to, 117–119
 - copying over network, 120
 - emailing data to self, 119
 - overview of, 115
 - preparation for, 116
 - USB jump drive, saving data to, 116–117
- Data Project window (K3b)
 - Advanced tab, 32–34
 - Filesystem tab, 30–32
 - Settings tab, 29
 - Volume Desc tab, 30
 - Writing tab, 28
- dd command, 93, 100, 154–155
- dd_rescue command, 100–101
- Debian Jr. packages, 235–238
- Debian Linux, 273
- deborphan command, 250
- decrypting file, 127
- defragmenting hard drive, 106
- desktop environment, changing, 219
- desktop manager, changing, 266
- desktop publishing software, 40–41
- dev packages, removing, 234–235
- Development → Kompare, 43
- df -h command, 29
- DHCP (Dynamic Host Configuration Protocol), 51
- DHCP (Dynamic Host Configuration Protocol)
 - server, 47–48
- dial-up account, setting up, 46
- digitally signing file, 126
- Disconnected IMAP option (KMail), 61
- DistCCKnoppix, 173
- Domain Name Server (DNS), configuring, 52
- downloading
 - BitTornado, 54
 - FTP file, 72
 - Knoppix ISO with BitTornado, 54
- Driftnet, 181–182
- driver, changing for printing, 13
- du command, 230, 233
- dual-boot system, creating, 92
- DVD
 - burning data to, 117–119
 - playing, 267–268
- Dynamic Host Configuration Protocol (DHCP), 51
- Dynamic Host Configuration Protocol (DHCP)
 - server, 47–48
- E**
- editing
 - images
 - GIMP, using, 20–22
 - ImageMagick, using, 22–24
 - sound files with Audacity, 15, 17–19
 - text editors
 - Kate, 36–38
 - overview of, 34
 - vim, 35–36
 - text files, comparing, 43–44
 - Windows System Registry, 114–115
- Editors → Kate, 36
- 802.11b card, 48, 178
- emacs text editor, 34–35
- email, reading and sending. *See* KMail
- emailing
 - data to self, 119
 - encrypted data, 125–126
- emergency mode, 261
- encryption
 - GnuPG and
 - generating keys, 122–123
 - importing keys, 123–124
 - overview of, 121–122
 - using keys, 124–127
 - protecting against Ethereal and, 147
 - SSH and, 75
- ensuring machine will run Linux, 91–92
- error message when first opening Audacity, 17

- Ethereal
 - capture window, 143–144
 - Filter Expression window, 145
 - filtering capture, 145–146
 - main window, 142, 144–145, 146
 - overview of, 141–142
 - protecting against, 147
 - setting capture options, 142–143
- Ext2 and Ext3 filesystems, examining and repairing, 96–97
- F**
- fail-over cluster, 159
- Fat32 (VFAT) filesystems, examining and repairing, 97–98
- File Transfer Protocol (FTP), 71–73
- File → Export As WAV, 18
- filenames, 33
- File → Open, 17
- files
 - ASCII, 124
 - Audacity, editing with, 15, 17–19
 - boot .ini, accessing to resolve start issues, 111–114
 - configuration, saving, 207, 208–209
 - copying using SSH, 75–76
 - decrypting, 127
 - encrypting and digitally signing, 125–127
 - hosts, editing, 35
 - KNOPPIX/KNOPPIX, 214, 215
 - Konqueror file manager
 - adding music to playlist using, 15
 - Configure window, 6–7
 - fonts, changing, 6–8
 - FTP client software and, 72–73
 - opening image in, 19
 - Samba and, 78–85
 - SFTP and, 74–75
 - PDF, 39, 41–43
 - sharing
 - with BitTorrent, 53–55
 - with NFS, 85–86
 - with Samba, 76–85
 - std.vcf, 62–63
 - system, setting up, 244
 - text, comparing, 43–44
 - torrent, 53–54
 - XF86Config-4, 96
- filesystem check, performing, 96–98
- filesystems
 - examining and repairing
 - Ext2 and Ext3, 96–97
 - Fat32 (VFAT), 97–98
 - JFS, 98
 - NTFS, 98
 - XFS, 98
 - proc
 - mounting, 229
 - unmounting, 238
 - ReiserFS
 - examining and repairing, 97
 - QTParted and, 99
- Filter Expression window (Ethereal), 145
- Filters menu (GIMP), 21
- finding
 - all images on hard drive, 186–188
 - undocumented cheatcodes, 268
- Firefox (Mozilla)
 - extensions, installing, 55–56
 - fonts, changing, 8
 - Home Page, improving, 55
 - searches, focusing, 56–58
 - upgrading, 249–250
- firewall, 47
- floppy disk, for booting, creating, 278–279
- fonts
 - application, changing, 8–11
 - changing, 244
 - system, replacing, 4–8
- Fonts & Colors dialog box (Firefox), 9
- Fonts Control Center (KDE), 5–6
- forensics (The Coroner's Toolkit)
 - grave-robber, 148–150
 - lazarus, 152–153
 - mactime, 150–151
 - overview of, 147
 - unrm, 151–152
- formats
 - OpenOffice.org and, 39
 - XMMS and, 15
- FreeNX
 - command-line controls for, 71
 - overview of, 69–70
 - setting up, 70
- FTP (File Transfer Protocol), 71–73
- F2 or F3, 257
- function keys and virtual console, 262

