

# Index

## A

Absolute security, xvii

Acceptable risk  
 assessing, 6  
 defined, xvii

Access Control  
 defined, xvii  
 granting to files, 54–58  
 network security and, 24–25

Access Control Lists. *See* ACLs (Access Control Lists)

Access, network  
 Access Control, 24–25  
 denying, 39–40  
 directory, 16–19  
 remote, 60–61

Access tokens, 38–39

Account policies, 73–74

ACLs (Access Control Lists)  
 defending against hackers, 134  
 defined, 169  
 overview of, 25  
 sharing data, 41  
 Windows 2000 server and, 87–88

Acronyms, security, 167–169

Active Content, Web security, 156–157

Administrative shares, deleting on NT servers, 75–76

Administrator/Owner role, home users, 26–28

Administrators  
 controlling access/rights, 24–25  
 granting privileges, 27, 35–39  
 Web browsing precautions for, 156  
 Windows NT, creating false accounts, 80  
 Windows NT, renaming accounts, 54

## Advertisers

gleaning e-mail/browser information, 103  
 tracking user behavior, 121

Algorithms, encryption, 22

AllowedPaths Key(s), securing NT servers in Registry, 80–81

Antivirus software/resources. *See* AV (Antivirus) software

Application layer filtering  
 defined, 170  
 server security with, 70–71

Attachments, e-mail, 113

AU (Authenticated Users)  
 defined, 170  
 granting access with, 55–58

Audit logs  
 defined, 170  
 managing privileges for, 38  
 parsing for Internet security, 99

Auditing  
 Internet security, turning on, 97  
 levels of, 134–137  
 NT servers, turning on, 72–73, 78–79  
 privilege, 38

Authentication, xvii

AV (Antivirus) software  
 Internet security with, 97  
 overview of, 152–154  
 reducing risk with, 150–152  
 Web resources for, 154–155, 165–166

## B

Back doors, 170

Back Orifice (BO), 94, 170

Backing store, defined, 170

- Backups
    - overview of, 42
    - protecting computer with, 50–51
    - user privileges for files/directories, 35
    - virus protection and, 150, 151
  - Banner ads, 103, 121
  - Base Objects, NT servers, 78–79
  - Batch jobs, 38
  - BlackIce Defender
    - alerting when under attack, 137
    - overview of, 50
  - Blockers, filtering junk e-mail, 117–118
  - Blowfish, 100
  - BO (Back Orifice), 94, 170
  - Border control
    - defined, 170
    - overview of, 46
    - server security using, 68
  - Browsers
    - defined, 170
    - patches, 125–126
    - sandbox/security settings, 125
    - security zones, 123–124
    - upgrading and, 151
  - Buffer overruns, software
    - security, 142
- C**
- Cable modem connections, 96, 170
  - Change Permission, files/directories, 31
  - Checklists, security
    - e-mail, 118
    - Internet, 105
    - network, 42–43
    - risk assessment, 9–14
    - server, 88–92
    - Virus and Trojan horse, 157
    - Web, 128–130
    - Windows workstation, 64–66
  - Classification, data
    - risk assessment, 3–4
    - risk checklist, 9–14
  - Clean systems, 147
  - Code Red worm, 148
  - Collectors
    - assessing risks from, 8
    - defined, 170
  - Computer Management applet,
    - Windows 2000, 28–29
  - Computer virus. *See* viruses
  - Computers
    - incident response centers, 164–165
    - protecting, 5
    - Workgroup vs. Domain, 34
  - Computers, Windows-based, 45–66
    - general practices, 46–49
    - Homestead example, 45
    - small businesses only, 61–66
    - Windows 9x, 49–53
    - Windows NT 4.0, 54–61
  - Connections
    - assessing security risk of, xxii
    - being watched on Internet through, 102–103
    - Cable modem connections, 96, 170
    - detecting intruders, 138
    - types of Internet, 93–97
  - Control Panel, Windows 2000, 28–29
  - Cookies
    - defined, 170
    - Web security and, 122–123
  - Costs, security
    - defined, 170
    - risk assessment vs., 1–2, 6
    - risk checklists and, 9–14
  - Crack, defined, 170
  - Crackers
    - always-on connections and, 24
    - assessing risks from, 8, xxi
    - defined, 170
    - encryption strength and, 22–23
    - Internet security and, 101–103
    - updating patches and, 48–49
  - Create Files/Write Data
    - permission, 30
  - Create Folders/Append Data permission, 30
  - Critical data, 170
  - Ctrl-Alt-Del, 170
- D**
- DACL (Discretionary or User Defined ACL), 25
  - DARPANET, 108

