

Index

Note to the Reader: Throughout this index boldfaced page numbers indicate primary discussions of a topic. Italicized page numbers indicate illustrations.

A

- abnormal shutdown, 421
- access
 - Internet, **320–324**, 322–323
 - object, **401–410**, 403–406
- Access Control dialog box, 354
- access control lists (ACLs), 35
- Access Denied error, 416
- Access Point (Infrastructure) Networks
 - Only option, 299
- access point security, **291–296**, 291–295
- Account Is Disabled option, 222, 224
- Account Is Locked Out For setting, 230
- Account Lockout Duration setting, 230
- Account Lockout Policy, **230–231**, 230–231
- Account Lockout Thresholds
 - setting, 230
- accounts
 - Administrator. *See* Administrator accounts
 - Administrator accounts
 - logon events for, **237–238**, 237–238
 - for services, **30–32**, 31–32
 - user. *See* users and user accounts
- ACLs (access control lists), 35
- Active Directory (AD), 239
- Active Directory Users And Computers (ADUC)
 - audit policy, 233
 - decoy domain administrator
 - accounts, 243–244
 - default users, 240
 - Deny groups, 248
 - external storage devices, 89, 89
 - GPOs, 225–226, 225–226, 402
 - operating system patching, 61, 61
 - organizational units, 256
 - resource servers, 405
 - security templates, 72
 - service lockdown, 33
 - user account templates, 221, 224
 - users and groups, 195, 412
 - VPN server dial-in privileges, 264
- AD-Aware program, **120–122**, 120–122
- Add A Port dialog box, 42, 42
- Add Data Recovery Agent Wizard,
 - 148–149, 149
- Add Digital Signature To This Message
 - option, 347
- Add IP Filter dialog box, 287–288, 287
- Add/Remove Templates option, 91
- Add Standalone Snap-in dialog box,
 - 65–66, 66
- Additional System Information
 - option, 381
- Additional Tasks screen, 433
- Address Resolution Protocol (ARP)
 - poisoning, **133–140**, 135–140
- addresses
 - IP
 - intrusion protection systems,
 - 482, 482
 - IPSec VPN, 304–306, 306, 308–309, 309
 - for packet filters, 286–287
 - SFTP, 356
 - tracking, 390–393, 391–393
- MAC
 - finding, 296
 - with switches, 429
 - in wireless security, **294–296**

- AdminEFSdra.cer file, 149
- AdminEFSdra.pfx file, 150
- Administration Tools Setup Wizard, 466
- administrative activities by
 - nonadministrator users, 281–283, 281–283
- Administrator accounts
 - decoy, 243–244, 243–244
 - disabling, 242
 - DSRM passwords, 245–246
 - renaming, 241
 - for services, 31–32, 31
 - for VPN server dial-in privileges, 264–265
- Administrator Properties dialog box, 244
- Adminpak.msi file, 466, 468
- ADUC. *See* Active Directory Users And Computers (ADUC)
- Advanced dialog box, 299, 299
- Advanced Attributes dialog box
 - encrypting data, 152, 152, 156
 - recovering data, 160–161
- Advanced Backup Options dialog box, 184, 184
- Advanced Encryption Standard (AES)
 - BitLocker, 205
 - IPSec. *See* IPSec (Internet Protocol Security) VPNs
- Advanced Privacy Settings dialog box, 329
- Advanced Security Settings For dialog box, 408, 408, 410
- Advanced Sharing dialog box, 302–303, 303
- Advanced tab
 - digital certificates, 352, 352
 - minidumps, 422, 422
 - spam, 342, 343
 - Windows Firewall, 43, 43
- adware, 118–123, 120–122
- AES (Advanced Encryption Standard)
 - BitLocker, 205
 - IPSec. *See* IPSec (Internet Protocol Security) VPNs
- AGDLP chain, 195
 - content for, 198–204, 198–204
 - for Deny group, 247–251, 248–251
 - users and groups for, 195–198, 196–198
- ALE (Annual Loss Expectancy)
 - calculating, 6–7
 - formula, 3
- allocation units, 472
- Allow Access option, 265
- Allow BitLocker Without a Compatible TPM option, 211
- Allow Change permission, 204
- Allow Inheritable Permissions option, 202
- Allow Service To Interact With Desktop option, 32
- Allow Users To Connect Remotely To This Computer option, 272
- Allow Write Permission option, 201
- Always Start In Wizard Mode option, 182
- Analyze Computer Now option, 68
- Annual Loss Expectancy (ALE)
 - calculating, 6–7
 - formula, 3
- Annual Rate of Occurrence (ARO)
 - calculating, 5–6
 - formula, 3
- antivirus software, 106–107
 - downloading and installing, 107–109, 108–109
 - scanning with, 110–111, 110–111
 - testing, 112
 - updating, 109–110, 110
- ARP (Address Resolution Protocol)
 - poisoning, 133–140, 135–140

- assessments, security
 - HFNetChk for, 382–385
 - Microsoft Baseline Security Analyzer for, 379–382, 380–382
 - risk, 2–3
 - Threat Analysis Index, 122
 - asset classification and control, 11
 - Assign Letter Drive Or Path screen, 178
 - Association tab, 297, 298
 - attributes, auditing, 409–410
 - Audio tab, 363
 - Audit Account Logon Events option, 232, 234
 - Audit Logon Events option, 232
 - audit logs
 - monitoring, 232
 - reviewing, 411–420, 413–419
 - Audit Object Access option, 403
 - Audit Policy
 - for object access, 401–410, 403–406
 - for security templates, 69, 73
 - setting, 233–234, 233–234
 - triggering, 415–416, 416
 - Audit Process Tracking Policy option, 70
 - Audit tab, 377, 377
 - auditing
 - attributes for, 409–410
 - logons, 231–238, 233–238
 - in Retina, 377, 377
 - Auditing Entry For dialog box, 409–410
 - Auditing tab, 408, 408
 - Authenticated Users from the resulting Name (FQDN) list, 408
 - authentication
 - IPSec VPN, 305
 - RDP, 275–276
 - VPN, 254–255, 260
 - Auto Download And Schedule The Install option, 63
 - Autoexec.bat file, 82, 82
 - Autoexec.nt file, 81–82
 - automated operating system patching
 - in Domain mode, 54–64, 55–63
 - in Workgroup mode, 53–54, 54
 - Automatic Picture Download Settings dialog box, 338, 338
 - Automatic (Recommended) option, 54
 - Automatic service startup type, 29–30
 - Automatic Updates tab, 54
 - Automatically Connect To Non-Preferred Networks option, 299
 - Automatically Restart option, 423
 - autorun.ini script, 84
 - Autorun security, 74–75
 - Autoexec.nt and Config.nt for, 81–82, 82
 - CD-ROM function disabling, 85–87, 86
 - Registry for, 79–82, 79–80
 - scripts for, 82–83, 83
 - Startup folder for, 81, 81
 - System Configuration Utility for, 75–79, 76–78
 - Autoruns tool, 74
 - availability, 454
 - avast! antivirus tool
 - downloading and installing, 107–109, 108–109
 - scanning with, 110–111, 110–111
 - testing, 112
 - updating, 109–110, 110
-
- B**
- background, desktop, 460
 - Backup dialog box, 184
 - Backup Job Information dialog box, 184–186, 184
 - Backup Or Restore Wizard, 182
 - Backup Progress dialog box, 185, 185
 - Backup tab, 182–183, 183
 - Backup Utility, 183, 183

