

Index

• Numerics •

- 16-bit architectures, 105
- 32-bit architectures, 105
- 64-bit architectures
 - GMER working with, 289
 - understanding, 105

• A •

- Abrams, Lawrence (Bleeping Computer Web site owner), 349
- access
 - backdoors giving, 12–13
 - limiting/controlling physical, 140
 - need to limit, 139–140
- account logon events, auditing, 124–125
- account management, auditing, 125
- AccuHash 2.0, verifying system file integrity with, 243
- Acronis True Image
 - on DART CD, 359
 - using, BC14
- Active@ Kill Disk, using, BC22–BC23
- ActiveX
 - blocking, 73–76
 - controls in Internet Explorer 7, 78
 - danger of accepting, 65
- Ad-Aware SE Personal, using, BC2–BC3
- administrative access
 - to disable System Restore, 325
 - rootkits needing, 153
- ADS (alternate data stream), 344
- Advanced Password Generator
 - on DART CD, 362
 - using, BC18–BC19
- Agnitum Outpost Firewall
 - on DART CD, 358
 - using, BC3–BC4
- AIM (AOL Instant Messaging) network, worm infecting, 69
- Answers that work process database, 199
- AntiHookExec
 - benefits of using with other tools, 263–264
 - installing, 263
 - overview, 262
 - user-friendliness of, 245
 - using, BC8
 - using Autoruns with, 265–268
 - using Process Explorer with, 268–269
 - using HijackThis with, 264–265
- anti-malware Real Time Monitoring, instant messaging with, 68
- anti-malware utilities. *See also specific utilities*
 - on DART CD, 358–359
 - recommended, BC2–BC7
- anti-spyware software, 97. *See also specific software*
- anti-trojan software, 98–99. *See also specific software*
- antivirus software, 98
- Any Password
 - on DART CD, 362
 - using, BC19–BC20
- AOL Instant Messaging (AIM) network, worm infecting, 69
- API HookCheck (SIG^2), 164
- API hooking, overview, 159
- Applnit_DLLs injection, functioning of, 165–166
- Application log (Windows), function of, 206
- application programming interface (API)
 - kernel-mode rootkits using, 156
 - user-mode rootkits using, 155
- application-based firewalls, 91. *See also software firewalls*
- applications. *See software*
- Apropos rootkits, 239, 340–341
- archiving, event logs automatically, 208–210
- attachments, guidelines for safe, 66–68

- auditing
 - categories of securities events available for, 124–126
 - overview, 119–120
 - resources for, 120
 - turning on event logging, 121–122
 - turning on security, 122–124
- auditing policies
 - configuring and enabling, 28
 - instant messaging with, 68
- Aumha Web site, 348
- AutoComplete (Internet Explorer), disabling, 77
- automatic updates, setting up, 105–106
- AutoPlay (Windows), disabling on external drives/devices, 59
- AutoRun (Windows)
 - disabling, 58–59
 - working without, 60
- Autoruns (Sysinternals)
 - on DART CD, 360
 - detecting persistent rootkits with, 246–247
 - editing startup list with, 49–50
 - using, BC8–BC9
 - using AntiHookExec with, 265–268
- AVG Anti-Spyware Free, using, BC4

• B •

- backdoor keyloggers, 289–290. *See also* keyloggers
- backdoors
 - allowing access through ports, 183
 - overview, 12–13
 - rootkits opening, 23
- backing up
 - importance of maintaining, 29
 - preparing recovery discs for, 147–148
 - recommended software for, BC14–BC16
 - Registry, 42–43
 - software available for, 304
 - software on DART CD for, 359–360
 - storing after, 304
 - with Windows Backup Utility, 44–46
- bad sectors
 - preparing, 327
 - rootkits hiding in, 326

- BadRKDemo rootkit, DarkSpy removing, 280–282
- bandwidth, measuring use of, 223–224
- BartPE (Bart Preinstallation Environment), 236–237
- baseline
 - using, 146–147
 - value of, 146
- BIOS
 - changing boot order in, 329–331
 - rootkits residing in, 324
- BitDefender antivirus software, 238
- blackhat hacker, 337
- BlackLight (F-Secure)
 - running with Rootkit Revealer, 246
 - scanning for rootkits with, 251–253, 340
 - user-friendliness of, 245
- black-market groups, using malware, 18
- Bleeping Computer Startup Programs Database, 199
- Bleeping Computer Web site, 348–349
- boot order, changing in BIOS, 329–331
- bootable CDs
 - Linux, 316
 - Microsoft, 235–236
 - non-Microsoft Windows, 236–238
- bootsector viruses, scanning for, 60
- browsers
 - configuring securely, 29
 - using alternate, 28
- bundling, installing spyware through, 14–15
- business plans, creating physical security, 143–144
- Butler, Jamie (*Rootkits: Subverting the Windows Kernel*), 177

• C •

- CastleCops Security Forum, determining toolbar legitimacy with, 14
- CastleCops Security Professionals, 349–350
- CastleCops Services Lists, 199
- CastleCops StartupList, 199
- CCleaner, using, BC17