G

G card, 48, 50, 51
 GAIM, 64–66, 194
 generating keys, 122–123
 GIMP (GNU Image Manipulation Program), editing
 images with, 20–22
 gkismet, 182–184
 Gmail account, 60
 GNU Octave, 162–163
 GnuPG (Gnu Privacy Guard)
 generating keys, 122–123
 importing keys, 123–124
 overview of, 121–122
 using keys, 124–127
 Googlebar, 56
 Gpart, 102–103
 GPG keyring, importing, 123–124
 GRAB, 186, 187
 GRand Unified Bootloader (GRUB)
 fixing, 94
 installation process and, 276
 graphics phase of boot process, 263
 Graphics → GIMP Image Editor, 20
 Graphics → Kuickshow, 19
 Graphics → More Applications → KSnapshot, 23
 grave-robber, 148–150
 grep command, 152
 Groove Search toolbar, 56
 GRUB (GRand Unified Bootloader)
 fixing, 94
 installation process and, 276
 Gutmann, Peter (security researcher), 155

H

hard drive
 chkrootkit program and, 129
 defragmenting, 106
 finding all images on, 186–188
 imaging, 186
 installing Knoppix to
 beginning install, 277–279
 configuring installation, 273–277
 overview of, 269–270
 partitioning for, 271–273
 preparations for, 270
 steps for, 270–271
 space on, and converting MP3 to WAV, 16
 wiping
 dd command and, 154–155
 overview of, 153–154
 wipe command and, 155–156
 writing ISO image to, 29
 hash value, 170
 Helix distro
 GRAB, 186, 187
 overview of, 185
 Retriever, 186–188, 189
 working on live Windows machine
 gathering information, 190–192
 overview of, 188–189
 viewing IE history, 192–193
 viewing passwords, 193–196
 help system
 Helix, 196
 vim, 36
 high-availability cluster, 159
 home directory, saving, 207, 209–211
 hosts file, editing, 35

I

IBM developerWorks Website, 33
 IE history, viewing, 192–193
 \$ ifconfig command, 51
 ImageMagick, manipulating graphics and, 22–24
 images
 editing
 GIMP, using, 20–22
 ImageMagick using, 22–24
 viewing using Kuickshow, 19–20
 imaging hard drive, 186
 IMAP option (KMail), 61
 importing keys, 123–124
 initial RAM disk, updating, 223–225
 INSERT (Inside Security Rescue Toolkit)
 ClamAV, 197–199
 overview of, 196–197
 reading and writing NTFS partitions, 199–200
 testing system RAM, 200–201
 tracing route, 201–202
 Windows Administrator password, changing, 200
 installing
 BitTornado, 54
 extensions to Firefox, 55–56