Backup Utility Advanced Mode screen, 182

backups, **180–181**
 catalog for, **181–183, 182–183**
 digital certificates, **348–353, 349–352**
 for file system conversions, 166
 initializing, **183–185, 183–185**
 for memory dumps, 421
 for Registry edits, 424
 restoring, **188–193, 190–193**
 scheduled, **186–188, 186–188**

banners, grabbing, 396

behavior-based IDS analytic engines, 476

binary rootkits, 112

BitLocker drive encryption, 142, 204–207
 implementing, **216–217, 216–217**
 partitions, **207–210, 207–209**
 USB keys and recovery password keys, **212–215, 212–215**
 USB thumb drives, **210–212, 210–212**

block rules in intrusion protection systems, 475

Blocked Encodings List, 339

Blocked Senders List, 339

Blocked Top-Level Domains List, 339, 341–342, 342

blocking cookies, **328–330, 329**

blue screen information, 425, 425

Bogus OU Properties dialog box, 94

BOOT.INI tab, 77, 77

booting
 “Known Good” configurations, **461–462**
 Safe Mode, **455–459, 456–458**

bouncing services, 281

Brazil, spam from, 342

browser headers, **389**

buffer size in packet capturing, 435

bugs, patches for. *See* operating system patching

business continuity planning, 10

C

Cain & Abel, **133–140, 135–140**

Capture dialog box, 436

Capture Interfaces dialog box, 434

Capture Options dialog box, 435

captured data viewing in IPsec VPN, **304–307, 304–307**

capturing packets, Wireshark packet analyzer for, **428–431**
 downloading, **431, 431**
 installing, **431–434, 432–434**
 network analysis with, **436–438, 437**
 packet capturing with, **434–436, 434–436**

catalogs for backups, **181–183, 182–183**

CBC (Cipher Block Chaining), 205

CCDU tab, 135

CD-ROM AutoRun function disabling, **85–87, 86**

Certificate dialog box, 346–347, 346

Certificate Export Wizard, 350, 350

Certificate Import Wizard, 150, 351, 351

certificates
 backups, **348–353, 349–352**
 installing, **344–347, 345–346**

Certificates dialog box, 349

Change Advanced Settings option, 297

Change Approval option, 60

Change Automatic Download Settings option, 337

Change Scope dialog box, 42, 42

Change Security Settings dialog box, **345–346, 345**

Check For Problems option, 125

Check For Publisher’s Certificate Revocation option, 352

Check For Server Certificate Revocation option, 352

CheckDisk scans, 471–472

China, spam from, 342

chkdsk utility, 471

- Choose A Wireless Network dialog box, 297
- Choose Components screen, 432, 432
- Choose Installation Location screen, 433
- Cipher Block Chaining (CBC), 205
- Cipher.exe, 470–471, 474, 474
- classification of information, 20–22
- Client For Microsoft Networks option, 332
- Client Respond IPsec Policy GPO, 259
- Client (Respond Only) option, 259
- clients
 - ICS, 333–334, 334
 - RDP, 273–276, 273–277
 - SFTP, 356–357, 356–357
 - VPN, 266–270, 267–270
 - wireless security, 296–300, 297–299
- Clients DLG Properties dialog box, 200, 200
- Clients GG Properties dialog box, 199
- ClipBook service, 30–32, 31–32
- clusters, 472
- Cohen, Fred, 106
- command-line Run As, 283–284
- commercial classification of information, 21–22
- Common Vulnerabilities and Exposures (CVE) list, 373
- Comodo certificates, 345
- company overviews, 9–10
- comparing hashes, 360, 360
- Compatws security template, 67
- Complete Memory Dump option, 423
- Completing The New Connection Wizard screen, 268
- compliance, policy development for, 10
- computer and network management, policy development for, 11
- Computer Management console
 - disk initialization, 176, 176
 - FAT partitions, 166
 - non-administrator users, 280
 - Safe mode, 457
 - service management, 27–28, 27
 - user accounts, 158–159, 159
- Computer setting for RDP, 276
- confidential classification, 21–22
- Confidential Clients Properties dialog box, 259
- Confidential Servers Properties dialog box, 405
- confidentiality, 454
- Config.nt file, 81–82
- Config.sys file, 82
- Configure And Enable Routing And Remote Access option, 262
- Configure Automatic Updates option, 63
- Configure Computer Now option, 68
- Configure Device dialog box, 264, 264
- Confirm Restore dialog box, 191–192, 191
- Confirm Setting Change warning option, 405
- confirming
 - NTFS partitions, 173–174, 173
 - System Restore, 464
- Connect To The Network At My Workplace option, 267
- Connect VPN dialog box, 268–269
- Connect When This Network Is In Range option, 298
- Connection Availability screen, 268, 268
- Connection Name screen, 268
- Connection Security Rules option, 308, 308
- connections
 - RDP, 277
 - VPN, 267–270, 267–270
 - wireless networks, 298–299, 298
- Connections tab, 298, 298, 322
- connectivity, IPsec VPN, 304–307, 304–307
- Console Root window, 27

Content tab, 349, 349, 352
 Control Panel Setup: Enable Advanced Startup Options dialog box, 211, 211
 conversions
 to dynamic disks, 175–177, 176–177
 FAT to NTFS, 165–174, 167–173
 Convert utility, 165, 172–173, 172
 cookies, 328–330, 329
 CoolWebSearch spyware, 123
 Copy Items dialog box, 451–452
 counterattacks, 475
 Cracker tab, 135
 CrashOnCtrlScroll entry, 424–425, 425
 Create a Restore Point screen, 465, 465
 Create This Connection For setting, 268
 Critical Objects tab, 122
 Custom Configuration dialog box, 262, 262
 custom security templates, 67–71, 67–71
 Customize Data Protection Settings dialog box, 313, 313
 Customize IPsec Settings dialog box, 312, 313, 315, 315
 CVE (Common Vulnerabilities and Exposures) list, 373

D

DACL (Discretionary Access Control List), 414
 daily backups, 186–188, 186–188
 Data Encryption Standard (DES), 255, 260
 Data Recovery Agent (DRA), 143
 creating, 147–150, 147–150
 for recovering data, 157–161, 159–160
 Database tab, 363

databases
 LAD, 239
 Link Logger, 363
 SAM, 161–162
 DCPromo, 239
 De-Authentication frames, 475
 Decoders tab, 135
 decoy domain administrators, 243–244, 243–244
 Default Domain Controllers Policy
 Audit Policy in, 233–234, 233–234
 Security Event Log in, 236–237, 236–237
 security logging in, 236–237, 236
 Default Domain Policy
 Account Lockout Policy in, 230–231, 230–231
 for default users, 240–242, 241–242
 password policies in, 228–229, 228–229
 Default Security Setting For This Secure Message Format option, 345
 default security templates, 65–67, 66
 default users, 239–240
 decoy domain administrator account, 243–244, 243–244
 Default Domain Policy for, 240–242, 241–242
 DSRM administrator passwords, 245–246
 Define These Policy Settings option, 403–404
 Define These Policy Settings to Success and Failure option, 234
 Define This Policy Setting field, 241–242
 Define This Policy Setting option, 35
 deleted data, sanitizing, 470–475, 472–474
 deleting user accounts, 159
 denial of service (DoS) attacks, 5
 Deny All AGDLP, 247–251, 248–252

- Deny All GG Properties dialog box, 250–251, 250
- Deny All permission, 252
- Deny Full Control permission, 252
- Deny groups, 247–252, 248–252
- dependencies between services, 28–29, 28
- Dependencies tab, 28–29
- deploying IPSec, 255–259, 258
- DES (Data Encryption Standard), 255, 260
- Description field for Security log, 418
- desktop, 460
- Desktop Application Scan option, 381
- Desktop Properties dialog box, 460–461, 461
- destination computer shares, 302–304, 302–304
- Destination option for packet filters, 287
- Device Manager, 282–283
- dial-in for VPN servers, 264–265, 264–265
- Dial-in tab, 265, 265
- digital certificates
 - backups, 348–353, 349–352
 - installing, 344–347, 345–346
- Digital Subscriber Line (DSL), 331
- Directory Services Restore Mode (DSRM), 239
- Disable USB Settings option, 94
- Disabled service startup type, 29
- disabling
 - Administrator account, 242
 - CD-ROM AutoRun function, 85–87, 86
 - daily backups, 187–188, 188
 - external storage devices, 87–94, 89–94
 - services, 28–30, 29
- discarding media, 470–475, 472–474
- Discovery tab, 376, 376
- Discretionary Access Control List (DACL), 414
- Disk Drives option for RDP, 274
- Disk Management
 - FAT partitions, 166
 - volumes, 180
- diskpart command, 208–209, 208–209
- disks
 - FAT to NTFS conversions, 165–174, 167–173
 - initializing, 175–177, 176–177
- Display Adapter Properties dialog box, 282–283
- Display tab, 273, 273
- displaying file extensions, 336–337, 336
- DLG (Domain Local Group)
 - global security groups in, 223–224
 - permissions, 247
- DNS (Domain Name System), 38, 334
- Do Not Overwrite Events option, 235, 405
- Do Not Store Updates Locally; Clients Install From Microsoft option, 58
- documents, value of, 19–22
- domain administrator accounts, 243–244, 243–244
- Domain Controllers Properties dialog box, 237
- Domain Local Group (DLG)
 - global security groups in, 223–224
 - permissions, 247
- Domain mode, automated operating system patching in, 54–64, 55–63
- Domain Name System (DNS), 38, 334
- Domain setting
 - IPSec VPN firewalls, 310
 - RDP, 276
- Donations option, 125
- Don't Download Pictures option, 338
- Don't Search. I Will Choose The Driver To Install option, 458
- DoS (denial of service) attacks, 5