- CDs. *See also* Dummies Anti-Rootkit Toolkit (DART)
- burning ISO image to, 321–322, 357
 - Linux boot, 316
 - making computers boot from, 321
 - Microsoft bootable, 235–236
 - non-Microsoft bootable, 236–238
- Cermak, Mike (Tech Support Guy), 353–354
- chat clients, monitoring instant messaging accounts with, 68
- checklist for improving security, 118–119
- checksums, assessing file integrity with, 240
- ChrisRLG (Malware Removal Web site owner), 351
- cleaners, recommended for Registry and system, BC17–BC18
- cloaked rootkits, defined, 232
- computer
- activity, comparing with bandwidth usage, 224
 - needing new, 115
- computer privileges, understanding, 153.
See also user accounts
- connections, disabling network before cleaning rootkits, 319–320
- Content Zones (Internet Explorer), adjusting, 74–76
- contests, avoiding online, 67
- Coyote, Tom (Tom Coyote Security Forum owner), 354
- CPU cycles, monitoring, 228–229
- cross-diff comparison, using different rootkits-detection tools, 234
- **D** •
- DarkSpy
- analyzing Registry with, 279–280
 - comprehensiveness and user-friendliness of, 245
 - on DART CD, 361
 - detecting/removing rootkits with, 277–278
 - evaluating process activity with, 227–228
 - overview, 276–277
 - Registry Analyzer, 278
 - removing difficult rootkits with, 280–282
 - using for port-to-process mapping, 190
- DART. *See* Dummies Anti-Rootkit Toolkit
- data
- controlling flow of with packets, 199–200
 - tracking suspicious flow of, 191
- Data Sentinel, verifying system file integrity with, 244
- databases
- creating security settings, 131–133
 - researching process, 198
- dd, creating hard drive image with, 316–317
- dd for Windows, copying RAM dump with, 313–314
- DDoS (Distributed Denial of Service)
- network of zombies used in, 18
 - object of attacks, 23
- defragmenting, hard drive, 53–57
- dialers, overview, 12
- Diamond CS, Port Explorer, 190–191, 202–205, 293–300
- direct kernel object manipulation (DKOM), 171–173, 341, 342
- Direct Revenue LLC, litigation against, 309
- directory service access, auditing, 125
- Diskeeper Pro (Executive Software), 57
- Distributed Denial of Service (DDoS)
- network of zombies used in, 18
 - object of attacks, 23
- DLL injection
- Applnit_DLLs, 165–166
 - detecting with IceSword, 290–291
 - detecting with Process Explorer, 291–293
 - functioning of, 164
 - overview, 159
- DLLs (dynamic link libraries)
- kernel and user, 161–163
 - overview, 160, 162
 - rootkits targeting, 160
 - user-mode rootkits using, 155
- domain, defined, 125
- domain controller, defined, 125
- double filename extensions, viewing, 12
- downloading
- guidelines for safe, 65
 - using scanners before, BC2
- drive-by downloads, installing spyware by, 15–16

drivers, installing as rootkits, 166–168
 Dummies Anti-Rootkit Toolkit (DART)
 anti-malware utilities and scanners with,
 358–359
 backup and imaging software on, 359–360
 CD contents, 357–358
 installing CD with Microsoft Windows,
 356–357
 password protectors and generators
 on, 364
 rootkit-detection-and-removal software
 on, 361–362
 system requirements for, 355–356
 system-analysis software on, 360–361
 troubleshooting, 363
 dynamic link libraries. *See* DLLs

● E ●

Easter eggs, backdoors installed as, 13
 EAT (Export Address Table), as avenue to
 DLLs, 162
 eEye BootRoot, 343
 Elite toolbar, 339–340
 e-mail
 guidelines for safe, 66–68
 rootkits facilitating spam, 23
 EnCase, forensic assistance from, 318
 Encrypting File System (EFS), safe surfing
 with, 64
 End User License Agreements (EULAs),
 65, 339
 Eraser, using, BC21–BC22
 Eshelman, James A. (Aumha owner), 348
 Ethereal, sniffing hackers with, 205
 EULalyzer, protecting from spyware, 15
 evaluating Web sites safety with, 81–82
 Event Log Explorer, advantages of, 217–219
 event logging. *See also* auditing
 overview, 119–120
 turning on, 121–122
 event logs
 automatically archiving, 208–210
 changing default size, 207–208
 inspecting with Event Log Explorer,
 217–219
 inspecting with Event Viewer, 210–213

 inspecting with MonitorWare, 219–222
 monitoring for rootkits clues, 180
 overview, 207
 types of, 206
 Event Viewer (Windows)
 accessing, 206–207
 evaluating inspection results in, 213–214
 filtering event log data with, 214–216
 finding rootkits with, 126
 inspecting event logs with, 210–213
 upgrading to Event Log Explorer from,
 217–219
 events
 categories available for auditing, 124–126
 filtering by type of, 214–216
 evidence
 collecting, 304
 collecting RAM dump to USB flash drive,
 312–316
 guidelines for preserving, 310–312
 hiring professional to analyze, 317–318
 tracking perpetrators with, 307–308
 executable files, hidden, 11–12
 Executive Software (Diskeeper Pro), 57
 Export Address Table (EAT), as avenue to
 DLLs, 162
 external media, scanning for bootsector
 viruses, 60

● F ●

false security alerts, encouraging purchase
 of malware programs, 17
 FanBot, 343–344
 Farmer's Boot CD (FBCD), 316
 file analysis services, availability of, 305
 FileAlyzer, verifying system files with,
 240–243
 file-integrity checks, recommending, 145
 Filemon (Sysinternals)
 tracking forensic tool changes with, 312
 tracking outbound access with, 197
 filename extensions, viewing, 12
 files
 backing up with Windows Backup Utility,
 44–46
 checking for legitimacy of, 257