- Knoppix to hard drive
 - beginning install, 277–279
 - configuring installation, 273–277
 - overview of, 269–270
 - partitioning for, 271–273
 - preparations for, 270
 - steps for, 270–271
 - Microsoft Web fonts, 4–5
 - pre-made kernel, 220
 - search toolbar, 56
 - software
 - for kids distro, 235–238
 - with KPackage, 205–207
 - remastering and, 216–219
 - instant messaging, 64–66
 - Intel Centrino technology, 48
 - Internet
 - accessing
 - broadband connection, 47–48
 - modem connection, 45–47
 - static address, setting, 51–52
 - wirelessly, 48–51
 - browsing with Mozilla Firefox, 55–58
 - sharing with BitTorrent, 53–55
 - Internet → Bittornado Client, 54
 - Internet → Ethereal (as root), 141
 - Internet → Gaim Internet Messenger, 64
 - Internet → KMail, 10, 58
 - Internet → More Applications → LinNeighborhood, 80
 - Internet → Remote Desktop Connection, 68
 - IP Subnet Mask Calculator Website, 131
 - ISO, testing, 226
 - IT Conversations Website, 16
- J**
- JFS filesystems, examining and repairing, 98
 - job, definition of, 159
 - John the Ripper, 169–172
 - Joliet extensions, 31, 33
 - Jybe extension, 56
- K**
- KAddressBook (KMail), 62
 - Kanotix, 270
 - Kate text editor, 37–38
 - KDE
 - default panel, changing, 244–245
 - fonts, changing, 5–6
 - network transparency information Website, 38
 - preferences, setting, 244
 - KDE Desktop, 257
 - KDE PPP tool (KPPP)
 - Configuration window, 46
 - New Account window, 46–47
 - KDE printer configuration tool, 12
 - KDE Printer Wizard, 12
 - kernel level rootkit, 128
 - kernel regression, 162–163
 - kernel, swapping Linux
 - cloop Linux Kernel Module, adding, 222
 - copying kernel, 225
 - installing pre-made kernel, 220
 - make-kpkg command, 221
 - overview of, 219–220
 - updating initial RAM disk, 223–225
 - key pair, 122
 - keyboard shortcuts
 - Alt+SysRq+B (reboot), 266
 - F2 or F3, 257
 - function keys and virtual console, 262
 - PgDn/Page Down and PgUp/Page Up, 19
 - keyserver, importing keys from, 124
 - kids, distro for
 - background, changing, 238–239
 - boot screen, changing, 239, 241
 - customizing look of, 238–241
 - environment, preparing, 229
 - installing software for, 235–238
 - mastering CD, 241
 - preparation for creating, 228
 - reasons for creating, 227
 - removing unneeded software, 230–235
 - testing, 242
 - Kismet, 182–184
 - KMail
 - configuring, 59–62
 - fonts, changing, 10
 - working with, 62–64
 - Knoppix → Configure → Create a Persistent Knoppix Home Directory, 209
 - Knoppix → Configure → Save Knoppix, 3
 - Knoppix → Configure → Save Knoppix configuration, 208, 245

knoppix-mkimage script, 207, 209–211
 Knoppix → Services → Start NX Server, 70
 Knoppix → Services → Start openMosix Terminal Server, 167
 Knoppix → Services → Start Samba Server, 76
 Knoppix → Services → Start SSH Server, 73
 Knoppix → System → QTParted, 106
 Knoppix → Utilities → Manage Software in Knoppix (kpackage), 205
 Kompare, 43–44
 Konqueror file manager
 adding music to playlist using, 15
 Configure window, 6–7
 fonts, changing, 6–8
 FTP client software and, 72–73
 opening image in, 18
 Samba and, 78–85
 SFTP and, 74–75
 Konsole, 229
 KPackage, 4–5, 205–207
 KPDF, 43, 205–207
 KPPP (KDE PPP tool)
 Configuration window, 46
 New Account window, 46–47
 KSnapshot, 23
 K3b
 Advanced tab, 32–34
 Burn button, 26, 33
 burn speed, setting, 27–29
 burning CD with, 25–27
 Filesystem tab, 29–32
 settings, changing, 29–30
 Volume Desc tab, 30
 Website, 33
 Kubuntu, 270
 Kuickshow, 19–20
 KWrite, boot.ini file open in, 112–113

L

language, setting, 218
 laptops and Linux, 91
 lazarus command, 152–153
 LILO (LIInux LOader), fixing, 93–94
 LinNeighborhood
 learning syntax of smbmount using, 84–85
 mounting share using, 80–84

Linux

ensuring machine will run, 91–92
 partitions
 backing up, 100–102
 QTParted and, 98–100
 restoring lost, 102–103
 swapping kernel
 cloop Linux Kernel Module, adding, 222
 copying kernel, 225
 installing pre-made kernel, 220
 make-kpkg command, 221
 overview of, 219–220
 updating initial RAM disk, 223–225
 system issues
 filesystem check, performing, 96–98
 root password, forgotten, resetting, 94–95
 X, fixing, 95–96
 Linux cluster, 160
 Linux Kernel Module (LKM), 128
 LIInux LOader (LILO), fixing, 93–94
 LinuxPrinting.org, 13
 live system, 148
 Load Files dialog box (XMMS), 15
 Local mailbox option (KMail), 61
 Logout → End Current Session, 5
 Logout → Restart Computer from within KDE, 258, 263
 Logout → Turn off Computer, 258, 263
 Lucent Orinoco Gold 802.11b card, 48, 178