Download Updates For Me, But Let Me Choose When To Install Them option, 54

downloads

- avast!, 107–109, 108–109
- e-mail, 338, 338
- validating, 357–360, 360
- Wireshark, 431, 431

DRA (Data Recovery Agent), 143

- creating, 147–150, 147–150
- for recovering data, 157–161, 159–160

Drive Properties dialog box, 442–443, 445–446

Driver tab, 282–283, 282

drivers, 282–283, 282, 456

Drop All Packets Except Those That Meet The Criteria Below option, 288

DShield tool, 364–365, 391–393, 391–393

DSL (Digital Subscriber Line), 331

DSRM (Directory Services Restore Mode), 239

DSRM administrator passwords, 245–246

dumps, memory, 420–428, 422–427

dynamic disks, conversion to, 175–177, 176–177

E

e-mail, 334–335

- digital certificates
 - backups, 348–353, 349–352
 - installing, 344–347, 345–346
- encryption, 347
- file extensions for, 336–337, 336
- graphics in, 337–338, 337–338
- Link Logger, 363
- security zones for, 338–339, 338
- spam, 339–343, 341–343

Edit A Service dialog box, 42

Edit DWORD Value dialog box, 424–425, 425

education in user awareness programs, 12–16

EF (exposure factor), 4

EFS. *See* Encrypting File System (EFS)

EICER (European Institute of Computer Antivirus Research), 112

802.11 wireless security, 289–291

- access points, 291–296, 291–295
- clients, 296–300, 297–299

Elephant Diffuser function, 205–206

Email tab, 363

Enable All But Dangerous Plugins With Default Settings option, 371

Enable Internet Connection Sharing For This Connection option, 333

Enable Strong Protection option, 350

Enable the Save My Password option, 276

Enabled (Scheduled Task Runs At Specified Time) option, 188

Encrypt Contents To Secure Data option, 152, 154

Encrypt The File Only option, 152, 154

Encrypting File System (EFS), 142–143

- content for
 - accessing, 153–154, 156–157
 - creating, 151–153, 151–153
 - recovering, 157–161, 159–160
 - sharing, 155–156, 155–156
- Data Recovery Agent policy for, 147–150, 147–150
- users for, 145–146, 146
- volume configuration for, 144–145, 144–145

encryption

- BitLocker. *See* BitLocker
- drive encryption
- e-mails, 347

- performance with, 266
 - SAM database, 161–162
 - in VPNs, 254, 260
 - Encryption Details dialog box, 156, 160–161
 - End Process Tree option, 486
 - End User License screen, 450
 - Enforce Password History option, 229
 - erasing media, 470–475, 472–474
 - Error option for Security log, 417, 419
 - Error Report Contents dialog box, 427
 - Error Signature dialog box, 427
 - escalation of privilege, 25
 - estimating potential loss, 4–5
 - European Institute of Computer Antivirus Research (EICER), 112
 - Event IDs, 417
 - Event Log option, 403
 - event logs
 - monitoring, 237–238, 237–238, 416–419, 416–419
 - settings, 404–405, 404–405
 - Event Properties dialog box, 418–419
 - Event Viewer, 237–238, 237, 416–419, 416–419
 - exceptions for Windows Firewall, 41, 41
 - Exceptions tab, 41, 41
 - Experience tab, 274, 275
 - exploit software, 420
 - Explore All Users option, 81
 - Export Template option, 71
 - exposure factor (EF), 4
 - extensions, displaying, 336–337, 336
 - external storage devices, disabling, 87–94, 89–94
-
- F**
- Failed option, 409
 - Failure Audit option, 417, 419
 - Failure option, 403
 - failures, triggering on, 415–416, 416
 - fault tolerance, 174–180, 176–180
 - File Allocation Table (FAT) filesystem
 - converting to NTFS, 165–174, 167–173
 - EFS support for, 144
 - File And Print Sharing For Microsoft Networks option, 332
 - File And Printer Sharing service, 38, 41, 193–194
 - File Download - Security Warning Dialog screen, 431, 431
 - files
 - exchanging, 353–357, 354–357
 - extensions, 336–337, 336
 - Filter tab, 418–419
 - filters
 - MAC addresses, 294–296
 - packet, 284–289, 286–288, 435
 - security logs, 238, 418–419
 - spam, 342–343, 343
 - firewalls
 - configuring, 40–44, 40–43
 - IPSec VPN, 310–312, 310–312
 - packet filters in, 284
 - first-party cookies, 329
 - Fix Selected Problems option, 126
 - Folder Options dialog box, 336, 336
 - Folder Selection option, 110
 - Font Download option, 339
 - forcing memory dumps, 420–428, 422–427
 - Format Partition screen, 170, 170
 - Format Volume screen, 179
 - free space, determining, 471–474, 472–474
 - FTP, 353–357, 354–357
 - fully qualified domain names (FQDNs), 246

G

General tab

- EFS, 151, 160
- packet filters, 286, 286
- RDP, 276–277, 276
- services, 29
- System Configuration Utility, 76
- Windows Firewall, 40, 40

global security groups, 223–224

golden child applications, 95

government regulations, 19

Gramm-Leach-Bliley Act, 19

graphics, 337–338, 337–338

Group Or User Names field, 35

Group Policy Objects (GPOs)

- Client Respond IPSec Policy, 259
- external storage devices, 87–94, 89–94
- IPSec Secure Server Policy, 257–258
- object access, 402–405, 403–405
- refreshing, 406–407
- Secure Server IPSec Policy, 258
- security templates, 72–73
- service lockdown, 32–36, 33–35
- services, 26
- users, 225–226, 225–226

Group Policy tab, 90, 90, 402–403

groups

- AGDLP, 195–198, 196–198
- Deny, 247–252, 248–252

GuardianEdge Technologies utility, 142

Guest accounts, 239

Guidelines for Media Sanitation, 470

H

Hardened Servers.inf file, 73

hardening systems, 24

- Autorun security. *See*
Autorun security

hardware devices, 84–94, 86, 89–94
patches. *See* operating system

patching

port management, 38–48, 40–43,
46–47

security templates, 64–65

- custom, 67–71, 67–71

- default, 65–67, 66

- GPOs for, 72–73, 72–73

service management. *See* services

virtualization, 95–103, 97–102

hardware devices, 84–85

- CD-ROM AutoRun function,
85–87, 86

- external storage devices, 87–94,
89–94

hardware failures, threat analysis for, 5

Hardware tab, 281, 281

Hardware Update Wizard,
457–458, 458

hashes

- for download validation,
357–360, 360

- SHA, 255

Have Disk option, 458

headers, browser, 389

Health Insurance Portability and

- Accountability Act (HIPAA), 19–20

Hellix Live distribution, 96, 102

HFNetChk program, 382–385

Hide File Extensions For Known File
Types option, 337

HIDSs (host-based intrusion detection
systems), 475–486, 477–486

High Priority patches, 51

High setting

- Internet Explorer security, 325
- spam, 341

HIPAA (Health Insurance Portability
and Accountability Act), 19–20

Hiscews security template, 67

Hisecdc security template, 67

host-based intrusion detection systems (HIDSs), 475–486, 477–486
 hostile IP tracking, 390–393, 391–393
 Hosts tab, 135
 How To Correct The Problem
 option, 381

