

# Index

## SYMBOLS AND NUMERICS

### \$ (dollar sign)

- indicating computer account, 115
- indicating hidden shares, 121

### 3DES (Triple DES), 299, 464

### .386 files, 202

### 2004 Computer Crime and Security Survey (FBI), 5

### 2004 ICSA Labs Tenth Annual Computer Virus Prevalence Survey, 5, 391

## A

### access control, 80–82. *See also* authentication; NTFS permissions

### Access Control Entry (ACE) permissions, 126

### Access Control List (ACL), 126

### access mask, 118

### Access (Microsoft), file vulnerabilities in, 193, 199

### access module shortcut files, 199

### access token (security token), 88, 117–119, 126

### Access11.adm template, 516

### account lockouts

- enabling, 185–186
- group policy settings for, 493

### Account Operators group, 74, 86, 102

### accounting phase, access control, 81

### accounts. *See also specific accounts*

- built-in, list of, 99–101
- computer accounts
  - definition of, 115–116
  - password attacks on, 177–179

### highly-privileged accounts

- password protections for, 186–187
- renaming, 73–75, 186
- service accounts, 260–263, 292–293

### ACE (Access Control Entry) permissions, 126

### ACL (Access Control List), 126

### action-based groups, 95–96

### Active Directory. *See also* group policy

- accessing with LDAP, 525
- applying group policy in, 481, 482–483
- baseline security policy for, 539
- container objects in, 481
- definition of, 519–520
- domains in, 521–523
- finding GUID for objects in, 82
- forests in, 521
- FSMO (Forest Single Master Operations) roles, 523–524
- group policy objects in, 481, 482–483
- guidelines for, 536–542
- organizational units in
  - default, list of, 520
  - definition of, 481, 520–521
  - role-based structure for, 537–538
- partitions in, 525
- parts of, 525
- RBAC (Role-Based Access Control) for, 537
- role-based incremental security policy for, 539
- role-based OU structure for, 537–538
- sites in, 524
- trusts in, 522–523

### Active Directory Domains and Trusts console, 482

### Active Directory Integration, for IIS, 446

## **Active Directory mixed-mode, 96**

**Active Directory Users and Computers console, 96, 482**

**Active Server Pages (ASP), for IIS, 447, 449**

**Active Sites and Services console, 482**

## **ActiveX controls**

IE settings for, 368–370, 375–376

IE 7 features restricting, 349

kill bit for, 335–336

vulnerabilities of, 29, 199

## **Ad-Aware (Lavasoft), 70**

**add-ons, exploitation of, 364–365**

**address lookups, anti-spam software using, 407–409**

**.ade files, 193**

**Administrative templates, group policy settings in, 481, 485, 515–517**

## **Administrator account**

compared to other administrators, 88

DCPromo effects on, 100

definition of, 99–100

as DRA (Data Recovery Agent), 100

password protections for, 186–187

renaming, 73–75, 186

security options for, 502–503

SID enumeration identifying, 75

## **Administrators group**

computer accounts in, 116

default GPO permissions for, 535

definition of, 102

not allowing end users to log in as, 329–330, 366

not including end users in, 58–63, 246

password protections for, 186–187

renaming, 74, 186

SID for, 86

**.adp files, 193**

## **ADS (Alternate Data Streams)**

definition of, 214–215

vulnerabilities of, 21, 215–216

**Adsiedit.msc console, 82**

**Advanced Windows Password Recovery program, 181**

**adware, 18–19**

**AES (Advanced Encryption Standard), 299, 464**

**AGULP method, 97–99**

**AH (Authentication Header) protocol, 298, 299**

**Aim URI handler, 249**

**Alerter service, 268**

## **Allow permissions**

overriding Deny permissions, 128

setting, 122–123

**%ALLUSERSPROFILE% folders, 28**

## **Alternate Data Streams (ADS)**

definition of, 214–215

vulnerabilities of, 21, 215–216

**.ani files, 193, 247**

**Anonymous authentication, IIS, 429, 431, 449**

**anonymous enumeration, 6, 75**

**Anonymous Logon group, 85, 103, 113**

**Anonymous SID, 113**

**ANSI-bombs, 189**

**Ansi.sys file, 189**

**Anti-Phishing Workgroup, 5**

**anti-spam software. See also spam**

client-based solutions for, 417

definition of, 69–70

gateway appliances or software for, 415–416

hosted services for, 414–415

methods used by

address lookups, 407–409

comparisons of, 414

distribution analysis, 410

fingerprinting, 413

human analysis, 413

message analysis, 411–413

rate controls, 409–410

real-time blacklists (RBLs), 410–411

server software for, 416

**anti-spyware software, 70**

**antivirus software. See also viruses**

best practices for, 68–69

effectiveness of, 12, 57

failure of, assuming, 55

for incoming e-mail, 406–407

multiple, using, 57

**Append Data permission, 125, 126**

**application control. See software restriction policies**

**Application Experience Lookup Service, 268**

**application files. See executable files; software**

**Application Layer Gateway Service, 268**

**Application Management service, 268**

**application pools, IIS, 422–425, 453–455**

**Application Server Console, IIS, 444**

**Apply Group Policy permission, for GPOs, 534**

**.arc files, 194**

**archive files, vulnerabilities of, 20, 199, 200, 202. See also compressed files**

**.arj files, 194**

## **Aronoff, Andrew**

IERESET.INF attack proposal, 24, 210

registry vulnerabilities discovered by, 36, 37, 39, 43, 45–48, 244–246

**ARP spoofer, 168**

.asf files, **194, 247**

**ASP (Active Server Pages), for IIS, 447, 449**

**ASP.NET, for IIS, 444, 449**

**ASP.NET State Service, 283**

#### associations

file associations

hidden, 212

high-risk, blocking, 247–249

permission to change, 250–251

in registry, 231–235

vulnerabilities of, 30, 38, 39, 203, 243

in Windows Explorer, 235

security associations (SAs), IPsec, 300

.atf files, **194**

#### attachments

blocking, 398–401

malicious, 391–392

**attack surface, lessening, 253**

**attack vectors, decreasing, 57**

#### attackers

dedicated attackers

compared to automated malware, 4–7

defeating, inability to, 52

defending against, 6–7

forensic analysis of attacks by, 10

methodology used by, 8–10

types of, 10–11

insider attacks, 17

knowing, importance of, 3

**attacks. See also defense strategy; malware; password cracking**

in IE (Internet Explorer)

browser interface manipulation, 364

buffer overflow attacks, 357

cookie manipulation, 363–364

cross-site scripting, 357–358

directory transversal attacks, 362

file execution attacks, 361–362

malicious content, 363

MIME type mismatches, 363

plug-in exploits, 364–365

URL spoofing, 354–357

zone manipulation, 358–361

increasing number of, 52

prevalence of, 4–7, 13–14, 19, 51

types of

adware, 18–19

automated, 4–7, 11–14

dedicated attacker, 4–7, 8–11, 52

directory transversal attacks, 18, 362

insider attacks, 17

local, 7–8

obscurity attacks, 17–18, 355–357

pharming attacks, 18–19, 397, 418

phishing attacks, 5–6, 18–19, 354–357, 396–397

physical attacks, 17, 56, 70–71

remote, 7–8, 14–17

social engineering, 18

spam, 18–19, 393–396

spyware, 6, 18–19

#### auditing

group policy settings for, 494–496

managing, 501

for Object Access, 224–225

as part of accounting phase, 81

**auditing permissions, 126**

**Austrumi, 163**

#### Authenticated Users group

computer accounts in, 115, 116

default GPO permissions for, 535

definition of, 103

replacing Everyone group with, 219

SID for, 85

Windows trusts and, 117

**authentication. See also passwords**

of e-mail, 417–418

IE settings for, 375, 377, 381–382

IIS (Internet Information Server), 182, 428–433, 449–450

for IPsec rules, 308–309

logon process for, 159–160

mistakes in, vulnerabilities caused by, 182–183

as part of access control, 80

password hashes protected during, 152

Password Reset Diskette, 182

protocols for

choosing, 156–159

Kerberos authentication, 154–156, 157

LM authentication, 152–153, 183–184

NTLM authentication, 153, 450

NTLMv2 authentication, 153–154

token-based authentication, 187

two-factor authentication, 187

**Authentication Header (AH) protocol, 298, 299**

**authorization phase, access control, 81**

**Autoexec.bat file, 22, 132**

**Autoexec.nt file, 22**

**automated malware. See malware**

**Automatic Updates, 65**

**Automatic Updates service, 268**

**automation of defense strategy, 58**  
**AutoPreview pane, disabling, 404–405**  
**auto-run application files, 21**  
**AUTORUN.INF file, 22**  
**Autoruns program (Sysinternals), 256**

## B

**Background Intelligent Transfer Service (BITS), 269, 445**  
**Backup Operators group, 86, 103–104**  
**backups**  
    allowing access to, 497–498  
    for EFS, 471–476  
    restoring, security options for, 502, 503  
**Barracuda Spam Firewall, 69–70**  
**.bas files, 194**  
**Baseline Security Analyzer, Microsoft (MBSA), 65**  
**Basic authentication, IIS, 430, 431, 432, 449**  
**.bat files, 194, 247**  
**batch files, 23, 194, 247**  
**Batch group, 84, 104**  
**batch job**  
    allowing logons as, 500  
    denying logons as, 499  
**Bayesian filtering, anti-spam software using, 412–413**  
**Beagle.AV worm, 195, 200, 391**  
**BeatLM program, 168**  
**BHOs (Browser Helper Objects), exploitation of, 364–365**  
**BIOS, password-protecting, 71**  
**birthday attacks, 173**  
**BITS (Background Intelligent Transfer Service), 269, 445**  
**blacklists, anti-spam software using, 410**  
**Blaster worm, 8, 253**  
**blocked inheritance, for GPOs, 532**  
**Blowfish encryption, 299**  
**.bmp files, 194**  
**Bookmarker trojan, 41**  
**books. See publications**  
**boot files, permissions for, 135**  
**Boot Information Negotiation Layer service, 283**  
**boot sectors, viruses infecting, 12**  
**booting**  
    boot-up passwords, 71  
    restricting to primary hard drive, 71  
**Boot.ini file, 23, 132**  
**Bootsec.dos file, 23**  
**botnets, 13–14**  
**bots (spam bots), 5, 395, 409, 419**

**Bradley, Susan (The Complete Patch Management Book), 64**  
**Brett Hill's IIS Answers.com, 456**  
**Bropia trojan, 34**  
**Browser Helper Objects (BHOs), exploitation of, 364–365**  
**browser interface manipulation, 364**  
**browsers. See also IE (Internet Explorer)**  
    cell-phone-based, 350  
    Firefox browser, 52–53, 350, 351–352  
    Konqueror browser, 350  
    Lynx browser, 350, 351  
    Mozilla browser, 350, 351  
    Netscape browser, 350  
    Opera browser, 350, 351  
    Safari browser, 350  
**brute-force attacks for password cracking, 171–172**  
**Brutus program, 164**  
**buffer overflow attacks**  
    definition of, 15  
    file flaws allowing, 191  
    risks associated with, 217–218  
    services and, 254  
    using IE (Internet Explorer), 357  
**built-in groups, list of, 102–113**  
**Built-in OU, 520**  
**built-in users, list of, 99–102**  
**bulk e-mailing programs, 394–395**  
**bullet-proofing, 395**

## C

**CA (certification authority), 309**  
**.cab files, 194**  
**cabinet archive files, 194**  
**cached credentials, password attacks on, 176–177**  
**Cachedump utility, 176**  
**Cain & Able program, 16–17, 166, 169, 179**  
**Callto URI handler, 249**  
**Carnegie Mellon University CERT Coordination Center, 51**  
**Cascading Style Sheet files, 195**  
**CastleCop's listing of ActiveX controls, 335**  
**.cbl files, 194**  
**.cbm files, 194**  
**.cbo files, 194**  
**CD-ROM access, security options for, 504**  
**.cer files, 195**  
**CERT Coordination Center, Carnegie Mellon University, 51**  
**Cert Publishers group, 85, 104**