M

Macromedia Flash, OpenOffice.org and, 39
 mactime command, 150–151
 Mail Password Viewer (Helix), 194
 Maildir mailbox option (KMail), 61
 mailing list for K3b, 34
 Mailsnarf, 179–180
 make-kpkg command, 221
 Manage Identities screen (KMail), 59
 Managed mode for card, 49
 man-in-the-middle attack, 75
 Master Boot Record (MBR)
 restoring missing, 92–93
 wipe command and, 155
 Master mode for card, 49

- mastering CD
 - Archix, 241
 - Myppix, 252–253
 - overview of, 226
 - The Matrix Reloaded* (movie), 134
 - McFadden, Andy, CD-Recordable FAQ, 34
 - Medialogic NoMachine NX, 69–70
 - MEPIS, 270
 - Message Passing Interface (MPI), 159, 161
 - Messenger Password (Helix), 193–194
 - Microsoft
 - Office and OpenOffice.org, 38
 - schools and, 227
 - SMB/CIFS, 76, 85
 - Web fonts, installing, 4–5
 - Windows
 - Administrator password, changing, 200
 - partitions, resizing, 105–110
 - recovering data, 115–120
 - system issues, 111–115
 - working on with Helix, 188–196
 - miniT extension, 56
 - modem
 - connecting to Internet via, 45–47
 - setting cell phone or Bluetooth device up as, 51
 - Morphix-NLP, 173
 - Mount Dialog window (LinNeighborhood), 84
 - mounting
 - music share, 83–84
 - proc filesystem, 229
 - Mozilla
 - Firefox
 - extensions, installing, 55–56
 - fonts, changing, 9
 - Home Page, improving, 55
 - searches, focusing, 56–58
 - upgrading, 249–250
 - improving printing in, 13–14
 - Thunderbird, upgrading, 249–250
 - Update Website, 55
 - MPI (Message Passing Interface), 159, 161
 - MP3, converting to WAV, 16
 - mtr program, 201–202
 - multimedia
 - images
 - GIMP, editing using, 20–22
 - ImageMagick, manipulating using, 22–24
 - Quickshow, viewing using, 19–20
 - sound
 - Audacity, editing files with, 15, 17–18
 - XMMS, listening to music with, 14–15
 - video, watching, 25
 - Multimedia → Audacity, 17
 - Multimedia → K3b, 26
 - Multimedia → Video → xine media player, 25
 - Multimedia → Viewers → Acrobat Reader, 41
 - Multimedia → XMMS, 14
 - multiple persistent disk images, using, 267
 - music, listening to with XMMS, 14–15, 80
 - Myppix
 - configuring prior to creating, 244–245
 - creating, 247–251
 - customizing, 251
 - mastering CD, 252–253
 - overview of, 243
 - saved configurations, copying, 252
 - saving changes prior to creating, 245–246
 - testing, 253
- ## N
- ndiswrapper software, 48, 50–51
 - Nessus
 - client, opening, 135
 - description of, 134
 - logging in to, 136
 - plug-ins and, 134–135
 - report window, 139
 - saving reports, 140
 - Security Notes, 139
 - Target tab, 137–138
 - using, 137
 - network
 - copying data over, 120
 - sniffing packets on
 - Driftnet and, 181–182
 - Ethereal and, 141–147
 - Mailsnarf and, 179–180
 - overview of, 140–141
 - switched, 143
 - network ID, setting, 48
 - Network screen (KMail), 59–60
 - Network/Internet → ADSL/PPPOE, 48
 - Network/Internet → /dev/modem connection setup, 51
 - Network/Internet → ISDN connection, 48
 - Network/Internet → Modem Dialer, 46

Network/Internet → ndiswrapper configuration, 50
 Network/Internet → Wavelan configuration, 48
 New Account window (KPPP), 46–47
 NFS, sharing and accessing files with, 85–86
 Nikto, 177–178
 Nmap program, 130–134
 NoMachine NX (Medialogic), 69–70
 NTFS filesystems, examining and repairing, 98
 NTFS partitions, reading and writing, 199–200