I

I Connect Through A Local Area Network (LAN) option, 323
 I Love You virus, 106, 335
 iAvs option, 110
 iAVS Update option, 109–110
 ICMP frames, 43
 ICS (Internet Connection Sharing), 330–334, 332–334
 identity theft, 19–20
 IDs
 Event, 417
 Nessus information on, 373
 IDSs (intrusion detection systems), 475–486, 477–486
 If Message’s Character Set Is Different From English option, 342
 Immunize option, 125
 Import Policy option, 72
 Inbound Filters dialog box, 285–288, 287
 incident investigation, 400
 audit log reviews, 411–420, 413–419
 file recovery. *See* Volume Shadow Copy (VSC)
 memory dumps, 420–428, 422–427
 object access, 401–410, 403–406
 packet capturing, 428–438, 431–437
 Include All Certificates In The Certification Path If Possible option, 350
 Include All Local (Intranet) Sites Not Listed In Other Zones option, 326
 Include All Network Paths (UNCs) option, 326
 Include All Sites That Bypass The Proxy Server option, 326
 .inf extension, 67
 information classification, 20–22
 Information option for Security log, 417, 419
 inheritable permissions, 202
 inherited auditing attributes, 409
 Initialize And Convert Disk Wizard, 166–168, 167–168, 176–177, 176
 initializing
 backups, 183–185, 183–185
 disks, 175–177, 176–177
 restores, 191–192, 191–192
 VPN services, 261–264, 261–264
 Install From A List Or Specific Location (Advanced), 457
 Install From Disk dialog box, 458
 Install WinPcap? screen, 433, 433
 Installation Progress dialog box, 466
 Installation Summary for patches, 53
 installing
 AD-Aware, 120
 applications, 466, 467
 avast!, 107–109, 108–109
 Cain & Abel, 134–135
 digital certificates, 345–347, 345–346
 e-mail certificates, 351–352, 351
 Malicious Software Removal Tool, 128, 128
 McAfee Site Advisor, 131, 131
 Netcat, 394–395
 NetWatcher 2000, 477–481, 477–481
 Outlook spam filter, 342–343, 343
 Previous Versions, 448–452, 449–452
 Rootkit Hunter, 114–115
 Spybot-S&D, 124
 Wireshark, 302, 431–434, 432–434

- integrity
 - asset, 454
 - in VPNs, 254
 - Integrity and Encryption Algorithm dialog box, 314, 314
 - Interface Filters dialog box, 288
 - Interface Properties dialog box, 299
 - International tab, 341
 - Internet, 320
 - access, 320–324, 322–323
 - digital certificates
 - backups, 348–353, 349–352
 - installing, 344–347, 345–346
 - download validation, 357–360, 360
 - e-mail, 334–339, 336–338
 - file exchange, 353–357, 354–357
 - ICS, 330–334, 332–334
 - Internet Explorer
 - cookies, 328–330, 329
 - security zones, 324–328, 326–327
 - logging and recording activity, 361–365, 362–364
 - spam, 339–343, 341–343
 - vulnerability profiling, 385–390, 388
 - Internet Connection Sharing (ICS), 320, 330–334, 332–334
 - Internet Connection Wizard, 322
 - Internet Explorer
 - cookies, 328–330, 329
 - security zones, 324–328, 326–327
 - Internet icon, 325
 - Internet Information Services Scan option, 381
 - Internet Options dialog box
 - cookies, 329
 - digital certificates, 349, 349, 351–352
 - security zones, 325–327, 326
 - Internet Protocol option, 332
 - Internet Protocol Security. *See* IPsec (Internet Protocol Security) VPNs
 - Internet Protocol (TCP/IP) Properties dialog box, 333–334, 334
 - intrusion detection systems (IDSs), 475–486, 477–486
 - intrusion protection systems (IPSs), 475–476
 - investigating incidents. *See* incident investigation
 - IP addresses
 - intrusion protection systems, 482, 482
 - IPsec VPN, 304–306, 306, 308–309, 309
 - packet filters, 286–287
 - SFTP, 356
 - tracking, 390–393, 391–393
 - ipconfig command, 304
 - ipconfig /all command, 296, 334
 - IPsec Secure Servers Policy, 402
 - IPsec Settings tab, 312, 312
 - IPsec (Internet Protocol Security) VPNs, 300–302
 - configuring
 - AES-256, 312–315, 312–315
 - general, 307–311, 308–311
 - connectivity testing and captured data viewing, 304–307, 304–307
 - deploying, 255–259, 258
 - destination computer shares, 302–304, 302–304
 - validating encryption, 315–317, 316–317
 - Wireshark sniffer, 302
 - IPSs (intrusion protection systems), 475–476
-
- J**
- Junk E-mail Options dialog box, 340–342, 341
 - junk mail
 - managing, 339–343, 341–343
 - scanning for, 388

K

KeenValue spyware, 123
 Kerberos authentication, 255
 Kernel Memory Dump option, 423
 Key regeneration settings, 314
 keys
 BitLocker, 212–215, 212–215
 digital certificates, 350
 encryption, 158–159, 159
 keywords in spam filters, 343
 knowledge-based IDS analytic engines, 476

L

L2TP (Layer 2 Tunneling Protocol), 260, 263, 263
 L3 Titan Group, 142
 LAD (local accounts database), 239
 Language, Time Zone and Keyboard Selection window, 207
 LANs (local area networks), 320, 322–323, 322–323
 laptop computers encryption. *See* BitLocker drive encryption
 Last Known Good Configuration (LKGC), 459–462, 461
 LaunchPad Installer utility, 84
 Layer 2 Tunneling Protocol (L2TP), 260, 263, 263
 license agreements
 avast!, 108
 McAfee Site Advisor, 131
 Nessus, 369
 NetWatcher 2000, 478
 Retina, 375
 Volume Shadow Copy, 450
 WinPcap, 433
 Wireshark, 432
 Link Logger program, 362–364, 363–364
 LKGC (Last Known Good Configuration), 459–462, 461
 loadable kernel modules (LKMs), 113
 local accounts database (LAD), 239
 Local Administrators, 158, 239
 Local Area Network Interface option, 285–286
 Local Area Network Internet Configuration screen, 323
 local area networks (LANs), 320, 322–323, 322–323
 Local Disks option, 110–111
 Local Intranet icon, 325
 Local Intranet window, 326–327, 327
 Local Policies, 69, 73
 Local Resources tab, 274, 274
 Local Security Settings dialog box, 148–149, 148
 Local System account, 30–32, 31–32
 locking down services, 32–36, 33–35
 lockout policy, 230–231, 230–231
 Log On As service account, 30–32, 31–32
 logoff scripts for Autorun, 82–83
 logon scripts for Autorun, 82–83
 logons, auditing, 231–238, 233–238
 logs, 232
 account logon events, 237–238, 237–238
 Default Domain Controllers Policy, 234–238, 234–238
 Internet activity, 361–365, 362–364
 reviewing, 411–420, 413–419
 settings, 404–405, 404–405
 size, 235, 235, 404, 404
 loss potential, estimating, 4–5
 lost encryption keys, 158–159, 159
 Low setting
 Internet Explorer security, 325
 for spam, 340