- scanning before opening, 67–68
- tracking forensic tool changes to, 312
- filtering, event log data, 214–216
- FIRE (Forensic and Incident Response Environment) Bootable CD, 316
- firewall logs
 - examining for Internet access attempts, 193–194
 - identifying process ID associated with identified part, 195
 - identifying process with, 195
 - identifying processes loaded by `svchost.exe` with PID 984, 196–197
 - monitoring for rootkits clues, 180–181
- firewalls
 - on DART CD, 358
 - functioning of, 83–84
 - hardware, 84–90
 - importance of having, 82
 - importance of using, 28
 - improving, 118
 - preventing drive-by downloads, 15–16
 - software, 90–93
 - understanding, 83
 - Windows XP, 93–95
- firmware, understanding, 324
- Forensic and Incident Response Environment (FIRE) Bootable CD, 316
- Forensics Acquisition Utilities, 314
- format and reinstall
 - changing boot order in BIOS, 329–331
 - for Microsoft Windows XP, 331–332
 - overview, 327–328
 - preparing for, 328–329
 - rootkits evading, 325–327
 - running rootkit detection software after, 333
 - weighing option of, 305–307
- forums
 - asking help from, 234
 - CastleCops Security Forum, 14
 - helping with Rootkit Revealer, 250–251
 - Malware Complaints, 309
 - on security Web sites, 348–354
- freeware, versus shareware, 357–358.
See also specific freeware

- F-Secure, BlackLight
 - running with Rootkit Revealer, 246
 - scanning for rootkits with, 251–253, 340
 - user-friendliness of, 245
- FU rootkit, 341–342
- FUto rootkit, 175–176, 342

● G ●

- Geeks to Go Web site, 350–351
- Genie-Soft Backup Manager Home, using, BC15
- Gibson Research Corporation
 - listing ports used by trojans, 186
 - SpinRite, 327
- Gladiator Security Forum, 351
- GMER
 - comprehensiveness and user-friendliness of, 245
 - on DART CD, 361
 - detecting/removing rootkits with, 284–286
 - enabling system monitoring/tracing in, 286–287
 - evaluating process activity with, 227–228
 - overview, 283
 - Registry feature, 288
 - using in Safe mode, 287–288
 - working with 64-bit architectures, 289
- gray-market groups, using malware, 18
- Greatis
 - Application Database, 199
 - UnHackMe, 245, 260–261, 361–362, BC12
- Group Policy Objects (GPO)
 - applying to networks, 139
 - importing security templates into, 138–139

● H ●

- HackerDefender rootkit, 185, 338
- hackers
 - catching with sniffers, 200–201
 - lack of intelligence of, 26
 - tracking, 307–308
 - using sniffers, 200
 - ways of using ports, 185–186
- HackerWatch (McAfee, Inc.), 182

- hard drives
 - choosing to reformat, 305–307
 - cleaning with Windows Disk Cleanup Utility, 51–52
 - copying infected, 304
 - creating image of infected, 315–316
 - defragmenting, 53–57
 - downloads available for
 - compromised, 364
 - firmware for, 324
 - malware using space on, 222–223
 - partitioning and formatting, 331–332
 - preparing for reformatting of, 328–329
 - problems of junked up, 46
 - rootkits evading reformatting of, 325–327
 - hard-drive erase and repair utilities, recommended, BC21–BC24
 - hardware
 - needing new computers, 115
 - obtaining updates for, 110–112
 - hardware firewalls
 - Network Address Translation (NAT) on, 87
 - overview, 84–86
 - port blocking/port stealthing with, 87–89
 - Stateful Packet Inspection component of, 89–90
 - hash values, assessing file integrity with, 240
 - Hayes, Bert (*Snort For Dummies*), 182
 - Healan, Mike (SpywareInfo Web site owner), 353
 - Helix Bootable CD, 316
 - heuristics
 - on scanners, 100, 244
 - VICE using, 270
 - HijackThis (HJT), using AntiHookExec with, 264–265
 - HIPS (Host-Intrusion Prevention Software)
 - GMER as, 286–287
 - monitoring for rootkits clues, 183
 - Hogland, Greg (*Rootkits: Subverting the Windows Kernel*), 177
 - hooking
 - direct kernel object manipulation as alternative to, 171–173
 - EAT, 162–163
 - function of, 158–159
 - IAT, 161–162
 - inline, 163–164
 - Interrupt Descriptor Table, 171
 - kernel inline, 170
 - overview, 157–158
 - percentage of threats employing, 245
 - SYSENTER, 170, 344
 - System Service Descriptor Table, 168–169
 - virtual memory manager, 176
 - hooks
 - installing drivers as rootkits, 166–168
 - privileged, 166
 - types of, 159
 - Host-Intrusion Prevention Software (HIPS)
 - GMER as, 286–287
 - monitoring for rootkits clues, 183
 - HOSTS file
 - applying updated, 29
 - using, 72–73
 - Howes, Eric (SpywareWarrior Web site owner), 353
- I ●
- IANA (Internet Assigned Number Authority), coordinating port assignments, 184–185
 - IAT (Import Address Table), as avenue to DLLs, 161–162
 - IceSword
 - comprehensive nature of, 245
 - destroying rootkits with, 257–258
 - detecting keyloggers with, 290–291
 - detecting rootkits changes with, 253–255
 - evaluating process activity with, 227
 - functions of, 259–260
 - interpreting scan results of, 256–257
 - overview, 253
 - using, BC9–BC10
 - using for port-to-process mapping, 189–190
 - IDS (Intrusion Detection Systems)
 - importance of implementing, 29–30
 - logs, monitoring for rootkits clues, 182
 - IDT (Interrupt Descriptor Table), hooking, 171