O

OASIS (Organization for the Advancement of Structured Information Standards), 38
 Octave, 162–163
 office software
 OpenOffice.org, 11, 38–40, 233
 Scribus, 40–41
 Offline NT Password and Registry Editor, 115
 OGG format, 15
 online forum for OpenOffice.org, 39
 opening
 Adobe Acrobat Reader, 41
 Apache Web server, 87
 Audacity, 17
 console window, 270
 Ethereal, 141
 FreeNX server, 70
 Gaim, 64
 GIMP, 20
 Kate, 37–38
 KDE Printer Wizard, 12
 KMail, 10, 58
 Kompare, 43
 Konqueror, 6
 KPackage, 4, 205
 K3b, 26
 Kuickshow, 19
 Nessus, 135
 NFS, 86
 OpenMosix Terminal Server, 167
 OpenOffice.org, 11
 Remote Desktop Connection, 68
 Samba, 76
 Scribus, 40
 sound file, 17
 SSH, 73
 vim, 35

 xine video player, 24–25
 XMMS, 14
 openMosix clustering technology, 167
 OpenOffice.org 1.1.4 → OpenOffice.org 1.1.4 Printer Administration, 11
 OpenOffice.org (OOo)
 fonts, changing, 11
 kids distro and, 233
 overview of, 38–40
 optimizing boot command, 264
 Organization for the Advancement of Structured Information Standards (OASIS), 39

P

packet
 description of, 140
 Ethereal and, 141–147
 sniffing programs and, 140–141, 179–182
 PaiPix, 173
 ParallelKnoppix
 description of, 159, 161
 getting data into, 164–165
 Octave for kernel regression, 162–163
 pi calculation, 163–164
 semi-permanent cluster for using, 165–167
 setting up, 161
 Partition Menu window, 272
 partitions
 for installing Knoppix on hard drive, 271–273
 Linux
 backing up, 100–102
 QTParted and, 98–100
 restoring lost, 102–103
 NTFS, reading and writing, 199–200
 Windows, resizing
 overview of, 105
 preparation for, 106
 QTParted and, 106–110
 passphrase for encryption, 122
 password
 creating, 70
 Ethereal and, 141
 for installing Knoppix on hard drive, 275–276
 resetting forgotten root, 94–95
 root, 149
 Samba and, 80, 81–82
 setting, 217

- viewing, 193–196
 - Windows Administrator, changing, 200
- password-auditing utility, 169–172
- PCI modem, 45
- PCMCIA modem, 45
- PDF file
 - Adobe Acrobat Reader and, 41–43
 - OpenOffice.org and, 39
- pdftotext command, 41
- pdf2ps command, 41
- persistent Knoppix disk image
 - benefits of, 5
 - multiple, using, 267
- personal Knoppix (Myppix)
 - configuring prior to creating, 244–245
 - creating, 247–251
 - customizing, 251
 - mastering CD, 252–253
 - overview of, 243
 - saved configurations, copying, 252
 - saving changes prior to creating, 245–246
 - testing, 253
- PgDn/Page Down and PgUp/Page Up, navigating
 - images with, 19
- pi calculation, 163–164
- pinging Website, 229–230
- playing DVD or CD with one CD/DVD-ROM drive, 267–268
- Playlist Editor window (XMMS), 14–15
- Plugins tab (Nessus), 136
- pmandel run, 166
- POP3 option (KMail), 61
- ports, open, scanning for, 130–134
- positioning cursor, 36
- PostScript document, converting to PDF, 42
- POV-Ray rendering, 160, 169
- Preferences window (LinNeighborhood), 81
- Printer Administration dialog box (OpenOffice.org), 11
- printers
 - setting up, 11–14, 244
 - sharing
 - with NFS, 85–86
 - with Samba, 78–85
- private key, 121
- proc filesystem
 - mounting, 229
 - unmounting, 238
- ps2pdf command, 41
- public key cryptography, 121

Q

- QEMU utility, 226, 242
- QTParted
 - Linux partitions and, 98–100
 - visual interface, 272
 - Windows partitions and, 105, 106–110
 - wiping hard disk and, 153–154
- Quantian, 174