- Certificate authentication, IIS, 432, 449, 450**
  - Certificate Auto-enrollment in Windows XP, 478**
  - certificate exception rules, SRP, 222, 341**
  - Certificate Services (Microsoft)**
    - CERTSVC\_DCOM\_ACCESS group created by, 104
    - for EFS, 475–476
    - operating systems available in, 283
  - Certificate Trust List files, 195, 201**
  - certificates**
    - EFS, 462–464
    - IE settings for, 372, 383–384
  - certification authority (CA), 309**
  - CERTSVC\_DCOM\_ACCESS group, 104**
  - challenge-response mechanism, 152**
  - Change permission, 119–121**
  - Change Permissions permission, 125, 126**
  - Character Map, viewing Unicode characters in, 142**
  - .chm files, 195, 247**
  - Cipher.exe program, 461, 472**
  - CipherTrust, zombie nets tracked by, 13–14**
  - Cisco IOS 12.x operating system, 53**
  - ClearCredCache program, 179**
  - ClipBook service, 269**
  - CLSID (Class ID), 83, 335–336**
  - Cluster Services, 284**
  - .cmd files, 195, 248**
  - Code Red worm, 419**
  - collision, in hash algorithm, 147**
  - COM+ access, for IIS, 444**
  - COM+ Event System service, 269**
  - .com files, 195, 248**
  - COM objects**
    - registry listing, 42
    - unregistering, 332–334
  - COM+ System Application service, 269**
  - command and control trojan, 13**
  - command files, vulnerabilities of, 23, 195, 199, 248**
  - Command.com file, 23**
  - Commercial Guardian Monitor spyware, 46**
  - Common.adm template, 515**
  - companion viruses, 12**
  - The Complete Patch Management Book (Bradley, Susan and Anne Stanton), 64**
  - compressed files. *See also* archive files**
    - EFS not encrypting, 460, 477
    - vulnerabilities of, 197, 203
  - computer accounts**
    - definition of, 115–116
    - password attacks on, 177–179
  - Computer Browser service, 269**
  - Computer Configuration section of group policy, 487**
  - Computename\$ group, 116**
  - Computers OU, 520**
  - Conf.adm template, 515**
  - Config.nt file, 23**
  - Config.sys file, 23, 132**
  - configuration files, 198, 201. *See also* registry**
  - Configuring Application Isolation on Windows Server 2003 and Internet Information Services (IIS) 6.0, 456**
  - constrained delegation, 92, 156, 471**
  - container objects, in Active Directory, 481. *See also* organizational unit (OU), in Active Directory**
  - contest, hacking, May 2005, 10–11**
  - Control Panel Applet files, 195**
  - cookie manipulation, 363–364**
  - CoolWeb Search Adware, 40**
  - .cpl files, 195**
  - Create Child Objects permission, for GPOs, 534**
  - Create Files permission, 124, 126**
  - Create Folders permission, 125, 126**
  - Create Link permission, registry keys, 242**
  - Create Subkey permission, registry keys, 241**
  - Creator Authority, 84**
  - Creator group, 84, 104, 114**
  - Creator Group Server account, 84**
  - Creator Owner group, 84, 104, 114**
  - Creator Owner Server account, 84**
  - CredDump program, 180**
  - Credential Manager, password attacks with, 179–181**
  - credentials, cached, password attacks on, 176–177**
  - crimeware, 19. *See also* malware**
  - cross-site scripting (XSS)**
    - in e-mail, 393
    - in IE (Internet Explorer), 357–358
    - malware in, 21
  - cross-zone attacks, IE, 362**
  - Crypt32.dll file, 352**
  - Cryptographic Services, 270**
  - cryptography. *See* encryption**
  - .cs files, 191, 202, 249**
  - Cscript.exe program, 191**
  - .css files, 195**
  - .ctl files, 195**
  - .cur files, 196, 248**
  - cursor graphic files, 248**
- ## D
- DAC (discretionary access control), 81, 126**
  - DACL (Discretionary Access Control List), 126**
  - Daqa trojan, 73**
  - Data Decryption Field (DDF), 465**
  - data, defending against attacks of, 56**

**Data Encryption Standard (DES), 299**

**Data Encryption Standard XOR (DESX), 464**

**Data Protection API (DPAPI), 180**

**Data Recovery Agent (DRA) account, 74, 100**

**Data Recovery Field (DRF), 465**

**databases. See also Active Directory**

Access database, 199

attacks on, 6

SAM password database, 150, 161

Security Association Database (SAD), 300

security policy database, IPSec, 299

.dbg files, **196, 248**

**DCOM applications, 105**

**DCOM Server Process Launcher service, 270**

**DCPromo, Administrator account and, 100**

**DDF (Data Decryption Field), 465**

**De Clercq, Jan (*Windows Server 2003 Security Infrastructures*), 86**

**debug files, 196, 248**

Debug.exe program, **189, 190**

**debugger, allowing use of, 499**

**dedicated attackers**

compared to automated malware, 4–7

defeating, inability to, 52

defending against, 6–7

forensic analysis of attacks by, 10

methodology used by, 8–10

types of, 10–11

**Default Domain Controllers Policy, 528**

**Default Domain Policy, 528**

**Default hive, registry, 229**

**default passwords, 146**

**Default Recovery Agent (DRA), for EFS, 473–475**

**defense strategy**

automation of, 58

conventional

anti-spam software, 69–70

anti-spyware software, 70

antivirus software, 68–69

host-based firewall, 65–68

patches, keeping up-to-date, 63–65

physical security, 70–71

TCP/IP stack, hardening, 71–73

users not having administrator privileges, 58–63

defense-in-depth principle, 55, 56–57

host-based defense, 55–56

principles of, 52–58

security-by-obscurity, 54

tradeoffs in, 53

unconventional

highly-privileged accounts, renaming, 73–75

services, running on non-default ports, 75–76

software, installing to non-default folders, 76

usability affected by, 53

**defense-in-depth principle, 55, 56–57**

**Define virus, 12**

**delegation**

constrained delegation, 92, 156, 471

definition of, 92–94

in IIS 7, 436

trusted for delegation, 470–471, 499–500

**Delete Child Objects permission, for GPOs, 534**

**Delete permission, 125, 126**

**Delete permission, registry keys, 242**

**Delete Subfolders and Files permission, 125, 126, 128**

**Dell Computers, survey by, 6**

**denial-of-service (DoS) attacks**

account of (Gibson), 15

in archive files, 20

definition of, 15

with IPSec, 322

LAND attack, 15

services increasing risk of, 254

**Deny Delete permission, 128**

**Deny permissions**

overriding Allow permissions, 128

setting, 122–123

**deny-by-default file attachment blocking, 398**

**deny-by-default software execution policy, 325–326**

**DES (Data Encryption Standard), 299**

.desklink files, **199**

**desktop, defense deployed on, 55–56**

**desktop icons, RunAs feature used with, 60**

Desktop.ini file, **24**

**DESX (Data Encryption Standard XOR), 464**

**detection bypass, in archive files, 20**

**device drivers, allowing loading and unloading of, 500**

**devices, security options for, 504–506**

**DHCP Administrators group, 104**

**DHCP Client service, 270**

**DHCP Server service, 270**

**DHCP Users group, 105**

.dhtml files, **197**

**Dialup group, 84, 105**

**Dial-up List (DUL), 410**

**dictionary-based attacks, 144, 145–146, 172–173**

**Diffie-Hellman protocol, 300**

**Digest authentication, IIS, 430, 431, 432, 450**

**Digest Authentication protocol**, 85

**directories**. *See* folders

**directory service**, 519. *See also* Active Directory

**directory service data**, synchronizing, 502

**Directory Services Restore Mode Administrator account**, 100

**directory transversal attacks**, 18, 362

**discretionary access control (DAC)**, 81, 126

**Discretionary Access Control List (DACL)**, 126

**Distributed COM Users group**, 86, 105

**Distributed File System service**, 270

**Distributed Link Tracking Client service**, 270, 287

**Distributed Link Tracking Server service**, 270, 287

**Distributed Transaction Coordinator service**, 271

**distribution analysis**, anti-spam software using, 410

**distribution groups**, 96

**Dllhost.exe process**, 422

**DLLs**

- DLL hell, 12
- unregistering, 332–334
- vulnerabilities of, 196

**DNS Admins group**, 105

**DNS black lists**, 410–411

**DNS Client service**, 271

**DNS lookups**, anti-spam software using, 408

**DNS namespace**, 519

**DNS security**, 418

**DNS Server service**, 271, 287

**DnsUpdateProxy group**, 105

- .doc files, 196

**docking station**, security options for, 501, 503

**Document Template files**, 196

**Document Template files**, Microsoft, 196

**Documents and Settings folder**, 132

**dollar sign (\$)**

- indicating computer account, 115
- indicating hidden shares, 121

**Domain Administrator account**, 85, 99–100

**Domain Admins group**

- default GPO permissions for, 535
- definition of, 105
- protecting, 74
- SID for, 85

**domain computer accounts**, password attacks on, 177–179

**Domain Computers group**

- computer accounts in, 115
- definition of, 106
- SID for, 85

**Domain Controllers group**

- computer accounts in, 116
- definition of, 106
- SID for, 85

**Domain Controllers OU**, 520

**Domain Guest account**, 85, 100

**Domain Guests group**, 85, 106

**Domain Local groups**, 96, 97

**Domain Naming Master**, FSMO role, 523

**Domain Users group**, 85, 106

**domains**

- in Active Directory, 521–523
- adding computers to, policy settings for, 497
- password attacks on, 177–179

**DoS attacks**. *See* denial-of-service attacks

**DOS batch files**, 194, 247

**DOSSTART.BAT file**, 24

- .dot files, 25, 196

**Downlevel Client Support**, for IIS, 446

**downloading files**, IE settings for, 370, 376, 380

**Download.Ject trojan**, 38

**DPAPI (Data Protection API)**, 180

**DRA (Data Recovery Agent) account**, 74, 100

**DRA (Default Recovery Agent)**, for EFS, 473–475

**DRF (Data Recovery Field)**, 465

**driver files**, 201

**driver installation**, security options for, 504

- .dsm files, 196, 248

**DTC access**, for IIS, 444

**DUL (Dial-up List)**, 410

**DUN export files**, 197, 248

- .dun files, 197, 248

**DUN scripts**, 201

**Dynamic Linking Library files**. *See* DLLs

## E

**EBCD-Emergency Boot CD**, 163

**ebook files**, 197

- .edt files, 197

**effective permissions**, determining, 129–131

**EFS (Encrypting File System)**

- best practices for, 477
- certificates for, 462–464
- decrypting files and folders, 461
- definition of, 459
- enabling and disabling, 459, 476
- enabling on Windows Explorer context menu, 461
- encrypting files or folders, 460–461
- FEK (File Encryption Key) for, 464–465
- file permissions and, 462
- file sharing of encrypted files, 466–467
- keys for, backing up individually, 471–473
- limitations of, 460, 477
- new features in Windows XP, 465–469
- offline file encryption, 467–469

## EFS (Encrypting File System) (continued)

---

### **EFS (Encrypting File System) (continued)**

- password changes affecting, 464
- permissions and, 130
- recovery policy for
  - backing up keys individually, 471–473
  - Certificate Services (Microsoft), 475–476
  - comparison of methods for, 475–476
  - DRA (Default Recovery Agent), 473–475
- on remote servers, 469–471
- resources for, 478
- for web files, 468

**Efs0.log file, 461**

**Efs0.tmp file, 461**

**Elk Cloner virus, 12**

**e-mail. See also Outlook; phishing attacks; spam; viruses; worms**

- attacks using
  - bulk e-mailing programs for, 394–395
  - cross-site scripting (XSS), 393
  - malicious file attachments, 391–392
  - malicious links, 7–8, 392–393
  - malware executed using, 7
  - pharming, 397
  - phishing, 396–397
  - spam, 393–396
  - unauthorized reading of e-mail, 397
- authentication, lack of, vulnerabilities from, 389–390
- defending against attacks
  - antivirus scanning for, 406–407
  - authenticating e-mail links, 405
  - authentication and encryption, 417–418
  - blocking malicious file attachments, 398–401
  - blocking spam, 407–417
  - blocking unauthorized e-mail, 405
  - configuring client for, 403–404
  - disabling AutoPreview and Reading panes, 404–405
  - disabling HTML content, 401–403
  - DNS security, 418
  - end-user training, 418
  - not following links, 366
- HTML content
  - disabling, 401–403
  - vulnerabilities from, 389–390
- prevalence of attacks using, 5, 7
- security providers for, 57

**e-mail addresses, harvesting, 395**

**.email files, 197, 248**

**embedded files, 21, 191**

**embedded links, 191**

**embedded scripts, 21**

**.eml files, 197, 248**

**Encapsulating Security Payload (ESP) protocol, 299**

**Encrypting File System. See EFS**

**Encrypting File System in Windows XP and Windows Server 2003, 478**

**encryption. See also EFS (Encrypting File System); hashes for passwords; IPSec (IP Security) protocol**

- AES (Advanced Encryption Standard), 299, 464
- Blowfish encryption, 299
- Cryptographic Services, 270
- Data Decryption Field (DDF), 465
- Data Encryption Standard (DES), 299
- Data Encryption Standard XOR (DESX), 464
- of e-mail, 417–418
- system cryptography, security options for, 510