illegal material, rootkits hiding, 23
 IM (instant messaging), guidelines for safe, 68
 imaging software
 on DART CD, 359–360
 for infected hard drives, 304
 recommended, BC14–BC16
 Import Address Table (IAT), as avenue to DLLs, 161–162
 infection
 guidelines for preserving evidence of, 310–312
 options for dealing with, 303–305
 reformatting and reinstalling “cure,” 305–307
 tracking perpetrator of, 307–308
 inline hooking, 163–164, 170
 instant messaging (IM), guidelines for safe, 68
 Intermix Media, litigation against, 309
 Internet Assigned Number Authority (IANA), coordinating port assignments, 184–185
 Internet browsers
 configuring securely, 29
 using alternate, 28
 Internet connection
 danger of leaving on, 64
 defragmenting with, 56
 Interrupt Descriptor Table (IDT), hooking, 171
 Internet, disconnecting infected machines from, 324
 Interrupt service routines (ISRs), rootkits misdirecting from, 171
 Intrusion-Detection System (IDS)
 importance of implementing, 29–30
 logs, monitoring for rootkits clues, 182
 Intrusion Prevention Systems (IPS),
 importance of implementing, 29–30
 inventory procedures, protecting equipment with, 143
 ISO image, burning to CDs, 321–322, 357
 ISRs (Interrupt service routines), rootkits misdirecting from, 171

• J •

Java, blocking, 73–76
 JavaScript, blocking, 73–76
 Jotti, checking for file legitimacy with, 257

• K •

Karen’s Replicator
 on DART CD, 360
 using, BC15
 Kaspersky Antivirus version 5.0, Rootkit Revealer interacting with, 249–250
 kernel DLLs, rootkits targeting, 161–163
 kernel inline hooking, 170
 kernel patching, 169
 kernel-mode rootkits
 reformatting and reinstalling after, 306
 summary of, 154
 types of hooks used, 159
 versus user-mode rootkits, 155–156
 kernels, drivers allowing access to, 167–168
 keyloggers
 detecting with IceSword, 290–291
 detecting with Process Explorer, 291–293
 overview, 289
 rootkits enabling, 23–24
 types of, 289–290
 Kleiman, Dave (Forensic Network Advisor), 318

• L •

Laudanski, Paul and Robin (CastleCops Security Professionals Web site owners), 349
 limited-access user accounts
 establishing, 70–71
 safe surfing with, 64
 using, 27
 using on networks, 141
 value of, 141
 links, embedded within instant-messaging text, 68
 LinkScanner Pro 2.0, on DART CD, 359

- Linux Knoppix, 316
 - LinuxDefender Live! CD, booting to, 238
 - litigation
 - pursuing, 308
 - against rootkit creators, 308–309
 - Local Security Policy Editor, editing
 - policies and configuring security with, 126–127
 - Log Parser utility, investigating event logs
 - with, 220–222
 - logical bad sectors
 - preparing, 327
 - rootkits hiding in, 326
 - logon attempts, evaluating unsuccessful, 213–214
 - logon events, auditing, 125
 - logs. *See also* event logs; firewall logs
 - monitoring for rootkits clues, 180–183
 - security logs, configuring and enabling, 28
 - sniffer logs, 181–182
- **M** ●
- malicious adware
 - understanding, 13–14
 - ways of installing, 14–16
 - malware
 - chasing dodging, 192
 - ensuring rootkit survival, 152
 - exploiting rootkits, 22
 - finding, 304–305
 - overview, 9–10
 - purpose of, 16–19
 - symptoms of presence of, 31–32
 - types of, 10–16
 - using device drivers, 167
 - Malware Complaints forum, 309
 - Malware Removal Web site, 351
 - master boot record (MBR), 324
 - McAfee, Inc.
 - HackerWatch, 182
 - SiteAdvisor, 81–82, 198
 - MD5summer, verifying system file integrity
 - with, 244
 - Metasploit, maintaining list of native API
 - entries, 169
 - Microsoft Corporation
 - finding updates/patches from, 105
 - getting automatic updates from, 105–106
 - obsolete versus supported systems of, 103
 - offering patches/updates, 103–104
 - responding to rootkit threat, 20
 - Microsoft Inside-the-box GhostBuster, 273
 - Microsoft Internet Explorer
 - adding Web sites to Trusted zone, 76
 - adjusting Content Zones in, 74–76
 - disabling AutoComplete in, 77
 - using version 7, 77–79
 - vulnerability of, 28
 - Microsoft Malicious Software Removal Tool (MSRT), scanning for rootkits with, 261–262, 338
 - Microsoft Management Console (MMC)
 - comparing current security system and template with, 128–130
 - customizing security templates for networks with, 136–137
 - Microsoft Newsgroups, getting help
 - from, 352
 - Microsoft Strider GhostBuster
 - inside-the-box, 273
 - overview, 273
 - WinPE, 274
 - Microsoft TechNet: Events and Errors for the Windows and the Windows Server System Web site, 120
 - Microsoft Telnet
 - disinfecting RATs with, 298–299
 - overview, 297
 - Microsoft Update
 - implementing, 107–109
 - installing, 109–110
 - overview, 106–107
 - preparing for, 107
 - resources on, 112–113
 - Microsoft Virtual PC, 145
 - Microsoft Windows
 - accessing Event Viewer in, 206–207
 - filtering event log data with Event Viewer in, 214–216
 - inspecting event logs with Event Viewer in, 210–213