R

- RAM, testing, 200–201
- RDP (Remote Desktop Protocol), 68–69
- reading email. *See* KMail
- reading partitions, 199–200
- rebooting, 258, 266
- recovering data
 - CD or DVD, burning data to, 117–119
 - copying over network, 120
 - emailing data to self, 119
 - overview of, 115
 - preparation for, 116
 - USB jump drive, saving data to, 116–117
- regedit command, 114
- regular expressions, 24
- ReiserFS filesystems
 - examining and repairing, 97
 - QTParted and, 99
- remastering
 - booting with different kernel, 219–225
 - changing Knoppix without, 207–211
 - extracting KNOPPIX/KNOPPIX file, 215
 - installing and removing software, 216–219
 - mastering CD, 226
 - mounting KNOPPIX/KNOPPIX file, 214
 - overview of, 213
 - preparation for, 214
- remote control
 - FreeNX and, 69–71
 - VNC and, 67–69
- Remote Desktop Protocol (RDP), 68–69
- removing software
 - for kids distro, 230–235
 - for Myppix, 247–249
 - overview of, 216–219
- Repeater mode for card, 49
- resetting forgotten root password, 94–95
- Resize Partition dialog box (QTParted), 107

- resizing
 - Windows partitions
 - overview of, 105
 - preparation for, 106
 - QTParted and, 106–110
 - XMMS interface, 14
 - Resource Configuration window, 63
 - restarting X, 5
 - restoring
 - lost partitions, 102–103
 - missing Master Boot Record, 92–93
 - Retriever, 186–188, 189
 - rm command, 98
 - Rock Ridge extensions, 31, 32
 - root password, forgotten, resetting, 94–95
 - rootkits, verifying absence of, 128–130
 - route, tracing, 201–202
 - router, 47, 48
 - runlevel, changing, 262–263
- S**
- salt value, 170
- Samba, starting and configuring, 76–77
- saveconfig script, 207, 208–209
- saving
 - changes when customizing, 3
 - configuration files, 207, 208–209
 - data to USB jump drive, 116–117
 - home directory, 207, 209–211
 - Nessus report, 140
 - personal settings, 245–246
 - screenshots in TIFF format, 23
 - in vim, 36
 - WAV file, 18
- scanning
 - for open ports, 130–134
 - for viruses, 197–199
 - Web servers, 177–178
- science-oriented Knoppix variants, 172–174
- SCP (secure copy), using, 75–76
- screenshots, saving in TIFF format, 23
- Scribus, 40–41
- Script-Fu menu (GIMP), 21
- searching with Firefox, 56–58
- Secondary mode for card, 49
- secure shell (SSH)
 - copying file using, 75–76
 - enabling for secure connections, 73
 - encryption and, 75
 - FTP and, 74–75
 - overview of, 73
 - using, 73–74
- security distros
 - Auditor
 - Driftnet, 181–182
 - Kismet, 182–184
 - Mailsnarf, 179–180
 - Nikto, 177–178
 - overview of, 175–177
 - reviews of, 184
 - URLsnarf, 180–181
 - Helix
 - GRAB, 186, 187
 - overview of, 185–186
 - Retriever, 186–188, 189
 - working on live Windows machine, 188–196
 - INSERT
 - ClamAV, 197–199
 - overview of, 196–197
 - reading and writing NTFS partitions, 199–200
 - testing system RAM, 200–201
 - tracing route, 201–202
 - Windows Administrator password, changing, 200
- security issues. *See also* encryption; security distros
 - FTP and, 71–72
 - NFS, 85, 86
 - openMosix and, 167
 - ParallelKnoppix and, 161, 162
 - portmap and, 86
 - SFTP and, 74
 - SMB and, 85
 - SSH and, 73
 - Telnet and, 73
- selecting printer, 13
- sending email. *See* KMail
- SessionSaver extension, 56
- Settings → Configure Konqueror, 6
- SFTP, using, 74–75, 120
- shared system, cluster compared to, 159
- sharing files
 - with BitTorrent, 53–55
 - with NFS, 85–86
 - with Samba, 76–85
- shutting down computer, 258, 263–264
- signing keys in keyring, 124–125