**end users. See users**

**enemy, knowing, 3. See also attackers**

**Enterprise Admins group**

- default GPO permissions for, 535
- definition of, 106
- protecting, 74
- SID for, 85

**Enterprise Domain Controllers group**

- computer accounts in, 116
- definition of, 106
- SID for, 85

**Enumerate Subkeys permission, registry keys, 241**

**enumeration, SID, 6, 75, 89**

**Error Reporting Service, 271**

**ESP (Encapsulating Security Payload) protocol, 299**

**Event Log service, 271**

**event log settings, group policy, 511**

**Event service, Microsoft Exchange, 285**

**Everyone group**

- Anonymous SID and, 113
- avoiding assigning permissions to, 136
- computer accounts in, 115, 116
- definition of, 106
- replacing with Authenticated Users group, 219
- SID for, 84
- Windows trusts and, 117

**e-worms, 391**

**Excel files, 202, 248**

**Excel SLK data-import files, 201**

**Excel111.adm template, 516**

**exception rules, SRP, 222–224**

**exceptions, firewall using, 66**

**Exchange Authority, 86**

**Exchange Domain Servers group, 107**

**Exchange Enterprise group, 107**

**Exchange (Microsoft)**

file blocking mechanisms in, 399–401  
services, 285

**.exe files, 197**

**executable files. See also software**

restricting execution of, 221–224  
vulnerabilities of, 20–21, 195, 197

**Execute File permission, 124, 126****execute permissions, IIS, 435****Exploits Block List (XBL), 410****Explorer Stylesheet files, 198****Expobot worm, 24****external trusts, 523****F****FakeGina trojan, 165**

**.far files, 196, 248**

**Fast User Switching Compatibility service, 271**

**.fav files, 197**

**Favorites list files, 197****Fax Service, 272****FBI, 2004 Computer Crime and Security Survey by, 5****Federal Information Processing Standards (FIPS), 464–465****FEK (File Encryption Key), 464–465****File Archive File Format files, 194****File Archive files, 194****file associations**

hidden, 212  
high-risk, blocking, 247–249  
permission to change, 250–251  
in registry, 231–235  
vulnerabilities of, 30, 38, 39, 203, 243  
in Windows Explorer, 235

**file attachments**

blocking, 398–401  
malicious, 391–392

**File Encryption Key (FEK), 464–465****file execution attacks, 361–362****The File Extension Source, 203****file extensions, hidden, 32–33****File Replication Service**

definition of, 272  
Replicator group for, 110  
Windows version comparisons for, 288

**File Service for Macintosh, 284****file sharing**

of EFS-protected files, 466–467  
Simple File Sharing, 131

**file system settings, group policy, 513–514****File Transfer Protocol (FTP), for IIS, 445****FileMon utility (Sysinternals), 240, 292, 425****files. See also specific files**

assigning permissions to, 97–99  
buffer overflow attacks on, 191  
decrypting with EFS, 461  
default permission settings for, 132–135  
defending against attacks of, 218–225  
downloading, IE settings for, 370, 376  
encrypting  
with Cipher.exe, 461  
with EFS, 460–461  
high-risk files  
ADS (Alternate Data Streams), 214–216  
auditing for, 224–225  
blocking, 225  
configuration files, 193  
Debug.exe program as, 189, 190  
definition of, 189–191  
file type mismatches, 192  
flawed by design, 191–192  
flaws allowing misuse of, 192–193  
list of, by type, 193–203, 247–249  
with magic names, 193  
MIME type mismatches, 214, 363  
naming tricks used on, 211–214  
NTFS permissions for, 218–221  
SRP for, 221–224  
unused applications, 217  
updating patches for, 225  
Windows files, list of, 204–211  
ownership of, 502  
permissions for, list of, 123–126  
unusual names for, malware using, 31–32

**filtering, anti-spam software using, 412–413****fingerprinting, 9, 413****FIPS (Federal Information Processing Standards), 464–465****Firefox browser**

exploitations of, 52–53, 350  
security statistics for, 351–352

**firewall ports for IPsec, 318–319****firewalls**

bypassing defenses of, 321  
failure of, assuming, 55  
host-based firewall, 65–68, 439

**firmware environment values, modifying, 501****Flash.ocx file, 353****floppy access, security options for, 504**

## **Flush.D trojan, 49**

### **folders. See also specific folders**

- assigning permissions to, 97–99
- decrypting with EFS, 461
- default permission settings for, 132–135
- encrypting with EFS, 460–461
- installing software to non-default folders, 76
- permissions for, list of, 123–126
- Share permissions for, 119–121
- unusual names for, malware using, 31–32

### **“Follow the Bouncing Malware” article, 19**

### **ForceSQL program, 165**

### **Foreign Security Principals OU, 520**

### **forest root domain, in Active Directory, 522**

### **forest trusts, 522**

### **forests, in Active Directory, 521**

### **Fp11.adm template, 516**

### **fraudulent e-mail. See phishing attacks**

### **FrontPage 2002 Server Extensions, for IIS, 445, 449**

### **FSMO (Forest Single Master Operations) roles, 523–524**

### **FTP (File Transfer Protocol), for IIS, 445**

### **FTP Publishing Service, 284**

### **ftp URI handler, 250**

### **Full Control permission**

- avoiding use of, 136
- definition of, 119–121, 124, 126, 127
- for GPOs (group policy objects), 534
- improperly configured, 16
- registry keys, 241

### **Fully Managed policies, 486**

## **G**

### **GAL (Global Address List), 96**

### **Gal11.adm template, 516**

### **Gartner Research report, November 2004, 9**

### **Gateway Services for Netware, 284**

### **Gibson, Steve (account of DoS attack), 15**

### **.gif files, 197**

### **global catalog, 88, 96**

### **Global groups, 96, 97**

### **global objects, creating, 498, 499**

### **Globally Unique Identifier (GUID), 82–83**

### **Gopher URI handler, 250**

### **Gpedit.msc program, 144, 483**

### **GPMC (Group Policy Management Console), 483**

### **GPO. See group policy object**

### **Gpresult.exe program, 535**

### **Gpupdate.exe program, 221**

### **graphics files, 194, 197, 198, 200, 248**

### **“The Great Password Debates: Pass Phrases vs. Passwords” (Microsoft), 145**

### **Greenborder virtual environment, 387**

### **group policy**

- in Administrative templates, 481, 485
- application of, 486–487, 529–536
- applying
  - with GPOs in Active Directory, 481, 482–483
  - with Local Computer Policy object, 481, 483–484, 528, 539
- Computer Configuration section of, 487
- definition of, 481
- Fully Managed policies, 486–487
- history of, 525–526
- preferences, 486–487
- in Security templates, 481, 485, 492, 538–539
- settings for
  - Administrative templates, 515–517
  - event log settings, 511
  - file system settings, 513–514
  - IPSec policies, 514
  - recommendations for, 517–518
  - registry settings, 513
  - restricted group settings, 512
  - script settings, 490
  - security settings, 491–511
  - software restriction policies (SRPs), 514
  - Software settings, 488–490
  - system services settings, 513
  - Windows settings, 490–514
- software publishing and, 488–490
- True policies, 486–487
- User Configuration section of, 487

### **Group Policy Administrator (NetIQ), 224, 346**

### **Group Policy Creator group, 107**

### **Group Policy Creator Owners group, 74, 85**

### **Group Policy Management Console (GPMC), 483**

### **Group Policy Object Editor console, 483–484**

### **group policy object (GPO)**

- application priorities for, 529–531
- blocked inheritance of, 532
- categories of, enforced or disabled based on, 531–532
- configuring in Active Directory, 481, 482–483
- default, 528–529
- determining effective policy for, 535–536
- disabling, 531
- for file permissions, 220–221
- location of, 485–486
- Loopback Policy Processing setting, 533
- No Override attribute, 533
- password complexity enforced by, 144

permissions for, 533–535  
 version number for, 539  
 WMI filtering of, 532

**groups. See also specific groups**

action-based groups, 95–96  
 assigning permissions to, 97–99, 135  
 built-in, list of, 102–113  
 definition of, 95  
 naming convention for, 95  
 nesting, 96–97  
 scope of, 96  
 types of, 96

**Guest account**

definition of, 100  
 security options for, 502–503

**Guests group, 86, 107**

**GUI skins, embedded links in, 192**

**GUID (Globally Unique Identifier), 82–83**

**Guid2obj tool, 82**

**guide to hacker personas (Hensing), 11**

.gz files, 197

.gzip files, 197

## H

**hackers. See dedicated attackers**

**hacking contest, May 2005, 10–11**

**hardware drivers, IIS, 438**

**hardware keystroke logging, 166**

**hash exception rules, SRP, 222, 341**

**hashes for passwords**

challenge-response mechanism for, 152  
 definition of, 146–147  
 extracting, 166–168  
 LM algorithm for, 147–148  
 not salted, effects of, 150  
 NT algorithm for, 147–148, 149  
 protected during authentication, 152  
 Syskey protecting, 150–152  
 when applied, 147

**Haxdoor.B backdoor trojan, 43**

**Haxor backdoor trojan rootkit, 41**

**HELO lookups, anti-spam software using, 408**

**Help and Support service, 272**

**Help files, 197**

**HelpAssistant account, 101**

**HelpServicesGroup group, 107**

**Hensing, Robert (guide to hacker personas), 11**

**hidden files, 30**

**hidden shares, 121–122**

**hives, in registry, 228–229**

**HKCC (HKEY\_CURRENT\_CONFIG) entries, registry**

default permissions for, 242  
 definition of, 228, 237

**HKCR (HKEY\_CLASSES\_ROOT) entries, registry**

default permissions for, 242  
 definition of, 228, 231–235  
 high-risk entries in, 243  
 malware using, 32–33, 45

**HKCU (HKEY\_CURRENT\_USER) entries, registry**

default permissions for, 242  
 definition of, 228, 229, 236  
 hardening permissions for, 247  
 high-risk entries in, 243–245  
 malware using, 33–40, 46–47

**HKLM (HKEY\_LOCAL\_MACHINE) entries, registry**

default permissions for, 242  
 definition of, 228, 229, 230–231  
 high-risk entries in, 244–246  
 malware using, 34, 35–46, 47–49