- Data
    - assessing risks, 3–4, 6
    - backups, 42
    - classification, 3–4, 9–14
    - defining important, 172
    - protecting, 4
  - DDE (Dynamic Data Exchange), 171
  - Debugging, user privilege for, 36–37
  - Delete permission, 31
  - Delete Subfolders and Files permission, 31
  - Denial of Service. *See* DoS (Denial of Service)
  - Denied Access messages, 39
  - Deny All, Grant Explicit permission
    - defined, 171
    - excessive privileges and, 52–53
    - file/directories and, 33
    - overview of, 39–40
    - vs. Grant All, Deny Explicit, 16–19
  - Device drivers, privilege for
    - loading/unloading, 37
  - DHCP (Dynamic Host Configuration Protocol), 96–97
  - Dial-up connections, 96
  - Digital Subscriber Line (DSL), 96, 171
  - Directories
    - controlling access, 24–25
    - granting permissions, 30–32
    - providing access, 16–19
    - securing NT servers, 71–72
    - user privileges for, 35, 39
  - Discretionary or User Defined ACL (DACL), 25
  - Disk quotas, 37
  - DNS Clients, Windows 2000, 84
  - DNS (Domain Naming System)
    - defined, 171
    - e-mail messages, 110
    - redirecting, 111–112
  - DNS Servers, Windows 2000, 85
  - Domain controllers
    - Domain Controller Account Database, 171
    - user privileges for, 35
    - Windows 2000 service, 85
  - Domain Naming System (DNS). *See* DNS (Domain Naming System)
  - Domain Users, defined, 171
  - Domains, defined, 171
  - DoS (Denial of Service)
    - defined, 171
    - hoaxes and, 156
    - Internet security and, 94
  - Drives
    - defined, 171
    - partitions, 171
    - securing Windows NT 4.0, 56–57
  - DSDM (Dynamic Shared Data Manager), 171
  - DSL (digital subscriber line), 96, 171
  - Dynamic Data Exchange (DDE), 171
  - Dynamic Host Configuration Protocol (DHCP), 96–97
  - Dynamic Shared Data Manager (DSDM), 171
- E**
- E-commerce
    - defined, 171
    - security, 127–128
  - E-mail security, 107–118. *See also* AV (Antivirus) software
    - checklist, 118
    - getting off e-mail lists, 117–118
    - Homestead example, 107
    - how e-mail works, 108–110
    - opening files from unknown sources, 51
    - overview of, 107–108
    - virus/worms, 148
    - weaknesses, attachments, 113
    - weaknesses, DNS redirection, 111–112
    - weaknesses, Read as HTML option, 112
    - weaknesses, scripting issues, 112–113
    - weaknesses, spam, 113–117
    - weaknesses, spoofing, 110–111
  - EFS (Encrypted File System), Windows 2000
    - enabling, 88
    - encryption with, 100

Encryption  
 defined, 171  
 e-mail, 112  
 Internet security and, 99–101  
 overview of, 21–24  
 Quicken, 17–19

Event logs  
 Windows 2000, 84  
 Windows NT, 75

Everyone Else role, network user security, 26

Everyone Full Control permission, sharing files, 40–41

Everyone Read permission, sharing files, 40–41

Exploits, defined, 171

Exposure  
 assessing risk and, 1–2, 9–14  
 defined, 171

**F**

FAT 16/32, 56–57

File infector, viruses, 148

File Replication Service, Windows 2000, 85

File Transfer Protocol (FTP), 161–164, 171

Files  
 auditing, setting, 136–137  
 detecting intruders, 138  
 file extensions, un hiding, 51–52  
 opening from unknown sources, 51–52  
 remote access, 60–61  
 Windows 2000, 87–88  
 Windows NT 4.0, 54–58