- sign-key command, 124–125
- Smart Boot Manager, 259
- SMB/CIFS (Microsoft), 76, 85
- smbclient command, 77–78
- sniffing
 - packets on network
 - Driftnet and, 181–182
 - Ethereal and, 141–147
 - Mailsnarf and, 179–180
 - overview of, 140–141
 - wireless network, 182–184
- software. *See also specific software*
 - The Coroner's Toolkit (TCT)
 - grave-robber, 148–150
 - lazarus, 152–153
 - mactime, 150–151
 - overview of, 147
 - unrm, 151–152
 - desktop publishing, 40–41
 - file-sharing, 53
 - installing
 - for kids distro, 235–238
 - with KPackage, 4–5, 205–207
 - when remastering, 216–219
 - office, 38–40
 - removing, 216–219, 230–235, 247–249
- sound
 - Audacity, editing files with, 15, 17–19
 - XMMS, listening to music with, 14–15
- split command, 102
- ssh command, 101–102
- SSH (secure shell)
 - copying file using, 75–76
 - enabling for secure connections, 73
 - encryption and, 75
 - FTP and, 74–75
 - overview of, 73
 - using, 73–74
- starting
 - Adobe Acrobat Reader, 41
 - Apache Web server, 87
 - Audacity, 17
 - Ethereal, 141
 - FreeNX server, 70
 - Gaim, 64
 - GIMP, 20
 - Kate, 37–38
 - KDE Printer Wizard, 12
 - KMail, 10, 58
 - Kompare, 43
 - Konqueror, 6
 - KPackage, 4, 205
 - K3b, 26
 - Kuickshow, 19
 - Nessus, 135
 - NFS, 86
 - OpenMosix Terminal Server, 167
 - OpenOffice.org, 11
 - Remote Desktop Connection, 68
 - Samba, 76
 - Scribus, 40
 - sound file, 17
 - SSH, 73
 - vim, 35
 - xine video player, 24–25
 - XMMS, 14
- static address, setting, 51–52
- std.vcf file, 62–63
- submount command, 80, 84–85
- sudo ifconfig eth1 down command, 50
- swapping Linux kernel
 - cloop Linux Kernel Module, adding, 222
 - copying kernel, 225
 - installing pre-made kernel, 220
 - make-kpkg command, 221
 - overview of, 219–220
 - updating initial RAM disk, 223–225
- switched network and Ethereal, 143
- SYN scanning, 132–133
- system files, setting up, 244
- system fonts, replacing, 4–8
- system hostname, creating, 276
- system issues
 - Linux
 - filesystem check, performing, 96–98
 - root password, forgotten, resetting, 94–95
 - X, fixing, 95–96
 - Windows
 - accessing boot.ini to resolve start issues, 111–114
 - editing System Registry, 114–115
 - overview of, 111
- System → QTParted, 98
- System → Root Terminal, 149
- System → Security → Nessus Security Tool → Network Scanner, 135

T

- tar command, 101–102
- Target tab (Nessus), 137–138
- Telnet, 73
- terminal application, 229
- test page, printing, 13
- testing
 - burned CD, 32
 - ISO, 226
 - key pair, 123
 - kids distro, 242
 - machine to ensure it runs Linux, 92
 - music mount, 84
 - Myppix, 253
 - Samba, 77
 - system RAM, 200–201
 - vga cheatcodes, 266
 - for vulnerabilities
 - checking for dangerous weaknesses, 134–140
 - scanning for open ports, 130–134
 - verifying absence of rootkits, 128–130
 - xmodules, 265
- text editors
 - choosing, 244
 - Kate, 37–38
 - overview of, 34
 - vim, 35–36
- text files, comparing, 43–44
- text phase of boot process, 259–263
- text selection, enabling, 42
- Thunderbird (Mozilla), upgrading, 249–250
- TIFF format, saving screenshots in, 23
- tiff2pdf command, 41
- toolbars, search, installing, 56
- torrent files, 53–54
- traceroute command, 201
- Tridgell, Andrew (programmer), 76
- troubleshooting boot process
 - blank screen, 264–265
 - desktop manager, changing, 266
 - multiple persistent disk images, using, 267
 - playing DVD or CD with one CD/DVD-ROM drive, 267–268
 - rebooting, 266
 - undocumented cheatcodes, finding, 268
 - vga cheatcodes, 266
 - xmodules, testing, 265
- Trueg, Sebastian (creator of K3b), 34
- turning Samba on and off, 77

U

- Ubuntu, 270
- UDF (Universal Disk Format), 31
- UnionFS, 207
- unmounting `proc` filesystem, 238
- unrm command, 151–152
- updating
 - initial RAM disk, 223–225
 - Nessus plug-ins, 135
- upgrading Firefox and Thunderbird, 249–250
- uploading FTP file, 73
- URLsnarf, 180–181
- USB jump drive, saving data to, 116–117
- username, creating and changing, 274–275
- Utilities → Manage Software in Knoppix, 4

V

- VC (virtual console), 262
- verifying
 - absence of rootkits, 128–130
 - signature file, 127
- vga cheatcodes, testing, 266
- video, watching, 25
- viewing
 - IE history, 192–193
 - images using Kuickshow, 19–20
 - passwords, 193–196
 - PDFs with Adobe Acrobat Reader, 41–43
- vim text editor, 35–36
- virtual console (VC), 262
- virus, scanning for, 197–199
- VNC, 67–69
- vulnerabilities, testing for
 - checking for dangerous weaknesses, 134–140
 - scanning for open ports, 130–134
 - verifying absence of rootkits, 128–130