M

- MAC (Media Access Control) addresses
 - finding, 296
 - with switches, 429
 - in wireless security, 294–296
- Macro virus infections, 106
- malicious software
 - adware, 118–123, 120–122
 - ARP poisoning, 133–140, 135–140
 - Malicious Software Removal Tool, 127–130, 128–129
 - McAfee Site Advisor, 130–133, 131–133
 - rootkits, 112–118
 - spyware, 123–127, 125–126
 - viruses, 106–112, 108–111
- Malicious Software Removal Tool, 127–130, 128–129
- manual operating system patching, 50–53, 50–53
- Manual service startup type, 29
- Mark As Good option, 342
- Mark As Spam option, 342
- master boot record (MBR)
 - infections, 106
- Maximum Password Age
 - setting, 229
- Maximum Ports setting, 264
- Maximum Security Log Size dialog box, 235, 235
- Maximum Security Log Size Policy
 - option, 403
- MBR (master boot record)
 - infections, 106
- MBSA (Microsoft Baseline Security Analyzer), 379–382, 380–382
- McAfee Site Advisor, 130–133, 131–133
- MD5 algorithm, 359
- md5sum algorithm, 358–359
- media, sanitizing, 470–475, 472–474
- Media Access Control (MAC) addresses
 - finding, 296
 - with switches, 429
 - in wireless security, 294–296
- Medium setting, 325
- Medium-Low setting, 325
- Melissa virus, 334–335
- memory dumps, 420–428, 422–427
 - configuring, 422–424, 422–424
 - Registry for, 424–425, 425
 - reviewing, 426–428, 426–427
 - triggering, 425, 425
- Message Integrity Check (MIC), 260
- Message Options dialog box, 347
- Messenger spam, 388
- MIC (Message Integrity Check), 260
- Microsoft Baseline Security Analyzer (MBSA), 379–382, 380–382
- Microsoft Management Console (MMC)
 - security templates, 65–67, 66
 - services, 27
- minidumps, 422–424, 422–424
- Minimum Password Age setting, 229
- Minimum Password Length setting, 229
- mirrored volumes, 174, 177–180, 177–180
- MMC (Microsoft Management Console)
 - security templates, 65–67, 66
 - services, 27
- modems, 320, 333
- modes, Syskey, 161–164, 163–164
- monitoring
 - audit logs, 232
 - packet analyzers for. *See* Wireshark Network Analyzer
 - security logs, 237–238, 237–238
- Move dialog box, 406, 406
- MS GINA dialog box, 164
- MSConfig utility, 75–79, 76–78
- MSSecure.xml file, 51
- My Use Only option, 268

N

names

- Administrator accounts, 241
- IPSec VPN rules, 311, 311
- restore points, 465
- services, 36
- NAT (Network Address Translation), 266, 330
- Nessus penetration testing, 368–373, 370–372
- net stop command, 36
- Netcat tool, 393–397
- Netgroup Packet Filter driver, 433
- NETLOGON share, 83
- netstat command, 44–46, 391–393, 391–393
- NetWatcher 2000 HIDS, 477–486, 477–486
- Network Address Translation (NAT), 266, 330
- network analyzers, 428–431
 - data capture, 305–306, 306–307
 - downloading, 302, 431, 431
 - installing, 302, 431–434, 432–434
 - IPSec VPN encryption validation, 315–317, 316
 - network analysis with, 436–438, 437
 - packet capturing with, 434–436, 434–436
- Network And Dial-up Connections dialog box, 331–332, 332
- Network Connection screen, 267, 267
- Network Connections option, 299
- Network Interface Cards (NICs), 289–290
- network paths, 327
- network security, 254–255
 - IPSec. *See* IPSec (Internet Protocol Security) VPNs
 - packet filters, 284–289, 286–288
 - Run As, 278–284, 280–283
 - Secure Remote Administration, 270–277, 272–277
 - VPN
 - clients, 266–270, 267–270
 - servers, 259–266, 261–265
 - wireless, 289–291
 - access points, 291–296, 291–295
 - clients, 296–300, 297–299
- Network tab, 135
- Networking tab, 268, 268, 332
- New Connection Wizard, 267–268, 267–268
- New Object - Group dialog box, 196, 196, 249–250, 249–250
- New Object - User dialog box, 197, 197, 222, 222
- New Partition Wizard, 168–171, 169–171
- New Rules option, 308, 308
- New Technology File System (NTFS)
 - converting FAT to, 165–174, 167–173
 - permissions for, 201, 251–252, 251–252
- New User dialog box
 - EFS, 146
 - nonadministrator users, 280
- New Virtual Machine Wizard, 97–99, 97–99
- New Volume Wizard, 178–179, 178–179
- NICs (Network Interface Cards), 289–290
- Nmap program, 39–40, 47–48
- No Authentication option, 275
- No Automatic Filtering option, 340
- nonadministrator users for Run As function, 280–284, 281–283
- nonpromiscuous mode, 429
- nonrepudiation, 260
- Notepad, 89
- Notify Me But Don't Automatically Download Or Install Them option, 54

npf.sys file, 433
 NTDSUTIL utility, 245–246
 NTFS (New Technology File System)
 converting FAT to, 165–174, 167–173
 permissions for, 201, 251–252,
 251–252

O

object access, 401–402
 auditing GPOs for, 402–405,
 403–405
 group policy refreshing for,
 406–407, 407
 resource servers for
 auditing by, 407–410, 407–410
 location of, 405–406, 406
 Obtain An IP Address Automatically
 option, 333
 Obtain DNS Server Address
 Automatically option, 334
 Office spam filter, 342
 Only Show Policy Settings That Can Be
 Fully Managed option, 93
 Open File - Security Warning dialog
 box, 431
 open ports, 44–48, 46–47
 operating system patching, 49–51
 automated
 in Domain mode, 54–64, 55–63
 in Workgroup mode, 53–54, 54
 manual, 50–53, 50–53
 Options dialog box
 digital certificates, 345, 347
 graphics, 337–338, 337
 Organizational Unit option, 33
 organizational units (OUs)
 GPOs for, 33–34
 for groups, 196
 infrastructure for, 256–257
 for resource servers, 405–406, 406

outages, threat analysis for, 5
 Outlook. *See* e-mail
 Outlook Spam Filter Settings dialog
 box, 342–343, 343
 Override Automatic Cookie Handling
 option, 329

P

packet analyzers, 428–431
 data capture, 305–306, 306–307
 downloading, 302, 431, 431
 installing, 302, 431–434, 432–434
 IPSec VPN encryption validation,
 315–317, 316
 network analysis with, 436–438, 437
 packet capturing with, 434–436,
 434–436
 packet filters, 284–289, 286–288
 partitions
 BitLocker encryption, 207–210,
 207–209
 converting FAT to NTFS, 165–174,
 167–173
 Password Can Be Changed After
 setting, 229
 Password Must Be At Least setting, 229
 Password Must Meet Complexity
 Requirements option, 229
 Password Never Expires option, 146,
 197, 413
 Password tab, 136
 Password Will Expire In setting, 229
 passwords
 BitLocker, 212–215, 212–215
 Cain & Abel, 136, 140
 Data Recovery Agent policy, 148
 decoy domain administrator
 accounts, 244
 digital certificates, 150, 350–351
 DSRM administrators, 245–246

- encryption, 157
- RDP, 276
- Run As function, 283–284
- service management, 32
- SFTP, 356
- strong, 222
- Syskey, 164
- users, 145–146, 197, 413
 - default, 239
 - policies, 226–231, 228–231
 - templates, 224–225
- VPN clients, 269
- wireless access points, 291–292, 296
- wireless clients, 297
- patching operating systems, 49–51
 - automated
 - in Domain mode, 54–64, 55–63
 - in Workgroup mode, 53–54, 54
 - manual, 50–53, 50–53
- penetration testing
 - Nessus, 368–373, 370–372
 - Retina, 374–378, 375–378
- Perform A Quick Format option, 170
- permissions
 - AGDLP, 201–204
 - EFS, 145
 - encryption, 153–154
 - IPSec VPN, 304
 - log files, 411
 - NTFS, 201, 251–252, 251–252
 - services, 25
 - share points, 204
 - user accounts, 413–415, 413–414
- personal security, policy development
 - for, 11
- Personal tab, 349
- PGP Corporation utility, 142
- Phrase Filter tab, 343
- physical and environmental security
 - checklist, 16–19
 - policy development for, 10
- Pick Multiple Computers To Scan
 - option, 380
- pictures in e-mail, 338
- PIDs (Process Identifiers)
 - HIDS, 483–484, 483–484
 - Task Manager, 47
- ping command, 304
- PKI (Public Key Infrastructure), 157
- plug-ins, 369–371
- Point-to-Point Tunneling Protocol (PPTP), 260
- poisoning, ARP, 133–140, 135–140
- policies
 - audit. *See* Audit Policy
 - development overview, 10–12
 - group. *See* Group Policy Objects (GPOs)
 - password, 226–231, 228–231
 - ranking, 8–12
- pop-ups, 118–123, 120–122
- Port Authority tool, 42
- Port Authority website, 46
- Port Manager, 485–486
- port scanning, 395–396
- portable computers encryption. *See* BitLocker drive encryption
- ports and port management, 38–40
 - monitoring, 481, 485–486, 485
 - Nessus information on, 373
 - services for, 25
 - testing, 44–48, 46–47
 - VPN servers, 263–264, 263
 - Windows Firewall for, 40–44, 40–43
- potential loss, estimating, 4–5
- PPTP (Point-to-Point Tunneling Protocol), 260
- Pre-Shared Keys (PSKs)
 - IPSec VPN, 310, 310
 - wireless security, 290, 296–297

prebuilt packet filters, 435

Prevent Local Guests Group From
 Accessing Security Log option,
 235, 404

Previous Versions Client. *See* Volume
 Shadow Copy (VSC)