Files, network security  
 controlling access/rights, 24–25  
 granting permissions, 30–31  
 NT servers, 71–72  
 sharing, 40–41  
 user privileges for, 35, 39

Filters, junk e-mail, 117–118

Financial data  
 assessing risk to, 4  
 hackers and, 17–19

Firewalls  
 border control with, 46

defined, 172  
 Internet security with, 98  
 personal, 49–50  
 server security with, 68

FreeBSD Security Issues, 161

FTP (File Transfer Protocol), 161–164, 171

Full Control permission, 31, 32

**G**

Grant All, Deny Explicit permission  
 defined, 172  
 Deny All, Grant Explicit vs., 19–21  
 granting file/directory permissions, 33

Groups  
 defined, 172  
 directory permission, 32  
 file permission, 31  
 user, 28–30  
 Windows NT 4.0, 54

Guest account, Windows NT 4.0, 54

**H**

Hack, defined, 172

Hackers  
 always-on connections and, 24  
 assessing risks from, 8, xxi  
 defined, 172  
 getting information from Web sites, 121–122  
 Internet connections and, 94–97  
 Quicken encryption and, 17–19  
 watching you on Internet, 101–103

Hackers, defending against, 131–144  
 attacks and penetrations by, 137–138  
 determining if you are a target, 134  
 extent of current problem, 132–134  
 finding help, 143–144  
 Homestead example, 131–132  
 logging and auditing, 134–137  
 social engineering attacks, 139–141  
 who to blame, 140–143

Happy99.exe worm, 140

Hardware  
 assessing risk of failed, 7

- crackers/hackers and, xxi
  - Help, defense against hackers, 143–144
  - Hoaxes, 155–156
  - Homestead example
    - assessing risk, 1
    - defending against hackers, 131–132
    - e-mail security, 107
    - how to use, xiii
    - Internet security, 93
    - introduction to, xiv-xvi
    - network security, 15–16
    - server security, 67
    - Web security, 119
  - Hotfixes
    - defined, 172
    - overview of, 48
    - staying current on, 47
  - HTML (Hypertext Markup Language), e-mail security
    - avoiding, 151
    - defined, 172
    - turning off Read as HTML, 112
  - HTTP (Hypertext Transfer Protocol), 172
  - Human error
    - data loss and, 7–8
    - Grant All vs. Deny All and, 20–21
  - Hyperlinks
    - defined, 172
    - history of, 120
  - Hypertext Transfer Protocol (HTTP), 172
- I**
- I Love You worm, 148
  - Identity, online
    - identity theft and, 104
    - protecting, 4–5
  - Identity theft, 104, 172
  - IE (Internet Explorer)
    - security settings that Prompt, 125
    - security zones, 123–124
  - IETF (Internet Engineering Task Force), 172
  - IMAP (Internet Mail Access Protocol), 108–109, 172
  - Important data, 172
  - Infection, virus, 146
  - Integrated services digital network (ISDN) connection, 96, 172
  - Internal clocks, user privileges, 35–36
  - Internet Engineering Task Force (IETF), 172
  - Internet Explorer (IE)
    - security settings that Prompt, 125
    - security zones, 123–124
  - Internet Mail Access Protocol (IMAP), 108–109, 172
  - Internet (net)
    - comparing Web with, 120
    - defined, 171
  - Internet Protocol Security (IPSec), 84–87, 173
  - Internet security, 93–106. *See also*
    - Hackers, defending against advanced measures, 98–101
    - basic measures, 97
    - checklist, 105
    - Homestead example, 93
    - privacy issues, 103–105
    - types of connections, 93–97
    - who is watching you, 101–103
  - Internet service provider (ISP), 172
  - IP addresses, static vs. dynamic, 96–97
  - IPSec (Internet Protocol Security), 84–87, 173
  - ISDN (integrated services digital network) connection, 96, 172
  - ISP (Internet service provider), 172
- J**
- JavaScript, 173
  - Junk mail. *See* UCE (unsolicited commercial e-mail)
- K**
- Kerberos Key Distribution Center, Windows 2000, 85
  - Keys, encryption
    - lengths of, 22
    - overview of, 23–24
    - protecting Registry with, 58–60
    - technology for, 100