**HKU (HKEY\_USERS) entries, registry**

default permissions for, 242  
 definition of, 228, 229, 236

.hlp files, 197

**HoneyNet Project, botnets tracked by, 13**

**host-based defense, 55–56**

**host-based firewall, 65–68, 439**

**HOSTS file, 24**

**Hotbar adware, 46**

.ht files, 197

.hta files, 191, 197, 248

.htm files, 197

.html files, 197

**HTML files, 197, 199, 248**

**HTML links, malicious, 7–8**

.htt files, 198

**HTTP requests, IIS driver for, 421–422**

**HTTP SSL service, 272**

**HTTPS, running on non-default ports, 76**

**Http.sys driver, IIS, 421–422**

**human analysis, anti-spam software using, 413**

**Human Interface Device Access service, 272**

**hybrid dictionary attacks, 145–146, 173**

**Hyperterminal files, 197**

## I

**IAS (Internet Authentication Service), 284**

**ICMP traffic, allowing or disallowing, 66**

.ico files, 198

**Icon graphic files, 198**

**icons, desktop, RunAs feature used with, 60**

# ICS (Internet Connection Sharing) service

---

## **ICS (Internet Connection Sharing) service, 272, 281**

### **identification phase, access control, 80**

### **identities, IIS, 422–425**

### **IE (Internet Explorer)**

advisor ratings files, 201

attacks using

browser interface manipulation, 364

buffer overflow attacks, 357

cookie manipulation, 363–364

cross-site scripting, 357–358

directory transversal attacks, 362

file execution attacks, 361–362

malicious content, 363

MIME type mismatches, 363

plug-in exploits, 364–365

URL spoofing, 354–357

zone manipulation, 358–361

competitors of, 350

defending against attacks

browsing settings for, 378–379, 384

Enhanced Security Configuration for, 385–387

Java settings for, 379, 384

links in e-mails, not following, 366

security settings for, 379–385

third-party applications for, 387

untrusted web sites, not visiting, 366

updating patches for, 367

using latest browser, 366–367

zone settings for, 367–377

Dll files loaded by, 352

Favorites list files, 197

features of, 347–349

history of, 347

security features of, 348–349, 357

security statistics for, 351–352

security zones for, 358–361, 367–377, 385–387

startup process used by, 352–353

testing for vulnerabilities, 365

URL processing by, 353

version 7, 347, 348–349, 357

versions in use, 347

versions of, which to use, 366–367

`Ieframe.dll` file, 352

`IERESET.INF` file, 24

## **IETF (Internet Engineering Task Force), 296**

## **IIS Admin MMC console, 427**

## **IIS Admin Service, 284**

## **IIS (Internet Information Server)**

additional features, installing, 443–448

administration of, 427–428

application pools, 422–425, 453–455

authentication for, 182, 428–433, 449–450

configuration information, metabase file for, 427–428

configuring, 440, 443–451

definition of, 420

`Http.sys` driver, 421–422

identities, 422–425

IIS\_WPG (IIS Worker Process Group), 424–425

installing, 421

IUSR\_<computername> account, 101, 425–427

IWAM\_<computername> account, 101, 425–427

permissions for, 433–436, 450, 452–453

resources for, 456

securing

application installation and tightening, 456

cleaning and testing, 455–456

deployment, 456

hardware drivers, updating, 438

host firewall configuration, 439

IIS configuration, 443–451

IIS installation, 440

log files, monitoring, 456

logging configuration, 455

network/perimeter configuration, 437–438

operating system hardening, 441–443

operating system installation, 438–439

patch installation, 440–441

penetration tests, 456

physical security, 438

Remote Admin configuration, 439–440

steps for, 437

web sites, securing, 452–455

URLScan tool for, 450–451

version 7 modules, 449–450

versions of, default operating systems for, 420

vulnerabilities of, 419

Web Server Edition, 420

web service extensions, 436, 448–449

worker processes, 422–425

## **IIS logons, 182**

## **IIS permissions, 433–435**

## **IIS 6 Resource Kit, 456**

## **IIS 6 Technet Resources, Microsoft, 456**

## **IIS\_WPG (IIS Worker Process Group), 108, 424–425**

## **IKE (Internet Key Exchange), 300–301**

## **IM (Instant Messaging), attacks using, 8**

## **IMAP CD-Burning COM Service, 284**

## **IMAP4 service, Microsoft Exchange, 285**

## **impersonation**

bugs in, 90

of client after authentication, 90, 500

definition of, 90

- delegation and, 92
- enabling and disabling, 90
- levels of, 90–91
- policy settings for, 496–497
- in security token, 118
- viewing, 91
- Incoming Forest group, 108**
- Incoming Forest Trust Builders group, 86**
- Indexing Service, 272**
- Inetcorp.adm **template, 515**
- Inetesc.adm **template, 515**
- Inetres.adm **template, 515**
- Inetset.adm **template, 515**
- .inf **files, 198**
- Infll.adm **template, 516**
- Information Store service, Microsoft Exchange, 285**
- Information Technology-Information Sharing and Analysis Center, 51**
- Infrared Monitoring Service, 284**
- Infrastructure Master, FSMO role, 523**
- inheritance of permissions, 128–129**
- .ini **files, 198, 227–228**
- injection attacks, 15**
- .ins **files, 198**
- insider attacks, 17**
- Installer Files, Microsoft (MSI), 489**
- Installer package files, 199**
- Instalrll.adm **template, 516**
- Instant Messaging (IM), attacks using, 8**
- Integrated Windows Authentication (IWA), IIS, 429–430, 431, 432**
- Interactive group**
  - definition of, 108
  - SID for, 84
  - Windows trusts and, 117
- Interactive Training files, 194**
- Interactive Training files, Microsoft, 194**
- Internet Authentication Service (IAS), 284**
- Internet Connection Sharing (ICS) service, 272, 281**
- Internet Data Connector, for IIS, 447, 449**
- Internet Engineering Task Force (IETF), 296**
- Internet Explorer. See IE**
- Internet Information Server. See IIS**
- Internet Information Services Manager, IIS, 445**
- Internet Key Exchange (IKE), 300–301**
- Internet Printing, for IIS, 445**
- Internet Protocol Security working group, IETF, 296**
- Internet Security Association and Key Management Protocol (ISAKMP), 300**
- Internet shortcut files, 202**
- Internet Site Authority, 86**
- Internet site zone, IE, 360**
- Internet worms, 391**
- Internet Zone exception rules, SRP, 223, 341**
- Intersite Messaging service, 272, 288**
- Io.sys **file, 25**
- IP address, scanning for, 9**
- IP Version 6 Help (6to4) Service, 284**
- IPSec (IP Security) protocol**
  - AH protocol used with, 298, 299
  - attacks on, defending against, 321–322
  - authentication method for, 308–309
  - configuring, 302–303, 306
  - definition of, 295–296
  - ESP protocol used with, 299
  - example scenario for, 320–321
  - exemptions for, 315–317
  - filters for, 309–314
  - firewall for, 318–319, 321
  - IKE modes for, 300–301
  - key management for, 300
  - logging events for, 305
  - mode types for, 297–298
  - monitoring, 303–305
  - NAT or NAT-T used with, 301
  - open standard for, 296
  - performance of, 301–302
  - PFS (Perfect Forward Secrecy) for, 314–315
  - planning for, 319
  - policies for
    - creating, 302–303, 306–315
    - default, 305–306
    - definition of, 299
  - resources for, 322
  - rules for
    - creating, 308–315
    - definition of, 299
  - security associations (SAs) for, 300
  - Security Parameters Index (SPI) for, 300
  - security policy database for, 299
  - when to use, 319
- IPSec policies, group policy, 514**
- IPSEC Policy Agent, 273**
- IPSEC Services, 273**
- Ipseccmd.exe **program, 303**
- Ipsecmon.exe **program, 303**
- ISAKMP (Internet Security Association and Key Management Protocol), 300**
- island hopping, 183**
- .isp **files, 198**
- .it **files, 196, 248**
- IUSR\_<computername> account, 101, 425–427**

**IWA (Integrated Windows Authentication), IIS,**  
429–430, 431, 432  
**IWAM\_<computername> account,** 101, 425–427

## J

**.jar files,** 198  
**.jav files,** 198  
**.java files,** 198  
**Java, IE settings for,** 379  
**Javascript.dll file,** 353  
**.jfif files,** 198  
**John the Ripper program,** 166, 176  
**.jpe files,** 198  
**.jpeg files,** 198  
**.jpg files,** 198  
**.js files,** 198  
**.jse files,** 198  
**JS.Fortnight worm,** 46

## K

**Kak worm,** 46  
**Kerbrack program,** 170–171  
**Kerberos authentication package,** 159  
**Kerberos authentication protocol**  
attack tools for, 170–171  
definition of, 154–156  
group policy settings for, 494  
limitations of, 157  
**Kerberos Authentication Service (AS) exchange,** 155  
**Kerberos Client/Server exchange (Application Exchange),** 156  
**Kerberos Key Distribution Center service,** 273, 287  
**Kerberos Network Monitor,** 156  
**Kerberos Ticket Granting Service (TGS) exchange,**  
155–156  
**Kerbsniff program,** 170–171  
**Key Archival and Management in Windows Server 2003,** 478  
**.key files,** 201, 248  
**keystroke logging hardware,** 166  
**keystroke logging trojans,** 165  
**Klist utility,** 156  
**“Know Thy Enemy” strategy (Sun Tzu),** 3  
**Konqueror browser,** 350  
**KRA (Key Recovery Agent),** 74, 475–476  
**Krbtgt account,** 101  
**Krbtray utility,** 156

## L

**LAN Manager (LM) authentication protocol**  
definition of, 152–153  
disabling, 184–185  
**LAN Manager (LM) hash algorithm**  
definition of, 147–148  
disabling, 183–184  
**LAND attack,** 15  
**Lavasoft's Ad-Aware,** 70  
**LC5 program,** 174–175  
**LCP program,** 175  
**LDAP (Lightweight Directory Access Protocol)**  
accessing directory services using, 525  
signing requirements for, 504  
**Ldap URI handler,** 250  
**Ldp.exe program,** 82  
**Least Privilege Users group,** 219  
**License Logging service,** 273  
**Limited User Accounts.** See **LUAs**  
**linked files, malware in,** 21  
**links, malicious,** 7–8  
**List Folder permission,** 124, 126  
**List permission,** 123, 126  
**LM (LAN Manager) authentication protocol**  
definition of, 152–153  
disabling, 184–185  
**LM (LAN Manager) hash algorithm**  
definition of, 147–148  
disabling, 183–184  
**LMHOSTS file,** 24  
**.lnk files,** 199  
**Local Administrator account,** 85, 99  
**Local Authority,** 84  
**Local Computer Policy,** 481, 483–484, 528, 539  
**Local Computer zone, IE,** 358–359  
**local execution of attacks,** 7–8  
**Local group**  
assigning permissions to, 97  
definition of, 96, 108  
SID for, 84  
**Local Guest account,** 85, 100  
**Local intranet zone, IE,** 360–361  
**local logons**  
allowing, 497  
denying, 499  
**Local Security Authority (LSA) program,** 118, 159  
**Local Security Policy,** 144  
**Local Service account,** 101, 424

**Local System account, 101–102**

**Local Users and Groups console, 96**

**LocalService account, 85, 261, 262**

**LocalSystem account, 85, 261**

**logging**

- Event Log service, 271
- event log settings, group policy, 511
- hardware keystroke logging, 166
- for IIS, 455, 456
- keystroke logging trojans, 165
- password logging trojans, 165
- security log, 500, 501

**Logical Disk Manager Administrative Service, 273**

**Logical Disk Manager service, 273**

**logoff scripts, 490**

**logon screen warning messages, enabling, 187**

**logon scripts, 490**

**Logon session X-X group, 108**

**logons**

- authentication and, 159–160
- as batch job
  - allowing, 500
  - denying, 499
- IIS logons, 182
- local logons
  - allowing, 497
  - denying, 499
- previous logon requirements, 506
- as services
  - allowing, 500–501
  - denying, 499
- as Terminal Services
  - allowing, 497
  - denying, 499
- text for, 505–506

**Loopback Policy Processing setting, for GPOs, 533**

**LSA (Local Security Authority) program, 118, 159**

**LSA secrets, 178**

**Lsadump2 program, 178**

**Lsaext.dll program, 166**

**Lsass.exe program, 118, 159**

**LSDOU rule, for GPO application, 529**

**.lsf files, 194, 247**

**LSP software, malware in, 72–73**

**LSPfix program, 73**

**.lsx files, 194, 247**

**LUAs (Limited User Accounts). See also RunAs feature**

- activities allowed and not allowed by, 58–59
- administrators running programs as, 63
- features in Windows Vista for, 76

**Lynx browser, 350, 351**

**.lzh files, 199**

## M

**Machine Debug Manager Service, 284**

**macro viruses, 391**

**.mad files, 199**

**.maf files, 199**

**.mag files, 199**

**mail server directory harvesting, 395**

**MakeMeAdmin application, 62**

**malware. See also trojans; viruses; worms**

- defeating, inability to, 52
- definition of, 4
- as highest security threat, 4–5, 53
- locations of
  - ActiveX controls, 29
  - application files, 20–21
  - folders, 28–29
  - hidden files, 30
  - LSP software, 72–73
  - PATH locations, 29–30
  - preventing access to, 57
  - registry, 32–49
  - restored files, 30
  - scheduled tasks, 32
  - specific files, 21–27
  - Trusted Publishers, 31
  - unusual file or folder names, 31–32
  - URL Monikers, 32
- prevalence of, 4–7
- spam
  - definition of, 18–19
  - methods used by spammers, 394–396
  - motivation of spammers, 393–394
  - spam bots, 5, 395, 409, 419
  - speed of infection by, 5
  - spyware, 6, 18–19, 70
  - statistics regarding, 5–7
  - trends in, 19–20
  - types of, 11–14
- .mam files, 199**
- Management service, Microsoft Exchange, 285**
- man-in-the-middle (MitM) attacks, 16–17, 322**
- .maq files, 199**
- .mar files, 199**
- .mas files, 199**
- master hackers, 11**
- .mat files, 199**

