

# Index

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

## A

- AAA (Authentication, Accounting, and Authorization), 162–163, 166, 172–175, 172–173, 187
- AC (alternating current) circuits, 85, 85
- ACAP (Application Configuration Access Protocol), 75–76
- access control
  - in firewalls, 148, 162–163
  - policies for, 112–113
  - for viruses, 268
- access control lists (ACLs), 115
- access lists, 163
- access points (APs), 283
- Access Rules tab, 166–174, 167–171
- Access This Computer from the Network right, 334–335
- Access Through Share Permissions dialog box, 340–341, 340–341
- Account Lockout setting, 333
- account management. *See* users and user accounts
- Account Policies node, 328
- Account Policy dialog box, 331–332, 332
- accreditation, 27
- ACK flag
  - in connection-oriented communications, 57–58
  - in packet filtering firewalls, 125–126
  - in TCP flag field, 116–117
- ACLs (access control lists), 115
- actions
  - for access rules, 166, 174
  - for filter rules, 178–179
  - in OSA, 14–15, 14–15
  - in Snort, 206–207
- Activate section, 207
- Active Directory (AD)
  - for certificate services, 371
  - for Windows 2000, 317–321
- ActiveX blocking, 164
- actual occurrences, 8
- Ad-Hoc mode, 93
- AD Users and Computer utility, 321
- adaptive security algorithm (ASA), 161–162
- adaptive systems, 2, 5
- Add A Replication Pair dialog box, 310
- Add AAA Server dialog box, 172–173, 173
- Add access level, 343
- Add Address Translation Rule dialog box, 180–182, 180, 182
- Add & Read access level, 343
- Add Global Pool Item dialog box, 181–182, 181
- Add Host/Network? dialog box, 170, 170
- Add Key dialog box, 359
- Add Parameters for Websense URL Filtering dialog box, 175–176
- Add/Remove Programs applet, 331
- Add Rule dialog box
  - for AAA rules, 173–174, 173
  - for access rules, 168–170, 168–170
  - for filter rules, 177–178, 177
- Add Value dialog box, 359, 362
- address books, 73–74
- Address Mask Reply value, 120
- Address Mask Request value, 120
- Address Range Assignment screen, 248, 248
- address resolution protocol (ARP), 34–35, 34–36
- addresses
  - in bootp, 69
  - broadcast, 34
  - in Ethernet header frames, 33
  - IP. *See* IP addresses
  - MAC. *See* MAC (media access control) addresses
  - translating
    - NAT. *See* NAT (network address translation)
    - PAT, 145, 180, 182
- Adleman, Leonard, 232
- .adm files, 327–328
- administrative contacts, 417
- Administrative Templates, 325–327, 327
- Advanced Attributes dialog box, 365, 365
- Advanced category, 187
- Advanced Encryption Standard (AES), 228–229
- Advanced IP Addressing dialog box, 353, 353
- Advanced NAT Options dialog box, 172, 183–184, 183
- Advanced URL Filtering dialog box, 176, 176
- AES (Advanced Encryption Standard), 228–229
- AH (Authentication Header), 229, 372
- alert\_ formatting modules, 209
- alerts in Snort, 205–206, 209
- aliasing, 396–397
- all-networks broadcasts, 107
- Alta Vista Tunnel product, 243
- alternating current (AC) circuits, 85, 85
- alternatives, 8–9, 24
- AlterNIC site, 220
- Amateur Radio AX.25 Level 2? option, 398
- AMD LANCE and PCnet (AT1500 and NE2100)? option, 400
- anonymous FTP access, 404
- ANSI standards for DES, 228
- ANSI.SYS driver, 259
- anti-virus countermeasures, 262