**L**

Laws  
 anti-spam, 116  
 banner ads and, 121  
 getting off e-mail lists, 117

Layered security, networks, 16–19

Legal Notice, displaying at logon, 61–62

Linux Security Issues, 161

List Folder/Read Data, permission, 30

Local Security Authority (LSA), 173

Local Users and Groups System Tool,  
 Administrative tools, 28–30

Locked pages, privilege for, 37

Logging  
 appropriate levels of, 134–137  
 turning on, 41

Logical Disk Manager, Windows  
 2000, 84

Logon  
 as batch job, 38  
 displaying Legal Notice, 61–62  
 Internet security and, 97  
 Windows NT 4.0, 54  
 Windows NT servers, 78–79

LoveLetter worm, 148

LSA (Local Security Authority), 173

**M**

Macro virus infection, 148

Mailing lists, security information,  
 160–161

MBR (Master Boot Record), viruses  
 and, 147, 173

Microsoft. *See also* Windows  
 operating system management, 81  
 server security checklist, 88

Microsoft Developer Network  
 (MSDN), 81

Microsoft Security Bulletin, 143

Mitigation  
 assessing risk and, 1–2  
 defined, 173  
 risk checklists and, 9–14

Modify permission  
 directories, 32  
 files, 31

Moore's Law, 22

MSDN (Microsoft Developer  
 Network), 81

Multi-homing, 69, 173

**N**

NAT (network address translation),  
 99, 173

National Infrastructure Protection  
 Center (NIPC), 47

Natural disasters, assessing risk, 7

Navigation bars, Web page security, 126

Net. *See* Internet

Net Logon, Windows 2000 service, 85

Network address translation (NAT),  
 99, 173

Network Interface Card (NIC), 173

Network security, 15–44  
 access/rights, defining, 24–25  
 checklist for, 42–43  
 data backups, 42  
 denying access, 39–40  
 encryption or clear, 21–24  
 file/directory access, 30–33  
 Grant All vs. Deny All, 19–21  
 grouping users, 28–30  
 Homestead example, 15–16  
 in-depth or layered, 16–19  
 rights/privileges, granting, 34–39  
 sharing files, 40–41  
 users and their roles, 25–28

NIC (Network Interface Card), 173

Nimda worm, 148

NIPC (National Infrastructure  
 Protection Center), 47

NT LM Service Provider, Windows  
 2000, 85

NTBugTraq, 144

NTFS, Windows NT 4.0, 56

**O**

Obfuscation, 18, xviii

Open Systems Interconnection model  
 (OSI), 70, 173

Operating System Directory, Windows,  
 57–58

OS (operating systems)  
 assessing security risk of, xxii  
 Microsoft resources for managing, 81

user privileges for, 35  
 vulnerabilities to hackers, 133  
 OSI (Open Systems Interconnection)  
 model, 70, 173  
 Other data, defined, 173

## P

P3P (The Platform for Privacy Preferences Project), 104–105, 174  
 Packet filtering, 69, 173  
 Packets, defined, 173  
 Pagefiles, 36, 173  
 Passwords  
 cookies and, 122–123  
 Internet security and, 97  
 overview of, 25  
 protecting, 53  
 Patches  
 browser security with, 125–126  
 overview of, 47–49  
 Windows NT servers, 71  
 Payload, viruses, 146  
 Performance data, Windows NT  
 servers, 77–78  
 Permissions  
 denying access, 39–40  
 Grant All vs. Deny All, 19–21  
 granting access, 57  
 list of file/directory, 30–33  
 Registry protection, 58–60  
 sharing data, 40–41  
 Personalization, Web sites, 121, 122  
 PGP2 (Pretty Good Privacy), 100  
 Phreak, defined, 173  
 Physical security, defined, 174  
 Plain text, e-mail security, 151  
 The Platform for Privacy Preferences  
 Project (P3P), 104–105, 174  
 Plug & Play, Windows 2000 service, 84  
 Polymorphic, viruses as, 146  
 POP3 (Post Office Protocol 3),  
 108–109, 174  
 Ports, 174  
 Power surges, 7, 51  
 Privacy, online  
 Internet security issues, 103–105  
 protecting, 5  
 Web security and, 121–122