- installing DART CD with, 356–357
 - removing unused components of, 52–53
 - troubleshooting with, 206
- Microsoft Windows 2003 Server, turning on security auditing in, 122–124
- Microsoft Windows Access Control Mechanisms
- customizing security templates for networks with, 135–139
 - editing policies and configuring security with, 126–127
 - overview, 126
 - testing system against security templates with, 127–135
- Microsoft Windows Backup Utility, preparing recovery discs with, 147
- Microsoft Windows Disk Cleanup Utility
- cleaning hard drive with, 51–52
 - removing unused Windows components/installed programs/system restore points with, 52–53
- Microsoft Windows Update
- implementing, 107–109
 - overview, 106–107
 - preparing for, 107
 - resources on, 112–113
- Microsoft Windows XP
- firewall, 93–95
 - installing, 331–332
- Microsoft Windows XP Backup Utility
- backing up files with, 44–46
 - installing, 44
- Microsoft Windows XP Pro, turning on security auditing in, 123–124
- Microsoft WinPE Strider GhostBuster, 274
- Microsoft WinPE (Windows Preinstallation Environment), booting to, 235–236
- Microsoft's Security Monitoring and Attack Detection Planning Guide Web site, 120
- MMC (Microsoft Management Console)
- comparing current security system and template with, 128–130
 - customizing security templates for networks with, 136–137
- MonitorWare, investigating event logs with, 219–222
- Mozilla Firefox
- advantages of surfing with, 80–81
 - securing, 76–77
- MSCONFIG, editing startup list with, 48–49
- MSRT (Microsoft Malicious Software Removal Tool), scanning for rootkits with, 261–262, 338
- MyFip rootkit, 342–343
- N •
- native API hooking, 169
- Netbus 1.60
- disinfecting with Telnet, 298–299
 - disinfecting with Visual Basic program, 299–300
 - tracing with Port Explorer, 293–298
- Netstat, using for port-to-process mapping, 187–188
- Network Address Translation (NAT), with hardware routers, 87
- network-address translation (NAT) capability, routers with, 192
- networks
- cleaning of rootkits, 233
 - customizing security templates for, 135–139
 - disabling connections before cleaning rootkits, 319–320
 - monitoring for rootkits, 179–180
 - obtaining updates for, 110–112
 - options for dealing with infections on, 303–304
 - protecting ports of, 183–191
 - rebooting in disinfecting versus reinstalling operating system on, 306
 - using limited-access accounts on, 141–142
 - watching logs for rootkits clues, 180–183
- New York State, litigation against adware companies by, 309
- NIDS (Network Intrusion-Detection System) log, monitoring for rootkits clues, 182
- NOD32 Antivirus, using, BC5
- Norton Ghost, creating hard drive image with, 315–316
- NTFSShider, 339
- NTI Backup NOW!, using, BC15

• 0 •

- object access, auditing, 125
- online contacts, choosing carefully, 62
- Opera, securing, 76–77
- operating systems (OS)
 - choosing to reinstall, 305–307
 - importance of securing, 30
 - obsolete, unsupported, 103
 - preparing for reinstallation of, 328–329
 - rootkits evading reinstallation of, 325–327
 - rootkits hiding in, 151–153
 - rootkits infecting, 234–235

• p •

- packets, controlling data flow with, 199–200
- packet-sniffers, rootkits enabling, 23–24
- page fault, 346
- page-fault handler, 346
- parental control programs, versus spyware, 14
- Password Safe, using, BC20–BC21
- passwords
 - creating and storing, 29, 69–70
 - creating free e-mail accounts, 66
 - hackers deciphering weak, 17
 - recommend protectors and generators for, BC18–BC21
- patches
 - automatic Microsoft, 105–106
 - finding Microsoft, 105
 - Microsoft offering, 103–104
 - reasons for, 104
 - staying current with, 29
 - understanding, 102
- patching, miscellaneous software, 113–115
- peer-to-peer (P2P)
 - file sharing programs, spyware attached to, 15
 - networks, downloading from, 65
- persistent rootkits, detecting, 246–247
- personal information
 - hackers obtaining, 17
 - keyloggers collecting, 24

- pe386, 344
- phish, 343
- physical access
 - importance of limiting/controlling, 142
 - limiting/controlling, 140
- physical security, creating plan for, 143–144
- pings, sending out, 88
- plans, creating physical security, 143–144
- platforms, rootkits specific to, 21
- Pocket KillBox, using, BC17–BC18
- policy changes, auditing, 125
- pornography
 - avoiding, 64
 - drive-by downloads from, 15
- port blocking, with hardware routers, 87–89
- Port Explorer (Diamond CS)
 - sniffing capabilities of, 202–205
 - tracing RATs with, 293–300
 - using for port-to-process mapping, 190–191
- port stealthing, with hardware routers, 87–89
- ports
 - checking with port-to-process mapping, 186–191
 - identifying process ID associated with identified, 195
 - identifying process through, 195
 - overview, 183–185
 - ways hackers use, 185–186
- port-to-process mapping
 - checking ports with, 186–187
 - tracking suspicious data flow, 191
 - using DarkSpy for, 190
 - using Netstat for, 187–188
 - using Port Explorer for, 190–191
 - using TCPView, 188–189, 189–190
- preview panes, disabling e-mail, 66
- Privacy Policies, guidelines for safe downloading with, 65
- process activity
 - evaluating with DarkSpy and GMER, 227–228
 - evaluating with IceSword, 227
 - evaluating with Process Explorer, 226–227
 - evaluating with Task Manager, 224–226