- AntiOnline site, 446
  - AOL4FREE.COM Trojan horse, 267
  - Apache Web server, 404
  - Apollo 1, 21
  - AppleTalk DDP? option, 398
  - appliance-based firewalls, 133–134, 141–142
  - Application Configuration Access Protocol (ACAP), 75–76
  - Application Domain level, 375
  - application gateways. *See* proxy servers and clients
  - application layer, 42
  - application-level virus scanners, 272
  - Application Service Providers (ASPs), 298
  - application-specific integrated circuits (ASICs), 108, 243
  - application specific proxy servers, 130
  - application state, 128–129
  - APs (access points), 283
  - ARCNET Support? option, 400
  - ARCServe products, 298–299
  - arguments entry, 391–392
  - arity of sets, 11
  - ARP (address resolution protocol), 34–35, 34–36
  - arpspoof tool, 431
  - ASA (adaptive security algorithm), 161–162
  - ASICs (application-specific integrated circuits), 108, 243
  - ASPs (Application Service Providers), 298
  - Assemblies, 375
  - assigned applications, 331
  - asterisks (\*) in passwd files, 387
  - at signs (@) for event-based triggers, 15
  - ATM (Asynchronous Transfer Mode), 98–99
  - ATM emulation, 53
  - atstake site, 446
  - attachments, viruses in, 272
  - attack prevention
    - mailing lists for, 447–448
    - newsgroups for, 448
    - in PIX firewall, 163–165
    - vendor information for, 439–443
    - vulnerability databases for, 444–445
    - Web sites for, 446–447
  - attacks
    - brute force, 225–226, 436–437, 436
    - buffer overflow, 432–433
    - collecting information for, 415–421
    - FIN scanning for, 425
    - hidden accounts for, 430
    - host and service scanning for, 423
    - launching, 429–430
    - man-in-the-middle, 218–219, 219, 227–228, 430–432
    - against NIDS, 198–200, 199
    - nslookup command for, 418–420
    - passive monitoring in, 426–427, 426
    - physical access, 437–438
    - Ping scanning for, 423, 423, 434–435
    - port scanning for, 424–425, 424
    - preventing. *See* attack prevention
    - search engines for, 420–421, 420
    - Smurf, 434–435
    - SYN, 163, 433
    - TCP half scanning for, 425
    - teardrop, 195–197, 195, 433–434
    - traceroute command for, 421–422, 421–422
    - vulnerability checks in, 427–429, 427, 429
    - whois command for, 416–418
  - attributes
    - manipulation by viruses, 261
    - in PKI, 371
  - Audit Policy dialog box, 346–347, 347
  - auditing, 343, 344, 346–347, 347
  - authentication, 215
    - in Bluetooth, 95
    - for destinations, 219–220
    - Kerberos, 230–231, 366
    - in link state routing, 52–53
    - in PAM, 391–392
    - with proxy clients, 131
    - in public key cryptography, 370
    - for session hijacking, 218–219, 219
    - in TFTP, 289
    - token cards for, 233–234
    - in VPN. *See* VPN (virtual private networking)
  - Authentication, Accounting, and Authorization (AAA), 162–163, 166, 172–175, 172–173, 187
  - Authentication Header (AH), 229, 372
  - authentication service exchange, 368–369
  - authorization in Bluetooth, 95
  - authorized scripts, 331
  - Auto Update category, 187
  - automated vulnerability scanners, 428–429, 429
  - automating log reviews, 346
- ## B
- b-directional trusts, 321
  - b file type, 384
  - back doors, 267–268, 430
  - Back Orifice product, 238, 439
  - backbones, 90
  - Backup Files and Directories right, 335
  - backups
    - SAM files on, 323
    - server, 295–297
    - for WAN connections, 288
    - workstation, 461
  - bandwidth
    - with bridges, 101, 102
    - of fiber optic cable, 87
    - of T1 lines, 96