Previous Versions tab, 447–448,
 448, 451

principle of least privilege, 194

Privacy tab, 329–330

Privacy Objects tab, 122

private classification, 21–22

private keys, 350

Private option for IPsec VPN
 firewalls, 310

privileges for services, 25

problem child applications, 95

Process Identifiers (PIDs)
 HIDS, 483–484, 483–484
 Task Manager, 47

processes
 ending, 486
 listing, 46–47, 47
 monitoring, 482–484, 482–484

Processes tab, 46–47, 483–484,
 483–484, 486

Program Update option, 109

Programs tab, 274

Prohibit Adjusting Desktop Toolbars
 option, 226

Prohibit User From Changing My
 Documents Path option, 226

promiscuous mode, 429–430

protecting deleted data, 470–475,
 472–474

protocol analyzers, 428–431
 downloading, 431, 431
 installing, 431–434, 432–434
 network analysis with,
 436–438, 437
 packet capturing with, 434–436,
 434–436

PSKs (Pre-Shared Keys)
 IPsec VPN, 310, 310
 wireless security, 290, 296–297

public classification, 21–22

Public Key Infrastructure (PKI), 157

Public option for IPsec VPN
 firewalls, 310

purging media, 470–475, 472–474

PurityScan spyware, 123

pwned term, 84

Q

qualitative risk assessment, 2

quantitative risk assessment, 2–3

R

RAID (Redundant Array of Independent
 Disks) systems, 174–180, 176–180

random access memory (RAM) memory
 dumps, 420–428, 422–427

RDP (Remote Desktop Protocol),
 270–271
 clients, 273–276, 273–277
 connections, 277
 servers, 272–273, 272

Receive All Packets Except Those
 That Meet The Criteria Below
 option, 288

recording Internet activity, 361–365,
 362–364

Recover option, 124

recovering encrypted files, 157–161,
 159–160

recovery password keys, 212–215,
 212–215

Redundant Array of Independent Disks
 (RAID) systems, 174–180, 176–180

refreshing group policies, 406–407

Refreshing Policy window, 407

- Registry
 - Autorun security, 79–82, 79–80
 - editing dangers, 80
 - “known good” settings, 459
 - Last Known Good Configuration for, 459–461
 - for memory dumps, 424–425, 425
 - spyware changes to, 123
 - for system services, 36
- Remediate tab, 377, 377
- Remote Desktop Connection dialog box, 277
- Remote Desktop Protocol (RDP), 270–271
 - clients, 273–276, 273–277
 - connections, 277
 - servers, 272–273, 272
- remote systems, attacks on, 396–397
- Remote tab, 272, 272
- Removable Media option, 110
- Remove My Computer Icon On The Desktop option, 226
- renaming Administrator account, 241
- Replace Auditing Entries On All Child Objects With Entries Shown Here That Apply To Child Objects option, 410
- reports
 - Nessus, 372–373, 372
 - Retina, 378, 378
- Require Encryption For All Connection Security Rules That Use These Settings option, 313
- Require Startup USB Key At Every Startup option, 212
- Reset Account Lockout Counter After setting, 230
- resetting
 - DSRM administrator passwords, 245–246
 - services, 36–38, 37
- Resident Scanner option, 110
- resource servers
 - object access on, 407–410, 407–410
 - OUs for, 405–406, 406
- Restore And Manage Media tab, 189–191, 190
- Restore My Computer To An Earlier Time option, 467
- Restore Progress dialog box, 192, 192
- Restore Security option, 191
- restoring
 - backup data, 188–193, 190–193
 - system. *See* System Restore feature
- Restrict Drives folder, 92–93
- Restricted Sites icon, 325, 327
- Restricted Sites window, 327
- Retention Method For Security Log option, 235, 404
- Retina penetration testing, 374–378, 375–378
- reusing media, 470–475, 472–474
- Review and Install Updates option, 51
- reviewing
 - audit logs, 411–420, 413–419
 - memory dumps, 426–428, 426–427
- revocation, certificate, 352–353, 352–353
- rights for services, 25
- Rijndael ciphers, 205
- risk assessment, 2–8
- risk factors, Nessus information on, 373
- Rivest, Ron, 359
- rogue protocols, 428
- rootkit checkers, 112–118
- Rootkit Hunter tool
 - installing, 114–115
 - running, 116–118
- Rootsec security template, 67
- Router tab, 363, 363
- Routing and Remote Access Services (RRAS)
 - packet filters in, 285–289, 286–288
 - for VPN, 261–264, 261–264, 269
- Routing tab, 135

RRAS Setup Wizard, 262, 262
 rules
 intrusion protection systems, 475
 IPSec VPN, 308, 308, 311, 311
 Rules Type screen, 308, 308
 Run As dialog box, 282–283, 283
 Run As function, 278–279
 command-line, 283–284
 nonadministrator users for, 280–284,
 281–283
 Secondary Logon Service for,
 280–281, 280–281
 Run Components Not Signed With
 Authenticode option, 326, 339
 Run Components Signed With
 Authenticode option, 326
 Run entry, 80
 RunOnce entry, 79–80
 RunOnceEx entry, 79
 Russia, spam from, 342

S

SACL (System Access Control List), 408
 Safe Lists, 341
 Safe mode
 booting into, 455–459, 456–458
 System Restore from, 469
 Safe Senders List, 339
 SAM (Security Accounts Management)
 database, 161–162
 sanitizing media, 470–475, 472–474
 SANS Institute, 12
 SANS Internet Storm center, 391
 Satan tool, 393
 Save As dialog box
 for backups, 183, 183
 for RDP settings, 276
 Save This Username And Password For
 The Following Users option, 269
 saving RDP settings, 276

Scan A Computer option, 380
 Scan From The Localhost option, 371
 Scan Log tab, 122
 Scan More Than One Computer
 option, 380
 Scan Results tab, 122
 Scan Type screen, 128, 128
 scanners
 Nessus, 368–373, 370–372
 Retina, 374–378, 375–378
 scanning
 AD-Aware, 120–122, 120–122
 avast!, 110–111, 110–111
 Messenger spam, 388
 Netcat, 395–396
 SCAT (Security Configuration and
 Analysis Tool), 65, 67–71, 67–71
 Schedule Job dialog box, 186–188,
 186–188
 Schedule tab, 37, 37
 Scheduled Job Options dialog box,
 186–188, 186
 schedules
 daily backups, 186–188, 186–188
 resetting services, 36–38, 37
 Volume Shadow Copy, 442, 442
 Script ActiveX Controls Marked Safe
 For Scripting option, 338
 scripts
 Autorun security, 82–83, 83
 resetting services, 36–38, 37
 Search & Destroy option, 124–125, 125
 Secondary Logon service, 278, 280–281,
 280–281
 Secure Erase tool, 470
 Secure FTP (SFTP) server, 354–357,
 354–357
 Secure Hashing Algorithm (SHA), 255
 Secure Remote Administration,
 270–277, 272–277
 Secure Server IPSec Policy GPO,
 257–258, 258