Private keys, defined, 174  
 Privileges  
 browsing Web and, 156  
 defined, 34, 174  
 Domain vs. Workgroup  
 computers, 34  
 granting excessive, 52–53  
 User Rights and, 25, 27, 34–39  
 Windows NT 4.0, 58  
 Process, defined, 174  
 Profiling (performance sampling),  
 privilege for, 38  
 Prompt, Internet Explorer security set-  
 tings, 125  
 Protected Storage, Windows 2000 ser-  
 vice, 84  
 Protocol isolation, 69, 174  
 Protocols, defined, 174  
 Proxy servers  
 defined, 174  
 Internet security and, 98–99  
 server security and, 68–69  
 Public keys, defined, 174

## Q

Quicken program, hackers and,  
 17–19

## R

RAM memory, 38, 174  
 Read and Execute permission, 31, 32  
 Read as HTML, E-mail security, 112  
 Read Attributes permission, files/di-  
 rectories, 30  
 Read Extended Attributes permission,  
 files/directories, 30  
 Read permission, 31, 32  
 Registry  
 defined, 174  
 keys, Windows NT server, 76–77  
 overview of, 56  
 protecting, 58–60  
 remote access, granting, 61  
 Registry Editor  
 displaying Legal Notice before Log-  
 On, 62  
 protecting Registry with, 58–60  
 Security Configuration Editor, 63

- Relative security
    - defined, 174
    - encryption depending upon, 23
  - Remote Procedure Call (RPC), 84, 174
  - Remote Registry Service, Windows 2000, 84
  - Replaceable Data, defined, 174
  - Request for Comment (RFC), 175
  - The Resource Kit, 81
  - Resources. *See* Web site resources
  - RFC (Request for Comment), 175
  - Rights and Privileges, User
    - defined, 176
    - granting, 34–39
    - granting excessive, 52–53
    - overview of, 25
  - Rights, network security and, 16–19
  - Risk, assessing, 1–14
    - acceptable risk, 5–6
    - Administrator accounts, 27
    - areas that need protection, 4–5
    - checklists for, 9–14
    - data classification, 3–4
    - Homestead example, 1
    - overview of, 1–2
    - protecting Registry, 58–59
    - questions for, xxii
    - what/who you are protecting from, 7–9
  - Risk, defined, 175
  - Role-Based Access Model, 175
  - Roles
    - defined, 175
    - users and, 26–28
  - Routing, defined, 175
  - RPC Locator, Windows 2000, 85
  - RPC (Remote Procedure Call), 84, 174
  - RunAs service, Windows 2000, 84
- S**
- SACL (System Defined ACL), 25
  - Sandboxes, 125
  - Satellite system connection, 96
  - SCE (Security Configuration Editor), 63
  - Scheduling priority
    - defined, 175
    - user privilege for increasing, 37
  - Screen-savers, password-protecting, 53
  - Script kiddies
    - assessing risks from, 8
    - defined, 175
    - Internet security and, 101–103
  - Scripting
    - Active Content on Web, 156–157
    - e-mail security, HTML and, 112, 151
    - e-mail security, overview of, 112–113
  - Secure channels,, 126
  - Secure channels, 175
  - Secure Sockets Layer (SSL), 126, 175
  - Security
    - assessing, xxi-xxii
    - key concepts of, xvii-xviii
    - terminology, 169–177
  - Security Accounts Manager, Windows 2000, 84
  - Security audits
    - defined, 175
    - user privilege for generating, 37
    - user privilege for managing, 38
  - Security Configuration Editor (SCE), 63
  - Security Focus Web site, 144
  - Security in-depth, 16–19, 175
  - Security Log, accessing/viewing, 137
  - Security Policy Settings, Windows 2000, 82–84
  - Security tab
    - Internet Explorer, 123–124
    - Windows NT 4.0, 55
  - Security zones
    - browser, 123–125
    - defending vs. threats with, 156–157
  - Self-replication, defined, 146
  - Servers, 67–92. *See also* Windows NT, server security
    - checklist for securing, 88–92
    - defined, 175
    - Homestead example, 67
    - overview of, 67–68
    - where to start, 68–71
    - Windows 2000, 82–88
  - Service packs. *See* SPs (Service packs)
  - Shares
    - creating shared objects, 36
    - granting remote access, 60–61
    - sharing files, 40–41