banners, logon, 338, **361–362**  
 Basic category for security templates, 329–330  
 Basic level of service in MPLS, 56  
 Basic Service Set (BSS), 283  
 Basicdc.inf file, 330  
 Basicsv.inf file, 330  
 Basicwk.inf file, 330  
 BAT files, 259  
 beacon packets, 281–282  
 Berkeley Internet Name Domain (BIND) server, 403  
 Berkeley Software Distribution (BSD), 380  
 best of breed concept, 19, 228  
 best practices, 319  
 BIND (Berkeley Internet Name Domain) server, 403  
 Binhex program, 78  
 biological models, 5, 18–19  
 biometric security devices, 7  
 black box view, 4  
 block cipher encryption, **222–223**, 222  
 Bluetooth standard, **94–95**  
 bombs, **263**  
 boot manager, configuring, **402**  
 boot sector replication, **260**, 273  
 booting and viruses, 262  
 bootp service, **68–70**, **403**  
 BorderManager proxy server, 131  
 bound transmissions, **87–89**  
 boundaries in systems, 3  
 BRI ISDN, 288  
 BrickHouse firewall front-ends, 135  
 bridges, 93, **100–102**, *100–102*, **107–108**  
 broadband fixed wireless topologies, **99**  
 broadcast addresses, 34  
 broadcasts
 

- blocked by routers, 107
- in Smurf attacks, 434–435

 Brunner, John, “The Shockwave Rider”, 265  
 brute force attacks, **225–226**, **436–437**, *436*  
 BSD (Berkeley Software Distribution), 380  
 BSS (Basic Service Set), 283  
 buffer overflow attacks, **432–433**  
 Bugtraq mailing list, **447**  
 bulletin board areas in IMAP, 75  
 Bypass Traverse Checking right, 335

## C

c file type, 384  
 cable modems, 286  
 cabling
 

- fiber optic, **86–88**, *86*
- problems from, **278–280**
- security of, 86

 cache poisoning, **220**

caches
 

- ARP, 35
- DNS, 71

 Caesar ciphers, 221  
 Campatws.inf file, 330  
 Carrier Sense Multiple Access with Collision Detection (CSMA/CD), 91, 284  
 carrier waves, **88**  
 CAs (certificate authorities), 229, 371  
 case sensitivity
 

- in Snort, 213
- in Unix, 382

 case studies, **19–22**  
 Category 5 (CAT5) cabling, 279  
 Category 7 (CAT7) cabling, 279  
 cavity viruses, 261  
 CBC (Cipher Block Chaining), 372  
 centralized management, 372  
 centralized security, 318  
 CERT (Computer Emergency Response Team), 266, **446**  
 certificate authorities (CAs), 229, 371  
 certificate services, **370–371**  
 certification in SDLC, **25**  
 CGI Truncate field, 179  
 Change access level, 341, 343  
 changing
 

- groups, **385–386**
- ownership, **385–386**
- permissions, **385**

 channels in IRC, 80  
 Chargen service, 352  
 chassis hubs, 287  
 Check Point Firewall-1 NG, 150–151  
 checksums
 

- with NIDS, 197
- for viruses, **268–269**

 chgrp utility, 386  
 chmod utility, **385**  
 Choke virus, 258  
 Choose Whether Or Not To Reboot dialog box, 307, *307*  
 chown utility, 385–386  
 CIDR (Classless Inter-Domain Routing), 207  
 Cipher Block Chaining (CBC), 372  
 ciphers, deficiencies in, **225**  
 ciphertext, 220, **222–223**, 222  
 Cisco company
 

- patches and updates from, **441**
- technical information from, **440–441**

 Cisco firewalls. *See* PIX firewall  
 class performance, 53  
 classes, 11–12, *11*  
 Classless Inter-Domain Routing (CIDR), 207  
 clear text transmissions, **215–218**, *216–217*  
 client-server exchange, **369**