- Secure Server (Require Security)
 - option, 258
- Securedc security template, 67
- securews.inf file, 68
- Securews security template, 67
- Securing The Windows XP Account
 - Database dialog box, 163–164, 163
- Security Accounts Management (SAM)
 - database, 161–162
- security assessments
 - HFNetChk for, 382–385
 - Microsoft Baseline Security Analyzer
 - for, 379–382, 380–382
 - physical and environmental, 16–19
 - risk, 2–3
 - Threat Analysis Index, 122
- Security Configuration and Analysis
 - Tool (SCAT), 65, 67–71, 67–71
- Security dialog box for e-mail, 338–339
- security education, training, and awareness (SETA) task, 12–16
- Security for ClipBook dialog box, 35–36, 35
- Security logs
 - account logon events, 237–238, 237–238
 - in Default Domain Controllers Policy, 234–238, 234–238
 - reviewing, 416–419, 416–419
 - settings, 404–405, 404–405
- security organization, policy
 - development for, 11
- security policies
 - audit. *See* Audit Policy
 - development overview, 10–12
 - group. *See* Group Policy Objects (GPOs)
 - password, 226–231, 228–231
 - ranking, 8–12
- Security Properties dialog box, 347, 347
- security scanners
 - Nessus, 368–373, 370–372
 - Retina, 374–378, 375–378
- Security Settings dialog box, 326, 326, 338, 338
- Security Settings Name field, 345
- Security tab
 - e-mail, 338
 - EFS, 145, 145, 160, 160
 - graphics, 337, 337
 - Internet Explorer, 325, 326
 - RDP, 275, 275
 - shares, 201–202, 201, 203
 - user accounts, 413–414, 413
- security templates, 64–65
 - custom, 67–71, 67–71
 - default, 65–67, 66
 - GPOs for, 72–73, 72–73
- Security Update Scan Results
 - option, 381
- security zones
 - e-mail, 338–339, 338
 - Internet Explorer, 324–328, 326–327
- Select Certificate dialog box, 346, 346
- Select Columns option, 483
- Select Disks screen, 178, 178
- Select Disks To Convert screen, 168, 168, 177
- Select Disks To Initialize screen, 176, 177
- Select Partition Type screen, 169, 169
- Select Process Page Columns dialog box, 484, 484
- Select Recovery Agents screen, 149, 149
- Select The Program From A List
 - option, 427
- Select User dialog box, 156, 161
- Select User, Computer, Or Group dialog box, 408–409, 408–409
- Select Users, Computers, Or Groups dialog box, 414, 414
- Select Volume Type screen, 178, 178
- Send These Certificates With Signed Messages option, 347
- sensitive classification, 21–22

- servers
 - ICS, 331–333, 332–333
 - RDP, 272–273, 272
 - resource, 405–410, 407–410
 - VPN, 259–266, 261–265
- Service Control dialog box, 281
- services, 24–27
 - accounts for, 30–32, 31–32
 - Computer Management for, 27–28, 27
 - dependencies between, 28–29, 28
 - disabling and stopping, 28–30, 29
 - locking down, 32–36, 33–35
 - resetting, 36–38, 37
- Services tab, 78, 78
- Set Up Your Internet Mail Account screen, 323
- SETA (security education, training, and awareness) task, 12–16
- Settings dialog box, 442–443, 442
- Setup Security template, 67
- SFTP (Secure FTP) server, 354–357, 354–357
- SFTP Root field, 355
- SFTP Root Path dialog box, 355, 355
- SHA (Secure Hashing Algorithm), 255
- Shadow Copies Of Selected Volume section, 443
- Shadow Copies tab, 441–442, 441, 445–446, 445–446
- Shadow Copy Client, 439, 448, 450
- ShadowCopyClient.msi file, 449–450
- share points, 193–194, 204
- Share This Folder option, 303
- shares, 193–195
 - AGDLP for
 - content for, 198–204, 198–204
 - users and groups for, 195–198, 196–198
 - content for, 195
- Sharing tab, 302, 302
- ShieldsUP tool, 386–390, 388
- short-term outages, threat analysis for, 5
- SHOTGUN server, 405
- Show The Contents Of This Folder option, 144, 151, 153, 156
- Shut Down System Immediately If Unable To Log Security Audits option, 236
- Shut Down Windows dialog box, 164
- shutdown
 - abnormal, 421
 - scripts for, 82–83
- Signing Certificate field, 345
- Single Loss Expectancy (SLE), 3–8
- Site Advisor, 130–133, 131–133
- size
 - logs, 235, 235, 404, 404
 - packet capture buffers, 435
 - partitions, 169–170, 169
- slack space, 471–474, 472–474
- SLE (Single Loss Expectancy), 3–8
- Small Memory Dump (64 KB) option, 423
- Sniffer tab, 135
- sniffers, 428–431
 - Cain & Abel, 135
 - downloading, 431, 431
 - installing, 431–434, 432–434
 - network analysis with, 436–438, 437
 - packet capturing with, 434–436, 434–436
- Software Explorer utility, 74
- Source Network option, 286
- South Korea, spam from, 342
- spam
 - managing, 339–343, 341–343
 - scanning for, 388
- Spam Me With This Note option, 388
- Spam Recognition Keywords List dialog box, 343, 343
- SpamAid Settings dialog box, 342–343, 343

- Specify Disk Capacity screen, 99, 99
 - Specify Intranet Microsoft Update
 - Service Location Properties dialog box, 63, 63
 - Specify Partition Size screen, 169–170, 169
 - Spybot-S&D program, 123–127, 125–126
 - spyware, 123–127, 125–126
 - SQL Slammer virus, 335
 - SSIDs, 293–294
 - Start Scan Task option, 370
 - Startup And Recovery dialog box, 423–424, 423–424
 - Startup folder, 81, 81
 - Startup Key dialog box, 164
 - startup scripts, 82–83
 - Startup tab, 78, 78
 - Startup Type setting, 29–30
 - Status menu in Ad-Aware, 120, 120
 - stolen equipment, threat analysis for, 5
 - StopAlerter script, 36–38
 - stopping services, 28–30, 29
 - storage, 142
 - backups. *See* backups
 - encryption. *See* Encrypting File System (EFS); encryption
 - fault tolerance for, 174–180, 176–180
 - NTFS filesystems, 165–174, 167–173
 - shares, 193–204, 196–204
 - Syskey for, 161–164, 163–164
 - Store Startup Key Locally option, 164
 - Store Update Files Locally On This Server option, 58
 - strong passwords, 222
 - Subnet Mask setting, 286–287
 - success, triggering on, 415, 415
 - Success and Failure setting, 73
 - Success option for policy settings, 403
 - Success Audit option, 419
 - Successful Installation screen, 450
 - switches, sniffers with, 429
 - Synchronization Options option, 56
 - Synchronize From An Upstream Windows Server Update Services Server option, 57
 - Synchronize From Microsoft Update option, 57
 - Synchronize Manually option, 56
 - synchronizing patching, 54–61, 55–60
 - sysdata.xml file, 427
 - Syskey utility, 161–164, 163–164
 - system access control, policy
 - development for, 10
 - System Access Control List (SACL), 408
 - System Configuration Utility, 75–79, 76–78
 - system development and maintenance,
 - policy development for, 10
 - System Failure section, 423
 - SYSTEM.INI tab, 76, 76
 - System Properties dialog box
 - minidumps, 422–424, 422
 - Run As function, 281–283, 281
 - System Restore, 464–465, 464
 - System Recovery Options dialog box, 207–208, 207–208
 - System Restore feature, 462–464
 - new applications, 466, 467
 - process, 467–469, 467–468
 - restore points for, 424, 464–466, 464–466
 - from Safe Mode, 469, 469
 - System Restore tab, 464
 - System Restore Wizard, 465–466, 465–466
 - System Volume Information dialog box, 472–473, 472
-
- T**
- TAI (Threat Analysis Index), 122
 - Task Manager, 46–47, 47, 483–486, 483–484