**.mav files, 199**

**.maw files, 199**

**MBSA (Microsoft Baseline Security Analyzer), 65**

**McAfee Personal firewall, 68**

**.mda files, 199**

**.mdb files, 199**

**.mdbhtml files, 199**

**.mde files, 199**

**.mdn files, 199**

**.mdt files, 199**

**.mdx files, 199**

### **memory**

locking pages in, 500

quota for processes, 497

**message analysis, anti-spam software using, 411–413**

**Message Queuing Down Level Clients Service, 285**

**Message Queuing, IIS, 444**

**Message Queuing Service, 285**

**Message Queuing Triggers Service, 285**

**MessageLabs security service provider, 5, 57, 70, 392**

**Messenger service, 273**

**metabase file, IIS, 427–428**

**.mhtm files, 199**

**.mhtml files, 199**

**Microsoft Access, file vulnerabilities in, 193, 199**

**Microsoft Baseline Security Analyzer (MBSA), 65**

**Microsoft cabinet archive files, 194**

**Microsoft Certificate Services. See Certificate Services**

**Microsoft Document Template files, 196**

### **Microsoft Exchange**

file blocking mechanisms in, 399–401

services, 285

**Microsoft Help files, 197**

**Microsoft IIS 6 Technet Resources, 456**

**Microsoft Installer Files (MSI), 489**

**Microsoft Installer package files, 199**

**Microsoft Interactive Training files, 194**

**Microsoft Internet Explorer. See IE (Internet Explorer)**

**Microsoft network client, security options for, 506–508**

**Microsoft Office, Administrative templates for, 516**

**Microsoft Outlook. See Outlook**

**Microsoft Outlook Express. See Outlook Express**

**Microsoft Patch (MSP), 489**

**Microsoft Powerpoint files, 200**

**Microsoft Search service, 274**

**Microsoft Shell Command files, 199**

**Microsoft Update, 65**

**Microsoft Word. See Word**

**Microsoft/MS Software Shadow Copy Provider service, 274**

**Microsoft's anti-spyware software, 70**

**Microsoft's patch management document, 64**

**Microsoft's Ten Immutable Laws of Security, 7**

**Microsoft's Windows Server 2003 PKI Certificate Security, 309**

**.mim files, 199**

### **MIME files**

type mismatches, 214, 363

vulnerabilities of, 199

**misconfiguration weaknesses, 9, 16**

**MitM (man-in-the-middle) attacks, 16–17, 322**

**.mmf files, 199**

**Modify permission, 123, 126**

### **monikers, URL**

definition of, 353

malware using, 32

**Mozilla browser, 350, 351**

**MS-Blaster worm, 14, 56**

**Msdos.sys file, 25**

**.msg files, 199**

**Msgina.dll program, 159**

**.msh files, 199**

**Mshtml.dll file, 352**

**.msi files, 199**

**MSI (Microsoft Installer Files), 489**

**Ms-its URI handler, 250**

**MSMQ HTTP Support, for IIS, 446**

**.msp files, 199**

**MSP (Microsoft Patch), 489**

**Msrating.dll file, 352**

**MSSQL\$UDDI Service, 285**

**MSSQLServerAD Helper Service, 286**

**.mst files, 199**

**MST (Transform Files), 489**

**MSV1\_0 authentication package, 159**

**MTA Stacks service, Microsoft Exchange, 285**

**My Computer zone, IE, 358–359**

## **N**

**namespace, 519**

**NAT (Network Address Translation), 301**

**NAT-T (NAT-Transversal), 301**

**.NET Framework Support Service, 286**

**.NET Framework-reliant components, IE settings for, 367–368, 375**

**Net Logon service, 274, 287**

**NetBIOS protocol, 158–159**

**NetMeeting Remote Desktop Sharing service, 274****Netscape browser, 350**Netsh.exe **command, 67****network**

- access to computers on, policy settings for, 496, 499
- access to, security options for, 508–510
- defending against attacks of, 56
- edge protection of, inadequacy of, 55–56
- EFS (Encrypting File System) on, 469–471

**Network Address Translation (NAT), 301****network client, Microsoft, security options for, 506–508****Network Configuration Operators group, 86, 108****Network Connections service, 274****Network DDE DSDM service, 274****Network DDE service, 274****Network group**

- computer accounts in, 115
- definition of, 108
- SID for, 84

**Network Location Awareness (NLA) service, 275****Network News Transfer Protocol (NNTP) service, 286, 445****network protocol analyzer programs (sniffing attacks), 16–17, 168–171****Network Provisioning Service, 275****network security, IIS, 437–438****Network Service account, 101, 423–424****network traffic, securing. See IPSec (IP Security) protocol****NetworkService account, 85, 261, 262****NeverShowExt values, registry, 250****NewDotNet adware program, 73****News URI handler, 249****Nigerian scams, 394****NLA (Network Location Awareness) service, 275****Nmap fingerprinting tool, 9****NNTP (Network News Transfer Protocol) service, 286, 445****nntp URI handler, 249****Non-unique Authority, 84****Nordahl boot disk (Nordahl-Hagen, Peter), 161–163****Normal.dot file, 25****Norton Personal firewall, 68****Notify permission, registry keys, 242****Novell logon client, 41****NT Authority, 84****NT LM Security Support Provider service, 275****NT (NTLAN Man) hash algorithm, 147–148, 149****NT Resetter, 163****Ntbootdd.sys file, 132****Ntdetect.com file, 132****Ntlds.dit file, 80****NTFS permissions**

- best practices for, 135–136, 332
- changed as the result of another action, 128
- combinations of, 125–126
- compared to SRPs, 344
- default settings for, 132–135
- definition of, 122
- for distribution groups, 96
- effective permissions, determining, 129–131
- EFS (Encrypting File System) and, 130, 462
- group policy objects and, 220–221
- for high-risk files, 218–221
- for IIS, 435–436, 450, 452–453
- improperly configured, 16
- inheritance of, 128–129
- list of, 123–125
- misconceptions about, 79
- modifying, 122–123
- multiple groups contributing to, 88, 130
- for prevention of unauthorized execution of software, 330–332
- for security groups, 96
- in security token, 117
- for services, 290–292
- setting using AGULP method, 97–99
- Simple File Sharing and, 131

**NTLAN Man (NT) hash algorithm, 147–148, 149****Ntldr file, 25, 132****NTLM authentication protocol, 153, 450****NTLMv2 authentication protocol, 153–154****Ntuser.dat hive, registry, 229****Null Authority, 84****Nullsoft WinAmp media files, 196, 248****.nws files, 199****O****Oakley protocol, 300****Object Access auditing, 224–225, 455****objects. See also group policy object (GPO)**

- access control for, 80–81
- ACL (Access Control List) for, 126
- Browser Helper Objects (BHOs), exploitation of, 364–365
- COM objects
  - registry listing, 42
  - unregistering, 332–334
- container objects, in Active Directory, 481
- DACL (Discretionary Access Control List) for, 126
- global objects, creating, 498, 499

## objects (continued)

---

### objects (continued)

- GUID for, 82–83
- permanent shared objects, creating, 498
- RDP (Remote Desktop Protocol) connection objects, 181
- Shell scrap objects, 201, 248
- Shockwave Flash objects, 201, 249
- system objects, security options for, 503, 511
- token object, creating, 498

### obscurity attacks, 17–18, 355–357

#### .ocx files, 199

#### Office (Microsoft), Administrative templates for, 516

#### Office Source Engine service, 286

#### Office11.adm template, 516

#### Offline NT Password & Registry Editor, 161–163

#### .oft files, 199

#### OLE2 documents, 26

#### Oleview utility, 335

#### O&O BlueCon XXL, 163

#### Opera browser, 350, 351

#### operating systems, exploitations of, 52–53. *See also* Windows

#### Opposum worm, 24

#### opt-in execution. *See* software restriction policies

#### organizational unit (OU), in Active Directory

- default, list of, 520
- definition of, 481, 520–521
- role-based structure for, 537–538

#### OS X operating system, exploitations of, 53

#### OSI model, defense strategy for layers of, 56–57

#### Other Organization group, 85, 108

#### Outlkl1.adm template, 516

#### Outlook Express (Microsoft)

- configuration for, 403–404
- disabling, without disabling Outlook, 218
- files, vulnerabilities in, 197, 199

#### Outlook (Microsoft)

- configuration for, 403–404
- disabling HTML content, 401–403
- file blocking mechanisms in, 399–401
- files, vulnerabilities in, 200
- malicious links and, 392
- malware used to manipulate, 21
- Template files, vulnerabilities in, 199

#### .ovl files, 199

## P

#### pagefile, creating, 498

#### Pakistani Brain virus, 5

#### partitions, in Active Directory, 525

#### passfilt.dll file, 144

#### Passport Authentication, IIS, 430, 432, 433

#### password attacks

- on cached credentials, 176–177
- commonly-used password lists for, 146
- with Credential Manager, 179–181
- defending against, 183–187
- on domain computer accounts, 177–179
- island hopping, 183
- LM hash algorithm and, 149
- NT hash algorithm and, 149
- password capturing, 165–166
- password guessing, 163–165, 171–175
- password resetting, 160–163
- with physical access, 18
- on RDP connection objects, 181

#### password capturing, 165–166

#### password cracking

- birthday attacks, 173
- brute-force attacks, 171–172
- definition of, 166
- dictionary-based, 144, 145–146, 172–173
- hybrid dictionary attacks, 145–146, 173
- LC5 program, 174–175
- LCP program, 175
- password hashes, extracting, 166–168
- programs for, finding, 175
- rainbow tables, 173–174
- share password attacks, 169
- sniffing authentication traffic, 168–171

#### password files, 200

#### password guessing, 163–165, 171–175

#### Password List reader, 181

#### password logging trojans, 165

#### Password Reset Diskette, 182

#### password resetting, 160–163

#### passwords

- alternatives to, 187
- auditing, 187
- for BIOS, 71
- boot-up passwords, 71
- changing frequently, 186
- commonly used, 146
- complexity requirements for, 144–146, 184
- default passwords, 146
- definition of, 141
- expiration warning for, 506
- group policy settings for, 492–493
- hashes for
  - challenge-response mechanism for, 152
  - definition of, 146–147

- extracting, 166–168
  - LM algorithm for, 147–148
  - not salted, effects of, 150
  - NT algorithm for, 147–148, 149
  - protected during authentication, 152
  - Syskey protecting, 150–152
  - when applied, 147
- for highly privileged accounts, 74
- length requirements
  - guidelines for, 184
  - for strong passwords, 146
  - when complexity enabled, 144
- machine account changes of, 504–505
- multiple incorrect entries, lockout resulting from, 185–186
- number of possible passwords, 141–142
- random password generators, 187
- resetting, EFS keys lost by, 464
- for service accounts, 263
- size of, 141–142
- strong passwords, 146
- studies regarding, 145
- Unicode characters used in, 142–144
- patch management document, Microsoft, 64**
- Patch, Microsoft (MSP), 489**
- patches**
  - for high-risk files, 225
  - for IE (Internet Explorer), 367
  - installing, for IIS, 440–441
  - keeping up-to-date, 63–65
  - level of, 63
  - management tools for, 64–65
  - regression testing of, 64
  - for services, 293–294
  - as sign of attack, 10
- Path exception rules, SRP, 223, 343**
- PATH locations, malware in, 29–30**
- payload damage attacks, 23**
- PC Anywhere program, 41**
- pcAnywhere autotransfer files, 194**
- PDC Emulator, FSMO role, 523**
- .pdc files, 200, 248**
- PDF ebook files, 197**
- PDF files, exploitations of, 52, 200**
- penetration tests, for IIS, 456**
- Perfect Forward Secrecy (PFS), 314–315**
- Performance Log Users group, 86, 108**
- Performance Logs and Alerts service, 275**
- Performance Monitor Users group, 86, 109**
- Perl script files, 200**
- permanent shared objects, creating, 498**
- permissions. See also NTFS permissions; Share permissions**
  - for GPOs (group policy objects), 533–535
  - for IIS, 433–436
  - for registry, 241–243
  - setting on per-socket basis, 126
- Petch trojan, 33, 41**
- PFS (Perfect Forward Secrecy), 314–315**
- pharming attacks, 18–19, 397, 418**
- phishing attacks. See also malware**
  - definition of, 18–19
  - e-mail used for, 396–397
  - IE 7 features defending against, 348
  - prevalence of, 5–6
  - spearfishing, 396
  - URL spoofing used for, 354–357
- phishing filter, IE settings for, 374, 377, 382–383**
- physical attacks**
  - defending against, 70–71
  - definition of, 17, 56
- physical security, IIS, 438**
- .pif files (Program Information Files), 191, 200, 248**
- pings, scanning for IP addresses using, 9**
- .pl files, 200**
- platforms, exploitations of, 52–53. See also Windows Plug and Play service, 275**
- plug-in exploits, IE, 364–365**
- .png files, 200, 248**
- .pol files, 200, 248**
- PolicyMaker (Desktop Standard), 224, 346**
- POP3 service, Microsoft Exchange, 285**
- Popdis Trojan, 47**
- pop-up blocker, IE settings for, 374, 377**
- Portable Media Serial Number Service, 275**
- ports**
  - firewall ports for IPSec, 318–319
  - services, running on non-default ports, 6–7, 75–76
- Postini security service provider, 57, 70**
- .pot files, 200**
- .pothtml files, 200**
- Power Users group**
  - definition of, 109
  - protecting, 74
  - removed in Windows Vista, 76, 87
  - SID for, 86, 87
- Powerpoint files, 200**
- .ppa files, 200**
- .ppt files, 200**
- Ppt11.adm template, 516**
- .ppthtml files, 200**
- preEmpt product (Pivx), 387**