- Signing
    - defined, 175
    - overview of, 100
  - SMTP (Simple Mail Transfer Protocol), 108–109, 175
  - SNMP (Simple Network Management Protocol), 175
  - Social engineering
    - defined, 175
    - overview of, 139–140
    - signs of, 141
  - Software. *See also* Antivirus software
    - assessing risk of failed, 7
    - assessing risk of replaceable, 3
    - opening/downloading, 151
    - for personal firewalls, 98
    - security weaknesses in, 140–143
    - staying current on, 47–48
  - Spam. *See* UCE (unsolicited commercial e-mail)
  - Spammer, defined, 176
  - Spoofing, E-mail security, 110–111
  - SPs (Service packs)
    - defined, 175
    - overview of, 48
    - securing NT servers, 71
    - staying current with, 47, 49
  - SSL (Secure Sockets Layer), 126, 175
  - Stealth/stealthy, defined, 146
  - Subsystems, 176
  - Symbolic links, 176
  - SysKey, Windows 2000, 85
  - System Defined ACL (SACL), 25
  - System security, defined, 46
  - System time, user privileges, 35–36
- T**
- Take Ownership permission, files/directories, 31
  - Tampering, assessing risks of, 7
  - TCP/IP (Transmission control protocol/Internet protocol)
    - defined, 176
    - filtering, 176
    - Internet security and, 93–95
    - server security, overview of, 69
    - server security, Windows 2000, 86–87
    - server security, Windows NT, 80
  - TechNet, 81, 176
  - Telnet, defined, 176
  - Testing, Internet security, 101
  - Threads
    - debugging programs and, 36–37
    - defined, 176
  - Tiger teams, 139, 176
  - Token objects
    - defined, 176
    - user privilege for creating, 36
    - user privilege for modifying, 38–39
  - Tools
    - editing security and Registry, 62–64
    - security analysis, 101
    - Windows 2000 server, 87–88
  - Traverse checking, 176
  - Traverse Folder/Execute Files permission, files/directories, 30–32
  - Trojan horses, 145–158
    - active content on Web and, 156–157
    - affect of, 149–150
    - defined, 147, 176
    - Homestead example, 145–146
    - Internet security and, 94–95
    - minimizing risk of exposure, 150–155
    - overview of, 146–149
    - protection from, 51
    - security checklist for, 157
- U**
- UCE (unsolicited commercial e-mail)
    - assessing risks from, 8
    - defined, 176
    - overview of, 113–117
  - Updates, virus protection, 150
  - UPS (Uninterruptible Power Supply), 51
  - URLs, Web page security and, 126–127
  - User Rights and Privileges
    - defined, 176
    - granting, 34–39
    - granting excessive, 52–53
    - overview of, 25
  - Usernames, 25

Users, network security  
 defining access and rights, 24–25  
 Grant All vs. Deny All, 19–21  
 granting rights/privileges, 34–39  
 grouping, 28–30  
 roles of, 25–28

**V**

VBScript, 177  
 Vendors, buying online, 128  
 Virtual memory, 177  
 Viruses, 145–158. *See also* AV  
 (Antivirus) software  
 active content on Web and, 156–157  
 affect of, 149–150  
 assessing risks of, 7  
 defined, 177  
 Homestead example, 145–146  
 minimizing risk of exposure,  
 150–155  
 overview of, 146–149  
 protection from, 51  
 security checklist, 157  
 Web resources for, 166