W

- wallpaper
 - creating photos to download for, 24
 - Websites for, 240
- wardriving, 183
- Watt, Andrew, *Beginning Regular Expressions*, 24
- WAV, converting MP3 to, 16
- Web browser (Mozilla Firefox)
 - extensions, installing, 55–56
 - fonts, changing, 9

- Home Page, improving, 55
- searches, focusing, 56–58
- upgrading, 249–250
- Web server
 - Apache, 87–88
 - scanning, 177–178
- Websites
 - AllMusic, 57
 - APT information, 5
 - Astronomy Picture of the Day, 238
 - Audacity, 19
 - Auditor, 176, 184
 - of author, 56
 - BitTorrent, 53, 55
 - CD-Recordable FAQ (Andy McFadden), 34
 - CD-Writing HOWTO, 34
 - cheatcodes, 258
 - chkrootkit program, 128
 - chntpw program, 115
 - ClamAV, 199
 - ClusterKnoppix, 167
 - The Coroner's Toolkit, 153
 - Dynamic Host Configuration Protocol (DHCP), 47
 - email protocol information, 62
 - encryption information, 121
 - Ethereal, 143, 147
 - filesystems, 98
 - Firefox extensions, 55
 - forensics, 153
 - FreeNX, 70
 - GIMP, 21
 - Gmail account, 60
 - GnuPG, 127
 - Gpart, 103
 - Gutmann article, 155
 - Helix, 185, 196
 - IBM developerWorks, 34
 - IM account, 64
 - ImageMagick, 22
 - inode information, 148
 - INSERT, 196–197
 - IP addresses and classes, 131
 - IT Conversations, 16
 - KDE network transparency, 38
 - Kismet, 183
 - KMail, 59
 - K3b, 34
 - Linux on Laptops, 91
 - LinuxPrinting.org, 13
 - man-in-the-middle attack, 75
 - Mozilla Update, 55
 - ndiswrapper software, 50
 - Nessus, 135, 137
 - NFS, 87
 - Nikto, 178
 - Nmap, 134
 - NoMachine (Medialogic), 70
 - OpenOffice.org, 40
 - other distros, 270
 - packet sniffing, 141, 182
 - ParallelKnoppix, 161
 - password, creating, 70
 - PDF readers, 43
 - port information, 130
 - QEMU utility, 226
 - QTParted, 100
 - Remote Desktop Connection manual, 69
 - rootkit information, 128
 - Samba, 76
 - science-oriented Knoppix variants, 173–174
 - Scribus, 40
 - search toolbars, 56
 - Smart Boot Manager, 259
 - SYN scanning, 133
 - UNIX epoch, 150
 - VNC, 68
 - wallpaper, 240
 - wipe command, 156
 - XMMS, 15
 - Xorg project, 96
 - WEP (Wired Equivalent Privacy) key, 49
 - What's This button (K3b), 27
 - Wikipedia Website, 62
 - Windows (Microsoft)
 - Administrator password, changing, 200
 - partitions, resizing
 - overview of, 105
 - preparation for, 106
 - QTParted and, 106–110
 - recovering data
 - CD or DVD, burning data to, 117–119
 - copying over network, 120
 - emailing data to self, 119
 - overview of, 115
 - preparation for, 116
 - USB jump drive, saving data to, 116–117

- system issues
 - accessing `boot.ini` to resolve start issues, 111–114
 - editing System Registry, 114–115
 - overview of, 111
- working on with Helix
 - gathering information, 190–192
 - overview of, 188–189
 - viewing IE history, 192–193
 - viewing passwords, 193–196
- Wine, 114
- wipe command, 155–156
- wiping hard drive
 - `dd` command and, 154–155
 - overview of, 153–154
 - wipe command, 155–156
- Wired Equivalent Privacy (WEP) key, 49
- wireless Internet connection, 48–51
- wireless network, detecting and sniffing, 182–184

- writing
 - ISO image to hard drive, 29
 - partitions, 199–200

X

- X, fixing, 95–96
- `XF86Config-4` file, 95
- XFree86, 96
- XFS filesystems, examining and repairing, 98
- xine video player, 25
- XMMS (X Multimedia System), listening to music
 - with, 14–15, 80
- xmodules, testing, 265
- Xorg project, 96

Y

- Yahoo! toolbar, 56