## **pre-shared key (PSK), 309**

**Pre-Windows 2000 Compatibility Access group, 86, 113, 116**

**Pre-Windows 2000 group, 109–110**

**.prf files, 200**

**principal. See security principal**

**Print Operators group, 86, 110**

**Print Server for Macintosh service, 286**

**Print Spooler service, 276**

**printer drivers, security options for, 503**

## **privileges**

password protections for highly privileged accounts, 186–187

renaming highly privileged accounts, 73–75, 186

running software with decreased privileges, 63

running software with escalated privileges

RunAs feature, 59–63, 114

third-party applications for, 62

for users, 58–63, 218–219

## **processes**

accounts that can start, specifying, 501

memory quota of, policy settings for, 497

profiling, 501

worker processes, IIS, 422–425

**Profile Assistant, IE, 382**

**Program Files folder, 132**

**Program Information Files (.pif files), 191, 200, 248**

**program overlay files, 199**

**programs. See executable files; software**

**Protected Storage service, 276**

**protocol in URL. See URL monikers**

**Proxy SID, 85**

**Psgetsid utility (Sysinternals), 87, 89**

**PSK (pre-shared key), 309**

**.pst files, 200**

**Pub11.adm template, 516**

## **publications**

about anti-phishing and anti-spoofing, 357

Certificate Auto-enrollment in Windows XP, 478

about cross-site scripting, 357

about EFS, 478

EFS article (Russinovich), 478

Encrypting File System in Windows XP and Windows Server 2003, 478

“Follow the Bouncing Malware” article, 19

“The Great Password Debates: Pass Phrases vs. Passwords” (Microsoft), 145

Key Archival and Management in Windows Server 2003, 478

Microsoft’s Windows Server 2003 PKI Certificate Security, 309

Offline EFS, 468

security guides, 289

Windows Data Protection, 478

*Windows Server 2003 Security Infrastructures*

(De Clercq), 86

**Pwdump program, 166–168**

**PWL files, 181, 200**

**Pwl Tools, 181**

**Pwservice.exe program, 166**

**.py files, 200**

## **Q**

**Qaz trojan/worm, 190**

**Qhosts trojan, 48, 49**

**QoS RSVP service, 276**

**Query Value permission, registry keys, 241**

## **R**

**rainbow tables, 173–174**

**random password generators, 187**

**.rar files, 200**

**RAS and IAS Servers group, 86, 110**

**RAS Servers group, 86, 110**

**Rasphone.pbk file, 26**

**.rat files, 201**

**RAT (remote access trojan), 13**

**rate controls, anti-spam software using, 409–410**

**RBAC (Role-Based Access Control), 537**

**RBLs (real-time blacklists), 410–411**

**.rdp files, 201**

**RDP (Remote Desktop Protocol) connection objects, 181**

**Read and Execute permission, 123, 126, 127**

**Read Attributes permission, 124, 126, 127**

**Read Control permission, registry keys, 242**

**Read Data permission, 124, 126, 127**

**Read Extended Attributes permission, 124, 126**

**Read permission**

definition of, 119–121, 123, 126

for GPOs (group policy objects), 534

interactions with other permissions, 127

**Read Permissions permission**

definition of, 125, 126

interactions with other permissions, 127

**Reading pane, disabling, 404–405**

**realm trusts, 523**

- real-time blacklists (RBLs), 410–411**
- recovery console, security options for, 510**
- recovery policy for EFS**
  - backing up keys individually, 471–473
  - Certificate Services (Microsoft), 475–476
  - comparison of methods for, 475–476
  - DRA (Default Recovery Agent), 473–475
- Recycler **folder, 28**
- RECYCLER **folder, 132**
- Redfall trojan, 46**
- RedHat Linux, exploitations of, 53**
- .reg files, 201, 248**
- Reg\_Binary data type, registry, 230**
- Reg\_Dword data type, registry, 230**
- Regedit.exe **program, 82–83, 133, 228**
- Regedt32.exe **program, 228**
- Reg\_Expand\_Sz data type, registry, 230**
- registry**
  - alternate locations for, 237–238
  - data types in, 230
  - definition of, 227–228
  - editing tools for, 228, 238–240
  - group policy settings applied to, 486–487
  - group policy settings for, 513
  - high-risk entries
    - defending against attacks of, 246–251
    - list of, 243–246
  - HKCC (HKEY\_CURRENT\_CONFIG) entries
    - default permissions for, 242
    - definition of, 228, 237
  - HKCR (HKEY\_CLASSES\_ROOT) entries
    - default permissions for, 242
    - definition of, 228, 231–235
    - high-risk entries in, 243
    - malware using, 32–33, 45
  - HKCU (HKEY\_CURRENT\_USER) entries
    - default permissions for, 242
    - definition of, 228, 229, 236
    - hardening permissions for, 247
    - high-risk entries in, 243–245
    - malware using, 33–40, 46–47
  - HKLM (HKEY\_LOCAL\_MACHINE) entries
    - default permissions for, 242
    - definition of, 228, 229, 230–231
    - high-risk entries in, 244–246
    - malware using, 34, 35–46, 47–49
  - HKU (HKEY\_USERS) entries
    - default permissions for, 242
    - definition of, 228, 229, 236
    - permissions for, 241–243, 251, 332
    - settings for TCP/IP stack hardening, 71–72
    - structure of, 228–229
- Registry Editor tool, 82–83, 133, 228
- registry files, 201
- Regmon tool (Sysinternals), 239, 292
- Reg\_Multi\_Sz data type, registry, 230**
- regression testing of patches, 64**
- Reg\_String data type, registry, 230**
- Reg\_Sz data type, registry, 230**
- Relative Identifier Master, FSMO role, 523**
- Relative Identifier (RID), 84–86**
- Relay Spam Servers (RSSs), 410**
- Remote Access Auto Connection Manager service, 276**
- Remote Access Connection Manager service, 276**
- remote access trojan (RAT), 13**
- remote administration, IIS, 439–440**
- Remote Administration using HTML, for IIS, 447**
- Remote Assistance, HelpAssistant account created by, 101**
- Remote Desktop connection shortcuts, 201**
- Remote Desktop Help Session Manager service, 276**
- Remote Desktop Protocol (RDP) connection objects, 181**
- Remote Desktop Users group, 86, 110**
- Remote Desktop, using for IIS, 439–440**
- Remote Desktop Web Connection, for IIS, 448**
- remote execution of attacks. See also denial-of-service (DoS) attacks**
  - definition of, 7–8
  - types of, 14–17
- Remote Interactive Logon group, 85, 110**
- Remote Procedure Call (RPC) Locator service, 277, 288**
- Remote Procedure Call (RPC) service**
  - attacks on, 253
  - definition of, 267, 277
- Remote Registry service, 277**
- remote shutdowns, allowing, 500**
- Remote Storage Notification service, 286**
- Remote Storage Server Services, 286**
- Removable Storage service, 277**
- Replicator group, 86, 110**
- Resource Manager Authority, 86**
- resources. See publications; web site resources**
- restored files, malware in, 30**
- Restricted Code group, 85, 111, 114**
- restricted group settings, group policy, 512**
- Restricted sites zone, IE, 361**
- Resultant Set of Policy Provider, 277**
- Resultant Set of Policy (RSOP) tool, 535**
- reverse DNS lookups, anti-spam software using, 408**
- RFC 2401, 296**
- RFC 2412, 296**

**Rich Text Format files, 201**

**RID (Relative Identifier), 84–86**

**Riler trojan, 73**

**Rlogin URI handler, 250**

**Role-Based Access Control (RBAC), 537**

**RootKitRevealer (Sysinternals), 14**

**rootkits, 14**

**Routing and Remote Access service, 277**

**Routing Engine service, Microsoft Exchange, 285**

**Routing Support, for IIS, 446**

**RPC (Remote Procedure Call) Locator service, 277, 288**

**RPC (Remote Procedure Call) service**

attacks on, 253

definition of, 267, 277

**RSoP (Resultant Set of Policy) tool, 535**

**RSSs (Relay Spam Servers), 410**

**RTF files, 52, 201**

**Rudnyi, Evgenii B. (Sid2user and User2sid utilities), 89**

**RunAs feature**

command line execution of, 61–62

definition of, 59–60

limitations of, 62

LUA protections extended by, 63

Restricted Code group and, 114

using, 60

**RunAs Service, 278**

**RunAsAdmin application, 63**

**Russinovich, Mark (EFS article), 478**

**Rusty worm, 24**

## S

**Sabin, Todd (Lsadbump2 program), 178**

**SAC (System Access Control) permissions, 126**

**SAD (Security Association Database), 300**

**Safari browser, 350**

**salted hashes, 150**

**SAM hive, registry, 229**

**SAM password database, 150, 161**

**SAM (Security Accounts Manager), 80, 278**

**Samba protocol, 158**

**SANS Handler's Diary article about malware, 19**

**SAP Agent Service, 286**

**SAs (security associations), IPSec, 300**

**Saved Queries OU, 520**

**SC tool, 265–267**

**Sc.exe program, 256**

**.scf files, 201, 248**

**SChannel Authentication protocol, 85**

**scheduled tasks**

malware using, 31

security options for, 504

**scheduling priority, allowing increase of, 500**

**Schema Admins group, 74, 85, 111**

**Schema Master, FSMO role, 523**

**ScoopLM program, 168**

**scope of groups, 96**

**.scp files, 201**

**.scr files, 201**

**Scrap Shell (.shs) files, 191, 201, 248**

**screen saver files, 201**

**script kiddies, 10–11**

**scripting, IE settings for, 374, 377**

**scripts**

for computers, startup and shutdown, 490

embedded in Word, malware in, 21

embedded using XSS, malware in, 21

file vulnerabilities in, 200, 201, 202, 248

for users, logon and logoff, 490

**.sct files, 202, 249**

**Search service, Microsoft, 274**

**Secondary Logon service, 278**

**Secret Service report on insider attacks, 17**

**Secunia web site, 9**

**secure channel, 115**

**Security Accounts Manager (SAM), 80, 278**

**Security Association Database (SAD), 300**

**security associations (SAs), IPSec, 300**

**Security Center service, 278**

**Security certificate files, 195**

**Security Configuration Wizard, 289–290**

**security groups, 96**

**Security hive, registry, 229**

**Security Identifier. See SID**

**security log**

allowing generation of, 500

managing, 501

**Security Parameters Index (SPI), IPSec, 300**

**security policy database, IPSec, 299**

**security principal**

authentication of, 80

delegation for, 92–94

GUID for, 82–83

identification of, 80

impersonation of, 90–92

security token for, 88

SID for

definition of, 83–84

multiple, 88, 130

**security reference monitor, 81**

**security settings, group policy**

- account policies
  - account lockout policy, 493
  - Kerberos policy, 494
  - password policy, 492–493
- event log settings, 511
- file system settings, 513–514
- IPSec policies, 514
- local policies
  - audit policy, 494–496
  - security options, 502–511
  - user rights assignment, 496–502
- registry settings, 513
- restricted group settings, 512
- software restriction policies (SRPs), 514
- system services settings, 513

**Security templates, group policy settings in, 481, 485, 527–528, 538–539****security token, 88, 117–119, 126****security-by-obscurity, 54****Self group, 85, 111****sender confirmation, anti-spam software using, 408****sender domain verification, anti-spam software using, 408****Sender ID Framework (SIDF), 409****Sender Policy Framework (SPF), 408–409****Server Message Block (SMB) protocol**

- attack tools for, 168–169
- definition of, 158–159

**Server Operators group, 74, 86, 111****Server service, 278****server software, running on non-default ports, 75–76****Server-Side Includes (SSI), for IIS, 448, 449****service accounts, password attacks on, 177–179****Service group, 85, 111****service principal name (SPN), 92****services**

- accounts for, 260–263, 292–293
- allowing logons as, 500–501
- controlling with SC tool, 265–267
- default, list of, 268–283
- definition of, 254–255
- denying logons as, 499
- dependencies for, 264–265
- executable and path for, 257–258
- failures of, recovery from, 263–264
- identifying, 255–256
- installed by default, 255
- multiple, with one name, 258–259
- nondefault, list of, 283–288

- permissions for, 261, 290–293, 332
- RPC (Remote Procedure Call) service, 253, 267, 277
- running on non-default ports, 6–7, 75–76