- Process Explorer
 - on DART CD, 360–361
 - detecting keyloggers with, 291–293
 - evaluating process activity with, 226–227
 - identifying processes loaded by
 - `svchost.exe` with PID 984, 196–197
 - using, BC10
 - using AntiHookExec with, 268–269
 - The Process Library, 199
 - process tracking, auditing, 125
 - processes
 - identifying, 195–197
 - mapping recipient IP address with
 - reverse DNS search, 198
 - researching databases of, 198
 - professionals, hiring to analyze evidence, 317–318
 - programs. *See* software
 - PspCidTable, FUTO rootkits altering, 175–176
 - P2P (peer-to-peer)
 - file sharing programs, spyware attached to, 15
 - networks, downloading from, 65
 - puppet masters, rootkits delivering, 22–23
- R •**
- RAIDE, scanning for rootkits with, 275–276, 345
 - random-access memory (RAM), dumping to USB flash drive, 312–314
 - RATs (remote-access trojans)
 - accessing through ports, 183
 - commandeering computers, 17–18
 - disinfecting with Telnet, 298–299
 - reinstalling operating system for, 306–307
 - tracing with Port Explorer, 293–298
 - using ports, 185
 - writing Visual Basic program to disinfect, 299–300
 - reboots, planning after system compromise, 320–322
 - recognition
 - overview, 30–31
 - of problems not from malware, 33
 - signs of malware, 31–32
 - recovery, planning for, 33–34
 - recovery discs, preparing, 147–148
 - Red Screen of Death (RSOD), 343
 - Registrar Registry Manager, using, BC18
 - Registry
 - analyzing with DarkSpy, 279–280
 - backing up, 42–43
 - cleaning, 57–58
 - editing with GMER, 288
 - recommended cleaners for, BC17–BC18
 - tracking forensic tool changes to, 313
 - Registry Editor, backing up Registry with, 42–43
 - Regmon (Sysinternals), tracking forensic tool changes with, 313
 - remote transfers, installing spyware by, 15
 - remote-access trojans (RATs)
 - accessing through ports, 183
 - commandeering computers, 17–18
 - disinfecting with Telnet, 298–299
 - reinstalling operating system for, 306–307
 - tracing with Port Explorer, 293–298
 - using ports, 185
 - writing Visual Basic program to disinfect, 299–300
 - resistance
 - becoming intelligent computer user for, 26–27
 - need for, 26
 - security measures recommended for, 27–30
 - resources
 - on developing kernel device drivers, 168
 - on hard drive operation, 326
 - lists of ports used by trojans, 186
 - for security devices, 143
 - for security software, 144
 - security Web sites, 348–354
 - for software updates/patches, 114
 - for virtual machine software, 145
 - restore point. *See also* System Restore
 - creating, 39
 - removing installed, 52–53
 - restoring from, 41
 - restoring
 - Registry, 43
 - system, 41