- task scheduled scripts, 36–38, 37
 - Task Scheduler Wizard, 36
 - TCP Reset frames, 475
 - templates, 64–65
 - custom, 67–71, 67–71
 - default, 65–67, 66
 - GPOs for, 72–73, 72–73
 - user accounts, 221–225, 222–225
 - Terminal Services (TS), 270
 - testing, 368
 - avast!, 112
 - EFS data recovery, 161
 - Internet vulnerability profiling, 385–390, 388
 - Netcat, 393–397
 - open ports, 44–48, 46–47
 - penetration testing
 - with Nessus, 368–373, 370–372
 - with Retina, 374–378, 375–378
 - previous versions, 447–448, 447–448
 - restored data, 192–193, 193
 - security assessments for
 - HFNetChk for, 382–385
 - Microsoft Baseline Security Analyzer for, 379–382, 380–382
 - Syskey mode, 164, 164
 - tracking hostile IPs, 390–393, 391–393
 - Testing Open Ports processes, 47–48
 - The Following System Components
 - Depend On This Service field, 28–29
 - third-party cookies, 329
 - This Service Depends On The Following
 - System Components field, 28
 - threat analysis, 5–6
 - Threat Analysis Index (TAI), 122
 - threat levels, 4
 - 3DES, 255, 260, 300
 - thumb drives
 - BitLocker, 206, 210–212, 210–212
 - U3 system on, 84
 - Time service, 28–30, 29
 - Time Warp Client. *See* Volume Shadow Copy (VSC)
 - Top 10 page, 391–392, 391
 - TPM (Trusted Platform Module), 206
 - Traceroute tab, 135
 - tracking hostile IPs, 390–393, 391–393
 - training in user awareness programs, 12–16
 - triggering
 - Audit Policy, 415–416, 416
 - memory dumps, 425, 425
 - Triple Data Encryption Standard (3DES), 255, 260, 300
 - Tripwire program, 360
 - Trojaned rootkits, 112
 - troubleshooting, 454
 - host-based intrusion detection systems, 475–486, 477–486
 - Last Known Good Configuration for, 459–462, 461
 - Safe mode for, 455–459, 456–458
 - sanitizing media, 470–475, 472–474
 - System Restore for, 462–470, 464–469
 - Trusted Platform Module (TPM), 206
 - Trusted Sites window, 327, 327
 - TS (Terminal Services), 270
 - tunnels in IPSec VPN, 308, 309
 - Turn Off Automatic Updates option, 54
 - Turn Off System Restore, 464
 - Twcli32.msi file, 448
-
- U**
- U3 system, 84
 - UAC (User Account Control), 476
 - UDP (User Datagram Protocol), 438
 - United States, spam from, 342
 - Universal Naming Convention (UNC)
 - paths, 327
 - Universal Plug and Play (UPnP)
 - Framework option, 41

- Update Classifications option, 57
 - Update option, 125
 - updating avast!, 109–110, 110
 - UPN (User Principal Name), 243–244
 - USB keys, 212–215, 212–215
 - USB thumb drives
 - BitLocker, 206, 210–212, 210–212
 - U3 system on, 84
 - Use A Proxy Server When Synchronizing option, 57
 - Use Bridged Networking option, 98
 - Use Network Address Translation (NAT) option, 98
 - Use The Following IP Address option, 333
 - User Account Control (UAC), 476
 - User Authentication option, 339
 - user awareness programs, 12–16
 - User Cannot Change Password option, 145, 197
 - User Datagram Protocol (UDP), 438
 - User Must Change Password At First Logon option, 224
 - User Must Change Password At Next Logon option, 145, 197, 222, 244, 413
 - User Principal Name (UPN), 243–244
 - User tab, 363
 - usernames
 - RDP, 276
 - Run As function, 283
 - SFTP, 354, 356
 - user accounts, 224–225
 - wireless access points, 291–292
 - users and user accounts
 - for AGDLP, 195–198, 196–198
 - creating, 220–226, 222–226, 412–413
 - default, 239–240
 - decoy domain administrator account, 243–244, 243–244
 - Default Domain Policy for, 240–242, 241–242
 - DSRM administrator passwords, 245–246
 - Deny group for, 247–252, 248–252
 - for EFS, 145–146, 146
 - GPOs for, 225–226, 225–226
 - Link Logger, 363
 - logon auditing, 231–238, 233–238
 - passwords, 145–146, 197, 413
 - default, 239
 - policies, 226–231, 228–231
 - templates, 224–225, 224
 - templates, 221–225, 222–225
-
- V**
- validation
 - downloads, 357–360, 360
 - IPSec VPN encryption, 315–317, 316–317
 - in VPNs, 254
 - value of documents, 19–22
 - Verify Data After Backup option, 184
 - versions
 - file. *See* Volume Shadow Copy (VSC)
 - Rootkit Hunter, 114
 - View Available Wireless Networks option, 299
 - View Certificate option, 346
 - View Existing Reports option, 380
 - View Security Report screen, 381
 - View tab, 335–336, 336
 - Virtual Machine Settings dialog box, 100–101, 100–101
 - virtual machines (VMs), 95, 97–103, 97–102
 - Virtual Private Network Connection option, 267

virtual private networks (VPNs),
 254–255
 clients, 266–267
 configuring, 267–268, 267–268
 connecting to server, 268–269, 269
 IPSec VPN. *See* IPSec (Internet
 Protocol Security) VPNs
 servers, 259–261
 connecting clients to,
 268–269, 269
 dial-in privileges for, 264–265,
 264–265
 RRAS services for, 261–264,
 261–264
 virtualization, 95–103, 97–102
 Virus Chest option, 110
 viruses, 106–107, 334–335
 avast! antivirus tool for
 downloading and installing, 107–
 109, 108–109
 scanning with, 110–111, 110–111
 testing, 112
 updating, 109–110, 110
 threat analysis for, 5
 VMs (virtual machines), 95, 97–103,
 97–102
 VMware, 95–96
 VoIP tab, 136
 Volume Shadow Copy (VSC), 438–440
 configuring and enabling, 440–443,
 441–444
 previous versions for
 installing, 448–452, 449–452
 producing, 443–446, 445–446
 testing, 447–448, 447–448
 volumes
 for EFS, 144–145, 144–145
 mirrored, 177–180, 177–180
 VPN Server Selection screen, 268
 VPNs. *See* virtual private networks
 (VPNs)
 VSC. *See* Volume Shadow Copy (VSC)

VShell dialog box, 354, 354
 VShell SFTP server software, 354–357,
 354–357
 vulnerability profiling, 385–390, 388

W

WAN Miniport (L2TP) option, 264
 WAN Miniport (PPTP) option, 264
 Warn Me Before Downloading Content
 option, 338
 Warning option, 417, 419
 WGA (Windows Genuine Advantage)
 program, 50
 WIN.INI tab, 76–77, 77
 Windows Advanced Options Menu,
 456–457, 456, 469
 Windows Defender, 74
 Windows Error Reporting dialog
 box, 427
 Windows Firewall, 40–44, 40–43
 Windows Firewall with Advanced
 Security dialog box, 312, 312
 Windows Genuine Advantage (WGA)
 program, 50
 Windows Internet Name Service
 (WINS), 38
 Windows Scan Results option, 381
 Windows Time service, 28–30, 29
 Windows Update, 50–53
 Windows Update progress dialog box,
 52–53
 Windows XP Startup Password dialog
 box, 164, 164
 WinPcap program, 433, 433
 WINS (Windows Internet Name
 Service), 38
 WinSCP SFTP client, 356–357, 356
 Wireless Network Properties dialog
 box, 298
 Wireless Networks tab, 297, 297

wireless security, 289–291
 access points, 291–296, 291–295
 clients, 296–300, 297–299

Wireless tab, 135

Wireless Zero Configuration
 (WZC), 296

Wireshark Network Analyzer, 428–431
 data capture, 305–306, 306–307
 downloading, 302, 431, 431
 installing, 302, 431–434, 432–434
 IPSec VPN encryption validation,
 315–317, 316
 network analysis with, 436–438, 437
 packet capturing with, 434–436,
 434–436

Workgroup mode, patching in,
 53–54, 54

worms, 106

WPA-PSK option, 297

Write Debugging Information
 option, 423

WSUS
 configuring, 54–61, 55–60
 patching from, 61–64, 61–63

WZC (Wireless Zero
 Configuration), 296

Y

Yes, Export The Private Key option, 350

Z

Zone Settings option, 338

zones
 e-mail, 338–339, 338
 Internet Explorer, 324–328, 326–327