**securing**

- account for, 292–293
- disabling or removing services, 290
- guides for, 289
- in high-security environment, 288
- in normal security environment, 288–289
- permissions for, 290–292
- reasons for, 253–254
- recommendations for specific services, 268–283, 289
- Security Configuration Wizard for, 289–290
- updating patches for, 293–294
- Startup type for, 259–260
- unsigned, 256
- viewing in Services console
  - Dependencies tab, 264–265
  - General tab, 257–260
  - LogOn tab, 260–263
  - Recovery tab, 263–264

**Services console**

- definition of, 256–257
- Dependencies tab, 264–265
- General tab, 257–260
- LogOn tab, 260–263
- Recovery tab, 263–264

**Services.msc program, 256****session key, security options for, 505****Set Value permission, registry keys, 241****share password attacks, 169****Share Password Checker, 169****Share permissions**

- contributing to effective permissions, 130, 131
- default settings for, 132–135
- definition of, 119–122

**shares**

- creating, 121
- hidden shares, 121–122

**.shb files, 201, 248****Shdocvw.dll file, 352****Shell Command files, 199****Shell Command files, Microsoft, 199****Shell Hardware Detection service, 278****Shell scrap objects, 201, 248****Shockwave Flash objects, 201, 249****shortcut links, 199****.shs (Scrap Shell) files, 191, 201, 248****.shtml files, 197**

## **shutdown scripts, 490**

### **shutdowns**

- allowing, 502
- security options for, 503, 510

### **SID (Security Identifier)**

- anonymous enumeration of, 6, 75
- definition of, 83–84
- enumeration of, 75, 89
- filtering of, 90
- list of, 84–86
- multiple, for one security principal, 88, 130
- RID value of, 84
- in security token, 117
- Top-Level Authority value of, 83–84
- viewing tools for, 87–89

### **SIDF (Sender ID Framework), 409**

### **SIDHistory field, 89–90**

`Sid2user.exe` program, 87, 89

### **Simple File Sharing, 131**

### **Simple Mail Transfer Protocol (SMTP) service, 286, 446**

### **Simple TCP/IP Services, 286**

### **Single Instance Storage Groveler Service, 286**

### **Site Replication service, Microsoft Exchange, 285**

### **Site Server Authority, 86**

### **sites, in Active Directory, 524**

### **SKEME protocol, 300**

### **Skrenta, Richard (Elk Cloner virus), 12**

### **Slammer SQL worm, 75**

`.slk` files, 201, 248

### **Smart Card Helper service, 278**

### **Smart Card service, 278**

### **smart cards, security options for, 506**

### **SmartSearch adware, 47**

### **SMB Auditing Tool, 169**

### **SMB Downgrade Attacker, 169**

### **SMB (Server Message Block) protocol**

- attack tools for, 168–169
- definition of, 158–159

### **SMBGrind program, 168**

### **SMBRelay program, 168**

### **SMTP (Simple Mail Transfer Protocol) service, 286, 446**

### **snews URI handler, 249**

### **sniffing attacks, 16–17, 168–171**

### **SNMP and SNMP Trap Services, 286**

### **social engineering, 18**

### **sockets, setting permissions based on, 126**

### **software. See also executable files**

- defending against attacks of, 56
- installation of, by users, 59

installing to non-default folders, 76

malicious, from browser downloads, 363

misconfigurations of, 9, 16

patching of, as sign of attack, 10

permissions for, 135

popularity of, attracting hackers, 52–53

preventing installation of, 331–332

preventing unauthorized execution of, 329–336

removing, 330

researching vulnerabilities of, 9

unauthorized execution of, 8, 54

unregistering, 332–334

unused, dangers from, 217

updating patches for, 225

### **Software hive, registry, 229**

### **software publishing, 488–490**

### **software restriction policies (SRPs)**

benefits of, 326

compared to NTFS permissions, 344

definition of, 221, 325, 336

deny-by-default software execution policy, 325–326

developing, 327–329

disadvantages of, 327

exception rules for, 222–224, 340–344

group policy, 514

management console for, 221, 337

planning, 222, 337–340

security levels in, 344–346

third-party applications for, 224, 346

when to use, 327

### **Software settings, group policy, 488–490**

### **spam. See also anti-spam software; malware**

definition of, 18–19

methods used by spammers, 394–396

motivation of spammers, 393–394

spam bots, 5, 395, 409, 419

### **spawners (companion viruses), 12**

### **spearfishing, 396**

### **Special Administration Console Helper service, 279**

### **Special permissions**

for GPOs, 534

guidelines for, 136

list of, 124–126

### **SPF (Sender Policy Framework), 408–409**

### **SPI (Security Parameters Index), IPSec, 300**

`.spl` files, 201, 249

### **SPN (service principal name), 92**

### **spoofing**

ARP spoofer, 168

IE 7 features defending against, 348

URL spoofing, 354–357

- spyware.** *See also* malware
    - anti-spyware software, 70
    - definition of, 18–19
    - prevalence of, 6
  - Spyware Eblaster trojan, 38**
  - SQL Auditing Tool, 165**
  - SQL Server, 6, 165**
  - SQLAgent\$ Service, 286**
  - Sqlbf-all program, 165**
  - SQL.Slammer worm, 5, 14**
  - SRPs.** *See* software restriction policies
  - SSDP Discovery Service, 279**
  - SSI (Server-Side Includes), for IIS, 448, 449**
  - SSL Client-Side Mapping, IIS, 430–431**
  - SSL, IE settings for, 383**
  - Stanton, Anne (The Complete Patch Management Book), 64**
  - StartPage.I trojan, 45**
  - StartPage.O trojan, 43**
  - startup scripts, 490**
    - .stl files, 201
    - .stm files, 196, 248
  - streaming audio/video files, 194, 247**
  - Streams (Sysinternals), 216**
  - strong passwords, 146**
  - subtrees (hives), in registry, 228–229**
  - Support\_<number> account, 101**
    - .swf files, 201, 249
  - Symantec**
    - botnets tracked by, 13
    - Internet Security Threat Report, 19, 394
  - Synchronize permission, 125, 126**
    - .sys files, 201
  - Syskey utility**
    - for EFS, 477
    - protecting password hashes, 150–152
  - System Access Control (SAC) permissions, 126**
  - System account, 101–102, 261**
  - System Attendant service, Microsoft Exchange, 285**
  - system cryptography, security options for, 510**
  - System Event Notification service, 279**
    - System folder, 28
  - System hive, registry, 229**
  - System Management Server, 64**
  - system objects, security options for, 503, 511**
  - system performance, profiling, 501**
  - System Restore feature, 30**
  - System Restore Service, 279**
  - system services settings, group policy, 513**
  - system settings, security options for, 511**
  - system time, changing, 498**
  - System Volume Information folder, 132, 135, 485**
  - System.adm template, 515**
  - %SystemDrive% folder, permissions for, 132, 134**
  - SYSTEM.INI file, 26–27, 133**
  - System32 folder**
    - malware in, 28
    - permissions for, 133–134, 135
  - Sysvol folder, 132, 135, 485**
- ## T
- Take Ownership permission, 125, 126**
    - .tar files, 202
  - Task Scheduler**
    - definition of, 279
    - malware using, 31
  - Tasks folder, 29**
    - .taz files, 197, 202
  - TCP/IP NetBIOS Helper Service, 279**
  - TCP/IP Print Server Service, 286**
  - TCP/IP scanning program, 9**
  - TCP/IP stack, hardening, 71–73**
  - Telephony service, 279**
  - Telnet service, 280**
  - Telnet URI handler, 250**
  - TelnetClients group, 111**
  - templates**
    - Administrative templates, group policy settings in, 481, 485
    - Document Template files, 196
    - Outlook Template files, vulnerabilities in, 199
    - Security templates, group policy settings in, 481, 485
  - Temporary Internet Files folder (TIF), IE, 29, 362, 380**
  - Ten Immutable Laws of Security (Microsoft), 7**
  - Terminal Server License Servers group, 86, 112**
  - Terminal Server Users group, 85, 112**
  - Terminal Services, 280**
  - Terminal Services logons**
    - allowing, 497
    - denying, 499
  - Terminal Services Session Directory, 280**
  - TFTP (Trivial File Transfer program), attacks using, 8**
    - .tgz files, 197, 202
  - Themes service, 280**
  - This Organization group**
    - computer accounts in, 116
    - definition of, 112
    - SID for, 85
    - Windows trusts and, 117
  - 3DES (Triple DES), 299, 464**

**.386 files, 202**

**TIF (Temporary Internet Files) folder, IE, 29, 362, 380**

**Tiny Firewall, 68**

**TLS (Transport Layer Security), IE settings for, 383**

**TMKSoft.XPlugin adware, 48**

**Tn3270 URI handler, 250**

**token object, creating, 498**

**token-based authentication, 187**

**TokenMon utility (Sysinternals), 91**

**Top-Level Authority value, SID, 83–84**

**Transform Files (MST), 489**

**transport mode, IPSec, 297–298**

**traverse checking, bypassing, 498**

**Traverse Folder permission, 124, 126, 127–128**

**Triggers, for IIS, 446**

**Triple DES (3DES), 299, 464**

**Trivial File Transfer program (TFTP), attacks using, 8**

**Trivial FTP Daemon Service, 286**

**trojans. See also malware**

Bookmarker trojan, 41

botnets, 13

Bropia trojan, 34

command and control trojan, 13

Daqa trojan, 73

definition of, 13–14

Download.Ject trojan, 38

FakeGina trojan, 165

Flush.D trojan, 49

Haxdoor.B backdoor trojan, 43

Haxor backdoor trojan rootkit, 41

keystroke logging trojans, 165

password logging trojans, 165

Petch trojan, 33, 41

Popdis Trojan, 47

Qaz trojan/worm, 190

Qhosts trojan, 48, 49

RAT (remote access trojan), 13

Redfall trojan, 46

Riler trojan, 73

rootkits, 14

Spyware Eblaster trojan, 38

StartPage.I trojan, 45

StartPage.O trojan, 43

Webber trojan, 38

zombie trojan, 13

**True policies, 486**

**trust password, 523**

**Trusted for Delegation, enabling, 499–500**

**trusted man-in-the-middle (MitM) attacks, 322**

**Trusted Publishers, 31**

**Trusted sites zone, IE, 361**

**trusts**

in Active Directory, 522–523

Windows trusts, permissions and, 116–117

**TSGrinder program, 164–165**

**tunnel mode, IPSec, 297**

**twins (companion viruses), 12**

**two-factor authentication, 187**

**2004 Computer Crime and Security Survey (FBI), 5**

**2004 ICISA Labs Tenth Annual Computer Virus Prevalence Survey, 5, 391**

**.tz files, 202**

**Tzu, Sun (“Know Thy Enemy” strategy), 3**

## U

**überhackers, 11**

**.ult files, 196, 248**

**Unicode characters in passwords, 142–144**

**Uninterruptible Power Supply service, 280**

**Universal distribution group, 96, 97**

**Universal Plug and Play Device Host service, 280**

**Update (Microsoft), 65**

**Upload Manager service, 280**

**URI handlers, high-risk, 249–250**

**URI (Uniform Resource Identifier), 353**

**URL (Universal Resource Locator)**

definition of, 353

obscurity attacks using, 355–357

spoofing, 354–357

untrusted web sites, not visiting, 366

**URL authorization, IIS, 450**

**.url files, 202**

**URL monikers**

definition of, 353

malware using, 32

**Url.dll file, 353**

**Urlmon.dll file, 352, 353**

**URLScan tool, 450–451**

**usability, affected by security, 53**

**User Configuration section of group policy, 487**

**user rights assignment, group policy, 496–502**

**%UserName% folder, 132**

**%USERPROFILE% folders, 28**

**%UserProfile% folders, 28**

**users. See also LUAs (Limited User Accounts); security principal**

built-in, list of, 99–102

education of, failure of, 54

installation of software by, 59

not allowing to make security decisions, 54

not assigning permissions to, 135

permissions of, resulting from multiple groups, 88, 130  
 preventing execution of files by, 218, 221–224  
 preventing from logging in as administrators, 329–330, 366  
 privileges to give to, 58–63, 218–219  
 training of, 418  
 unauthorized execution of software by, 8, 54

**Users group**

computer accounts in, 115  
 definition of, 112  
 SID for, 86  
 Windows trusts and, 117

**Users OU, 520**

User2sid.exe **program, 87, 89**

**Utility Manager service, 281**

.uu **files, 202**  
 .uue **files, 202**

**V****Vaughn, Randal (Baylor University professor), 13**

.vb **files, 202, 249**  
 .vbe **files, 202, 249**  
 .vbs **files, 191, 202, 249**