Restricted Groups policy, implementing, 141–142

Rootkit Revealer Forum, 250

Rootkit Revealer (RKR) (Sysinternals)
on DART CD, 361

help resources for, 250–251

interpreting scan results of, 249–250

overview, 247–248

running with BlackLight, 246

understanding operation of, 248–249

user-friendliness of, 245

using, BC10–BC11

rootkit scanners. *See also specific scanners*

function of, 232–233

overview, 231–232

running after format and reinstall, 333

types of, 244–246

using from external storage devices,
235–238

using in Safe mode, 238–239

rootkits

cloaked verses on cloaked, 232

evading security systems, 21–22

history of, 19–20

invisible functions of, 151–153

kernel-mode versus user-mode, 155–156

overview, 19

planning defense against, 145–146

possible actions against creators of,
308–310

reasons for existence, 22–24

steps for removing, 233

types of, 154

Rootkits: Subverting the Windows Kernel
(Hogland, Butler), 177

Rootkitty, scanning for rootkits with,
274–275

routers, blocking tools with, 192–193

RSOD (Red Screen of Death), 343

rule-based firewalls, 91. *See also* software
firewalls

Russonovich, Mark (Sysinternals), 20, 352

RxTx, measuring bandwidth use with,
223–224



SA (SiteAdvisor) (McAfee, Inc.), 81–82, 198

Safe mode

booting into with System Configuration
Utility, 229

defragmenting in, 55–56

rootkits scanning and, 238–239

running system restore from, 41–42

using GMER in, 287–288

Safer-Networking Web site, 243

sandbox, defined, BC16

Sandboxie

on DART CD, 360

using, BC16

SANS Institute, listing ports used by
trojans, 186

saving, before reboots, 320

scam operations, hackers using systems
for, 17–18

scanners. *See also* rootkit scanners;
specific scanners

anti-spyware, 97

anti-trojan, 98–99

antivirus, 98

on DART CD, 358–359

importance of having, 82

importance of using, 28

most useful features of, 99–100

overview, 95–96

type of, 96–97

using before Internet downloads, BC2

Scott, Charlie (*Snort For Dummies*), 182

screen savers, defragmenting with, 56

security

configuring, 126–127

configuring selectively, 134–135

creating plan for physical security,
143–144

guidelines for improving, 118–119

importance of taking physical
measures, 142

security auditing

events, categories available for auditing,
124–126

turning on, 122–124

- Security Configuration Manager, editing
 - policies and configuring security with, 126–127
- security devices, protecting equipment with, 143
- security forums
 - asking help from, 234
 - helping with Rootkit Revealer, 250–251
- Security log (Windows), function of, 206
- security logs, configuring and enabling, 28
- security permissions, checking for
 - alteration of, 240
- security policies
 - editing, 126–127
 - setting up, 28
- security settings
 - comparing with security template, 128–130
 - copying from template to template, 137
 - creating database of, 131–133
- security systems, rootkits evading, 21–22
- security templates
 - customizing for networks, 135–139
 - testing system against, 127–135
- Self Monitoring And Reporting Technology (S.M.A.R.T.), helping rootkits hide, 326
- service installations/starts, evaluating for rootkits, 214
- security-analysis utility, making own, 127
- Shadow Walker, 345–346
- shareware, versus freeware, 357–358
- SIG² (API HookCheck), 164
- Sigcheck, verifying system file integrity with, 243
- Silberman, Peter (FUTo developer), 175
- Simovits, listing ports used by trojans, 186
- SiteAdvisor (SA) (McAfee, Inc.), 81–82, 198
- 16-bit architectures, 105
- 64-bit architectures
 - GMER working with, 289
 - understanding, 105
- size, changing event logs default, 207–208
- S.M.A.R.T. (Self Monitoring And Reporting Technology), helping rootkits hide, 326
- sniffer logs, monitoring for rootkits clues, 181–182
- sniffers
 - catching hackers with, 200–201
 - detecting, 201–202
 - Ethereal, 205
 - function of, 24
 - hackers using, 200
 - Port Explorer, 202–205
- Snort For Dummies* (Scott, Wolfe and Hayes), 182
- Snort, monitoring NIDS with, 182
- software. *See also specific software*
 - anti-spyware, 97
 - anti-trojan, 98–99
 - antivirus, 98
 - backup and imaging, BC14–BC16
 - blocking illegal computer use with, 144
 - for detecting/removing rootkits, BC7–BC12
 - editing startup configurations, 48–50
 - false security alerts encouraging
 - purchase of, 17
 - filtering by specific, 214–216
 - hard-drive erase and repair utilities, BC21–BC24
 - recommended anti-malware scanners and utilities, BC2–BC7
 - recommended password protectors and generators, BC18–BC21
 - recommended system and Registry cleaners, BC17–BC18
 - removing installed, 52–53
 - removing unused, 50–51
 - running to many at startup, 47
 - updating/patching miscellaneous, 113–115
 - virtual machine, 144–145
- software firewalls
 - functioning of, 91–92
 - knowing system needs, 95
 - overview, 90–91
 - setting rules for, 92–93
 - Windows XP, 93–95
- SONY Digital Rights Management (DRM)
 - rootkit, discovery of, 20
- spam e-mail, rootkits facilitating, 23
- SPI (Stateful Packet Inspection) component, with hardware firewalls, 89–90

- spies, rootkits acting as, 23–24
- SpinRite (Gibson Research Corporation)
 - described, 327
 - using, BC23–BC24
- Spitzer, Elliott (New York State Attorney General), 309
- spoofed Web sites, drive-by downloads from, 15
- Spybot-Search&Destroy
 - on DART CD, 359
 - inserting Hosts list into HOSTS file, 72–73
 - using, BC6
- spyware
 - understanding, 13–14
 - ways of installing, 14–16
- SpywareInfo Web site, 352–353
- SpywareWarrior Security Web site
 - overview, 353
 - resource on cyber-cor-pirates, 18
- SSDT (System Service Descriptor Table)
 - hooking, 168–169
 - replacing, 170–171
- SSV (System Virginty Verifier), scanning for rootkits with, 270–273
- startup
 - editing list using MSCONFIG, 48–49
 - running too many applications at, 47
- Stateful Packet Inspection (SPI)
 - component, with hardware firewalls, 89–90
- static DLLs, rootkits targeting, 160
- stop errors, evaluating for rootkits
 - activity, 214
- strategies, recommended for rootkit detection and removal, 234
- SubVirt rootkit, 177–178
- Sunbelt Kerio Personal Firewall, on DART CD, 358
- survivable systems, defined, 25
- svchost.exe
 - identifying process started by, 195–196
 - identifying processes loaded by, 196–197
- Symantec, list of top 19 threats from, 245
- symptoms, of malware presence, 31–32
- SYSENTER hooking, 170, 344
- Sysinternals
 - Autoruns, 49–50, 246–247, 265–268, 360, BC8–BC9
 - Filemon, 197, 312
 - PageDefrag, 57
 - Regmon, 313
 - Rootkit Revealer, 245–251, 361, BC10–BC11
 - TCPView, BC11–BC12
- Sysinternals Forum, 352
- system calls, user-mode rootkits using, 155
- system cleaners, recommended, BC17–BC18
- System Configuration Utility, booting into
 - Safe mode with, 229
- system events, auditing, 125
- system files
 - checking for replacement of, 240
 - verifying integrity of, 243–244
 - verifying with FileAlyzer, 240–243
- System log (Windows), function of, 206
- system monitoring, enabling in GMER, 286–287
- system requirements
 - Acronis True Image, 359
 - Advanced Password Generator, 362
 - Agnitum Outpost Firewall, 358
 - Any Password, 362
 - Autoruns, 360
 - BartPE CD, 237
 - checking downloads for, 109
 - DarkSpy, 361
 - DART, 355–356
 - GMER, 361
 - Karen’s Replicator, 360
 - LinkScanner Pro 2.0, 359
 - Process Explorer, 360
 - Rootkit Revealer, 361
 - Sandboxie, 360
 - Spybot-Search&Destroy, 359
 - Sunbelt Kerio Personal Firewall, 358
 - troubleshooting problems with, 363
 - UnHackMe, 361
 - Virtual PC, 145
 - Workstation, 145
- system resources, malware using, 222–223