**W**

W3C (World Wide Web Consortium), 177  
 Web security, 119–130  
 Active Content and, 156–157  
 browsers and, 123–126  
 checklist for, 119–121  
 cookies and, 122–123  
 defining WWW, 119–121  
 e-commerce and, 127–128  
 Homestead example, 119  
 Web pages and, 126–127  
 what they know about you, 121–122  
 Web site resources, 159–166  
 antivirus-related, 154–155, 165–166  
 computers incident response cen-  
 ters, 164–165  
 DHCP, 97  
 e-mail, encryption and security, 114  
 editing security and Registry, 63  
 firewalls, 50, 98  
 hacker-related, 143–144  
 mailing lists, 160–161

Microsoft server security  
 checklist, 88  
 patches, 47  
 The Platform for Privacy  
 Preferences Project, 104–105  
 Web and FTP sites, 161–164  
 worm infections, 148  
 Windows 2000  
 Computer Management applet,  
 28–30  
 Encrypted File System, 100  
 Professional, compared with  
 Windows NT 4.0, 62–64  
 Professional, workstation security  
 checklist, 64–66  
 User Rights for, 34–39  
 Windows 2000, server security, 82–88  
 IPSec filtering, 85–87  
 minimum services, 84–85  
 Security Policy Settings, 82–84  
 special files, 87–88  
 SysKey, 85  
 tightening TCP/IP, 87  
 using Encrypting File System, 88  
 Windows 9x  
 Administrator privileges on, 27  
 antivirus software, 50  
 granting rights/privileges in, 34  
 grouping users, 28  
 limitations of, 26  
 personal firewalls, 49–50  
 safe computing practices, 50–53  
 third-party software and, 54–61  
 workstation security checklist, 64  
 Windows ME  
 Administrator privileges on, 27  
 granting rights/privileges on, 34  
 grouping users and, 28  
 limitations of, 26  
 Windows NT, 54–61  
 compared with Windows 2000 secu-  
 rity, 62–64  
 granting access to files, 54–58  
 grouping users on, 28  
 list of User Rights for, 35–39  
 user privileges in, 34–39  
 users and groups, 54

- workstation security checklist, 64–66
  - Windows NT, server security, 71–81
    - access to event logs, 75
    - AllowedPaths Key(s) in Registry, 80–81
    - deleting administrative shares, 75–76
    - disabling Log-on caching, 78–79
    - disabling unneeded services, 74–75
    - false administrator accounts, 80
    - files/directories, 71–72
    - patches/service packs, 71
    - protecting performance data, 77–78
    - Registry keys, 76–77
    - removing unneeded subsystems, 77
    - setting account policies, 73–74
    - TCP/IP security, 80
    - turning on auditing, 72–73, 79–80
  - Windows Resource Kit, 177
  - Windows Scripting Host (WSH), 151–152, 177
  - Windows systems, securing, 45–66
    - comparing Windows 2000
      - Professional with NT 4.0, 62–64
    - general practices, 46–49
    - Homestead example, 45
    - small businesses and, 61–66
    - specific mailing list for, 161
    - using this book and, xx–xxi
    - Windows 2000 Professional, 64–66
    - Windows 9x, 49–53
    - Windows NT 4.0, file access, 54–58
    - Windows NT 4.0, user privileges in, 34–39
    - Windows NT 4.0, users and groups, 54
    - Windows NT 4.0, users groups, 28
    - Windows NT 4.0, workstation security checklist, 64–66
    - Windows XP, 64–66
  - Workgroups, 34
  - Workstations
    - adding to domains, 35
    - checklist for securing, 64–65
    - Windows 2000, 84
  - World Wide Web Consortium (W3C), 177
  - Worms
    - defined, 147
    - e-mail, 148
    - social engineering and, 140
  - Write Attributes permission, files/directories, 31
  - Write permission, 31, 32
  - WSH (Windows Scripting Host), 151–152, 177
  - WWW (World Wide Web). *See* Web security
- Z**
- Zone Alarm, firewall, 50