**VBScript files, 202, 249**

Vbscript.dll **file, 353**

**vCard file format files, 202, 249**

.vcf **files, 202, 249**

**Virtual device drivers, 202****Virtual Disk Service, 281****virtual private network (VPN), creating with IPSec, 295****viruses. See also antivirus software; malware**

boot sectors infected by, 12  
 companion viruses, 12  
 Define virus, 12  
 definition of, 12  
 Elk Cloner virus, 12  
 macro viruses, 391  
 Pakistani Brain virus, 5  
 prevalence of, 5, 391  
 web site listing, 5

**Vista. See Windows, Windows Vista****Visual Basic class modules, 194****Visual Basic Script, attacks using, 191****Visual Basic test source files, 199****volume maintenance tasks, performing, 501****Volume Shadow Copy service, 281****VPN (virtual private network), creating with IPSec, 295**

.vxd **files, 202**

**W****Wallz worm, 45****war dialing, 8–9****War Games movie, 8–9**

.wbk **files, 202**

**Web Element Manager service, 287****Web Manager tool, IIS, 428****Web Server Edition, IIS, 420****web service extensions, IIS, 436, 448–449****web site resources**

Ad-Aware (Lavasoft), 70  
 about Administrative template creation, 517  
 Advanced Windows Password Recovery program, 181  
 about anti-phishing and anti-spoofing, 357  
 Anti-Phishing Workgroup, 5  
 Austrumi, 163  
 Automatic Updates, 65  
 Autoruns program (Sysinternals), 256  
 Barracuda Spam Firewall, 69  
 Beagle.AV worm, 195, 200, 391  
 BeatLM program, 168  
 Bookmarker trojan, 41  
 Bropia trojan, 34  
 browser security statistics, 351  
 browser test sites, 365  
 Brutus program, 164  
 CACHEDUMP utility, 176  
 Cain & Able program, 16, 166  
 Carnegie Mellon University CERT Coordination Center, 51  
 CastleCop's listing of ActiveX controls, 335  
 CipherTrust, zombie nets tracked by, 13–14  
 ClearCredCache program, 179  
 The Complete Patch Management Book (Bradley, Susan and Anne Stanton), 64  
 CoolWeb Search Adware, 40  
 CredDump program, 180  
 about cross-site scripting, 357  
 Daqa trojan, 73  
 Define virus, 12  
 Dell Computers, survey by, 6  
 denial-of-service attack, account of (Gibson), 15  
 DES and DESX comparison, 464  
 EBCC-Emergency Boot CD, 163  
 about EFS, 478  
 Elk Cloner virus, 12  
 exploit research, 9  
 FakeGina trojan, 165  
 The File Extension Source, 203

## web site resources (continued)

---

### web site resources (continued)

- FileMon utility (Sysinternals), 240
- fingerprinting tools, 9
- Firefox browser, 350
- firewalls, 68
- ForceSQL program, 165
- Gartner Research report, November 2004, 9
- “The Great Password Debates: Pass Phrases vs. Passwords” (Microsoft), 145
- Group Policy Administrator (NetIQ), 224
- guide to hacker personas (Hensing), 11
- hacking contest, May 2005, 10–11
- Haxor backdoor trojan rootkit, 41
- HoneyNet Project, botnets tracked by, 13
- IE security, third-party tools for, 387
- for IIS, 456
- Information Technology-Information Sharing and Analysis Center, 51
- Internet Security Threat Report (Symantec), 394
- Internet Security Threat Report VIII (Symantec), 19
- IPSec (IP Security) protocol, 322
- John the Ripper program, 166
- Kerbrack program, 170
- Kerberos authentication protocol, 156
- Konqueror browser, 350
- LAND attack, 15
- Lsadump2 program, 178
- LSPfix program, 73
- Lynx browser, 350
- MakeMeAdmin application, 62
- McAfee Personal firewall, 68
- MessageLabs security service provider, 5, 57
- Microsoft Baseline Security Analyzer, 65
- Microsoft Update, 65
- Microsoft’s anti-spyware software, 70
- Microsoft’s patch management document, 64
- Microsoft’s Ten Immutable Laws of Security, 7
- Mozilla browser, 350
- MS-Blaster worm, 56
- Netscape browser, 350
- NewDotNet adware program, 73
- Nmap fingerprinting tool, 9
- Nordahl boot disk, 161
- Norton Personal firewall, 68
- NT Resetter, 163
- NTLMv2 authentication protocol, 154
- Offline EFS, 468
- Oleview utility, 335
- O&O BlueCon XXL, 163
- Opera browser, 350
- password complexity, enabling in Windows NT, 144
- password guessing programs, 164–165
- Password List reader, 181
- password resetting programs, 162–163
- patch management tools, 64–65
- Petch trojan, 33, 41
- PolicyMaker (Desktop Standard), 224
- Postini security service provider, 57
- Psgetsid utility (Sysinternals), 89
- Pwdump program, 167
- Pwl Tools, 181
- Qaz trojan/worm, 190
- RBLs (real-time blacklists), 410
- Regmon tool (Sysinternals), 239
- Riler trojan, 73
- RootKitRevealer (Sysinternals), 14
- rootkits, Windows, 14
- RunAsAdmin application, 63
- Safari browser, 350
- SANS Handler’s Diary article about malware, 19
- ScoopLM program, 168
- Secret Service report on insider attacks, 17
- Secunia web site, 9
- security guides, 289
- security surveys, 5–6
- Share Password Checker, 169
- SIDs, list of, 86
- Sid2user.exe program, 89
- SMB Auditing Tool, 169
- SMB Downgrade Attacker, 169
- SMBGrind program, 168
- SMBRelay program, 168
- SQL Auditing Tool, 165
- Sqlbf-all program, 165
- SRP-like applications, 224, 346
- Streams (Sysinternals), 216
- Symantec, botnets tracked by, 13
- System Management Server, 64
- Tiny Firewall, 68
- TokenMon utility (Sysinternals), 91
- trusts, 523
- TSGrinder program, 164
- 2004 Computer Crime and Security Survey (FBI), 5
- 2004 ICSA Labs Tenth Annual Computer Virus Prevalence Survey, 5, 391
- Unicode characters to avoid in passwords, 143
- URLScan tool, 450–451
- User2sid.exe program, 89
- Wallz worm, 45
- The Wild List, 5

- Windows Firewall, 68
- Windows Firewall group policy settings, 66
- Windows Server Update Service (WSUS), 64–65
- Windows Vista, blog regarding, 76
- Windows XP/2000/NT Key, 163
- Winternals Administrator's Pak, 163
- WMF exploit, 393
- W2K Server Resource Kit utilities, 156
- Xprobe2 fingerprinting tool, 9
- ZoneAlarm firewall, 68
- web sites. See also browsers; URL (Universal Resource Locator)**
  - EFS (Encrypting File System) and, 469
  - securing, 452–455
- Webber trojan, 38**
- WebClient service, 281**
- WebDAV (Web-based Distributed Authoring and Versioning)**
  - definition of, 448
  - EFS (Encrypting File System) and, 469
  - enabling, 449
- WFP (Windows File Protection), 12**
- white-listing. See software restriction policies**
- whitelists, anti-spam software using, 410**
- Whoami.exe program, 87–88**
- WIA (Windows Image Acquisition) service, 287**
- The Wild List web site, 5**
- WinAmp media files, 196, 248**
- %Windir% folders, 28**
- Windows**
  - authentication protocols supported by, 156–157
  - hardening, for IIS, 441–443
  - installation of, for IIS, 438–439
  - patches for, keeping up-to-date, 63–65
  - services installed by default on, 255
  - version of, hackers identifying, 9
  - Windows NT
    - authentication protocols supported by, 156–157
    - NT (NTLAN Man) hash algorithm introduced by, 147–148, 149
    - password complexity, enabling, 144
  - Windows 2000
    - Kerberos authentication protocol introduced by, 154
    - password complexity, enabling, 144
    - SRP-like features for, 224, 344
  - Windows Vista
    - features of, 76
    - Power Users group removed in, 87
  - Windows XP
    - LAND attack on, 15
    - password complexity enabled in, 144
- Windows Animated Cursor files, 193, 247**
- Windows Audio service, 281**
- Windows Authorization Access group, 86, 112–113, 116**
- Windows Compiled Help Files, 195, 247**
- Windows cursor graphic files, 196, 248**
- Windows Data Protection, 478**
- Windows Explorer command files, 201, 248**
- Windows File Protection (WFP), 12**
- Windows File System (WinFS), 228**
- Windows Firewall, 65–68, 318–319**
- Windows Firewall/Internet Connection Sharing (ICS) service, 272, 281**
- Windows folder, permissions for, 132–134, 135**
- Windows Icon graphic files, 198**
- Windows Image Acquisition (WIA) service, 287**
- Windows Installer service, 281**
- Windows Internet Naming Service (WINS), 287**
- Windows Management Instrumentation Driver Extensions service, 282**
- Windows Management Instrumentation service, 281**
- Windows Media Services, 287**
- Windows Policy file, 200, 248**
- Windows Scripting Host, attacks using, 191**
- Windows Server 2003 Security Infrastructures (De Clercq), 86**
- Windows Server Update Service (WSUS), 64–65**
- Windows settings, group policy, 490–514**
- Windows Time service, 282**
- Windows trusts, permissions and, 116–117**
- Windows User Mode Driver Framework service, 287**
- Windows XP/2000/NT Key, 163**
- Windows.adm template, 515**
- WinFS (Windows File System), 228**
- WinHTTP Web Proxy Auto-Discovery Service, 282**
- WIN.INI file, 27**
- Wininit.int file, 27**
- Winlogon.exe process, 159**
- WinRAR archived files, 200**
- WINS Users group, 113**
- WINS (Windows Internet Naming Service), 287**
- Winsock.dll file, 27**
- WINSTART.BAT file, 27**
- Winternals Administrator's Pak, 163**
- Wired Equivalent Privacy, 16**
- Wireless (Zero) Configuration service, 282**
- .wiz files, 202**
- Wizard files, 202**
- WLANs (wireless local area networks), sniffing attacks on, 16**
- .wma files, 196, 248**

**WMF exploit, 393**

**WMI filtering, for GPOs, 532**

**WMI Performance Adapter service, 282**

**Wmplayer.adm template, 515**

**Word (Microsoft)**

document vulnerabilities, 196, 202

malware in embedded scripts, 21

**Word11.adm template, 516**

**worker processes, IIS, 422–425**

**Workstation service, 283**

**World Authority, 84**

**World Wide Publishing Service, 287**

**World Wide Web Service, for IIS, 446, 448**

**WorldSearch adware, 47**

**worms. See also malware**

Beagle.AV worm, 195, 200, 391

Blaster worm, 8

Code Red worm, 419

definition of, 14

e-worms, 391

Internet worms, 391

MS-Blaster worm, 14

password-guessing routines in, 146

prevalence of, 7

SQL.Slammer worm, 5, 14

**Write Attributes permission, 125, 126**

**Write DACL permission, registry keys, 242**

**Write Data permission, 124, 126**

**Write Extended Attributes permission, 125, 126**

**Write Owner permission, registry keys, 242**

**Write permission**

definition of, 123, 126, 127

for GPOs (group policy objects), 534

**.ws files, 191, 202, 249**

**.wsc files, 202, 249**

**Wscript.exe program, 191**

**.wsf files, 202, 249**

**WSH files, 202, 249**

**WSUS Administrators group, 113**

**WSUS (Windows Server Update Service), 64–65**

**W3wp.exe process, 422–423**

**W2K Server Resource Kit utilities, 156**

**Wuau.adm template, 515**

**WuKill worm, 24**

**.xla files, 202**

**.xlb files, 202**

**.xlc files, 202**

**.xld files, 202**

**.xlk files, 202**

**.xll files, 202**

**.xlm files, 202**

**.xls files, 202**

**.xlshtml files, 202**

**.xlt files, 202**

**.xlthtml files, 202**

**.xlv files, 202**

**.xml files, 202**

**Xprobe2 fingerprinting tool, 9**

**.xsl files, 202**

**XSS (cross-site scripting)**

in e-mail, 393

in IE (Internet Explorer), 357–358

malware in, 21

## Z

**.z files, 203**

**ZAP file type, software publishing, 489**

**Zellome worm, 43**

**ZENworks (Novell), 346**

**.zip files, 192, 203**

**zombie trojan, 13**

**ZoneAlarm firewall, 68**

**zones, IE security**

customizing settings for, 367–377

enhanced configuration for, 385–387

manipulation attacks on, 358–361

## X

**X.500 directory service, 519–520. See also Active Directory**

**XBL (Exploits Block List), 410**