System Restore
 accessing, 39
 changing drive settings of, 39–40
 clearing out/shutting off, 40–41
 creating restore point, 39
 disabling, 325
 restoring from restore point with, 41
 running from Safe mode, 41–42
 understanding, 38
 working with after system compromise, 323–324

System Service Descriptor Table (SSDT)
 hooking, 168–169
 replacing, 170–171

system service, filtering by, 214–216

system tracing, enabling in GMER, 286–287

System Virginty Verifier (SSV), scanning
 for rootkits with, 270–273

system-analysis software, on DART CD, 360

• T •

Task Manager
 evaluating process activity with, 224–226
 monitoring computer activities with, 223–224
 monitoring CPU cycles with, 228–229

TCPView (Sysinternals), using, BC11–BC12

TCPView, using for port-to-process
 mapping, 188–189

Tech Support Guy Forum, 353–354

32-bit architectures, 105

thread injection, functioning of, 165

Tom Coyote Security Forum, 354

toolbars, adware, 13–14

tools. *See* utilities

training, security awareness, 144

Tripwire, verifying system file integrity
 with, 243

trojanized utilities, replacing system files,
 174–175

trojans. *See also* remote-access trojans
 (RATs)
 effects of, 63
 overview, 11
 using Applnit_DLLs injection, 165
 using ports, 185–186

Trusted zone (Internet Explorer), adding
 Web sites to, 76

Turner, Suzi (SpywareWarrior Web site
 owner), 353

• U •

Ultimate Boot CD For Windows
 (UBCD4Win), booting to, 237–238

uncloaked rootkits, defined, 232

UnHackMe (Greatis)
 on DART CD, 361
 scanning for rootkits with, 260–261
 user-friendliness of, 245
 using, BC12

University of Connecticut (UCONN),
 housing rootkit, 154

unpatched computers, worms effect on,
 11–12

unprivileged hooks, overview, 159

updates. *See also* Microsoft Update;
 Microsoft Windows Update
 automatic Microsoft, 105–106
 finding Microsoft, 105
 importance of, 103
 Microsoft offering, 103–104
 miscellaneous software, 113–115
 for networks and hardware, 110–112
 reasons for, 104
 staying current with, 29
 understanding, 102

USB flash drive, dumping RAM to, 312–314

user accounts
 establishing limited-access, 70–71
 safe surfing with limited-access, 64
 using limited-access, 27
 using limited-access on networks, 141
 value of limited-access, 141

user DLLs, rootkits targeting, 161–163

user-friendliness, of rootkits actors, 245

user-level rootkits, types of hooks
 used, 159

user-mode rootkits
 versus kernel-mode rootkits, 155–156
 summary of, 154

users, filtering event by, 214–216

utilities. *See also specific utilities*
 anti-malware on DART CD, 358–359
 to detect sniffers, 202–205
 hard-drive erase and repair, BC21–BC24
 recommended anti-malware, BC2–BC7
 trojanized replacing system files, 174–175
 for verifying system file integrity, 240–244

• U •

VICE (Virtual Intruder Capture Engine),
 scanning for rootkits with, 269–270
 video-card EEPROM, rootkits residing
 in, 324
 virtual machine (VM) software, 144–145
 virtual memory manager (VMM), hooking,
 176, 345
 virtual operating systems, fooling rootkits
 with, 144–145
 virtual-machine-based rootkits (VMBR),
 function of, 177–178
 Virus Total, checking for file legitimacy
 with, 257
 viruses
 finding, 304–305
 overview, 11
 Visual Basic programs, writing to disinfect
 Netbus, 299–300
 VM (virtual machine) software, 144–145
 VMware Workstation, 145
 vulnerability, to malware, 10

• W •

Web sites
 adding to Trusted zone, 76
 for bootable CDs, 236–238
 for checking for legitimacy of files, 257
 drive-by downloads from spoofed, 15
 evaluating safety of, 81–82
 on hard drive operation, 326

for Linux boot CDs, 316
 for maintaining list of native API
 entries, 169
 for process databases, 198
 resources for phishing, 343
 resources for security auditing, 120
 resources for security devices, 143
 resources for security software, 144
 resources for software updates/
 patches, 114
 resources for virtual machine
 software, 145
 resources listing ports used by
 trojans, 186
 resources on developing kernel device
 drivers, 168
 Safer-Networking, 243
 security, 338, 348–354
 Web surfing
 advantages of using Firefox for, 80–81
 guidelines for safe, 63–64
 importance of practicing safe, 30
 malware controlling, 16–17
 malware tracking, 16
 rootkits tracking, 24
 whoami .exe tool, tracking user access
 with, 141
 Windows File Protection (WFP), protecting
 DLLs, 160
 WinTasks Process Library, 199
 Win32/Hackdoor.B rootkit, using ports, 185
 WMF (Windows Metafile) exploit, installing
 spyware by, 15–16
 Wolfe, Paul (*Snort For Dummies*), 182
 worms, overview, 11

• Z •

zombies, for DDoS, 18
 ZoneAlarm Pro Firewall, using, BC6–BC7