- clients
  - proxy, 130–131
  - VPN, 250–253, 250–253
- CLR (Common Language Runtime), 375
- Cluster Server, 293
- clustering, 294–295
- Co-occurrence constraints, 13–14, 13
- Code Access Security Policy tool, 376
- Code fields in ICMP, 118, 120–122
- Code Red worm, 265
- code strings for viruses, 260
- collecting information for attacks, 415–421
  - nslookup command for, 418–420
  - search engines for, 420–421, 420
  - whois command for, 416–418
- collision detection in CSMA/CD, 91, 284
- collision domains, 101, 102
- collisions in WLANs, 284
- .com domain, 70
- COM files, infection of, 259
- COM ports for PIX firewalls, 158, 158
- commands in NIDS, 205
- Common Configurations screen, 246, 246
- Common Language Runtime (CLR), 375
- Common Open Software Environment (COSE), 380
- companion viruses, 259
- Compatible template, 330
- compiling Unix kernel, 401–402
- complementarity in Systems Theory, 2
- Completing the Network Connections Wizard screen, 252, 252
- complexity in Systems Theory, 2
- component and code review in SDLC, 24–25
- compressed files, viruses on, 270
- computer browser, 349
- Computer Configuration node, 325, 325
- Computer Economics study, 257
- Computer Emergency Response Team (CERT), 266, 446
- Computer Properties dialog box, 337–338, 337
- concealment of viruses, 261–263
- Conf.adm file, 328
- Config.pol file, 339
- Configurable Proxy Ping, 164
- configuration files, 288–289
- Configure tab, 305, 307, 308
- configuring
  - boot manager, 402
  - components, 24
  - Event Viewer, 344–345, 345
  - packet filtering, 354–355, 354–355
  - PIX firewall. *See* PIX firewall
  - proxy clients, 131
  - routers, 288
  - Snort NIDS, 211–212
  - systems, 25
  - Unix, 394–401, 395–396, 412–413
  - VPN
    - clients, 250–253, 250–253
    - servers, 245–249, 246–249
  - VSR, 304–307, 305–308
- conflicting objectives, 7
- Connect to a Private Network through the Internet option, 250
- Connect To dialog box, 157, 157
- Connect Virtual Private Connection dialog box, 253, 253
- Connection Availability screen, 251, 251
- Connection Complete dialog box, 254, 254
- connection control fields, 57
- Connection Graphs category, 188
- connection-oriented communications, 56–58, 58, 60
- connectionless communications, 56–57, 59–60, 59
- connections between objects, 11, 11
- consoles
  - in IDS, 192, 198
  - in VSR, 302, 304, 307, 311
- consolidated equipment as single points of failure, 287
- Constraint Shortest Path First (CSPF), 55
- constraints
  - in relationship sets, 13–14, 13–14
  - in systems analysis, 6–9
- constructivity in Systems Theory, 3
- content keyword, 208
- context filtering, 161
- Continue Replicating after Synchronization option, 310
- Control Bits field, 115
- control-flag entry, 391–392
- convergence
  - in distance vector routing, 48–50
  - in link state routing, 52
- CoS field, 54
- COSE (Common Open Software Environment), 380
- costs
  - in systems analysis, 6–9
  - of viruses, 257–258
- count to infinity, 50
- courses of action, 8
- CR-LDP, 55
- Cracking DES*, 226
- CRCs (cyclic redundancy checks)
  - in frame check sequences, 32
  - in layer 3 switching, 108
  - in routers, 106–107
  - for viruses, 268–269
- Create Host/Network dialog box, 170–171, 171
- credibility, importance of, 27
- Critical level of service, 56
- crypto algorithms, 220
- crypto keys, 220
- cryptoAPI, 374
- cryptography. *See* encryption

CSMA/CD (Carrier Sense Multiple Access with Collision Detection),  
91, 284

CSPF (Constraint Shortest Path First), 55

csv formatting modules, 209

*Cuckoo's Egg* (Stoll), 194

Custom shared folders setting, 338

cut-through proxies, 163

CyberCop Server, 202–203

cyclic redundancy checks (CRCs)

in frame check sequences, 32

in layer 3 switching, 108

in routers, 106–107

for viruses, 268–269

## D

d file type, 384

daemons, Unix, 137

data

in Ethernet frames, 32

integrity of, 372

in systems analysis, 9–10

Data Encryption Standard (DES), 222, 228

in IPsec, 372

keys in, 226

for passwd files, 388

Data Link Connection Identifiers (DLCIs), 98

data link layer, 38, 40–41

data manipulation, NIDS detection of, 197

data ports for FTP, 66–67

data streams

viruses in, 261

in VPN, 255–256, 255

data translation, 80

databases

in Snort, 209, 213

vulnerability, 444–445

Datacenter Server, 374

date stamps, virus modification of, 261

DC (direct current) circuits, 85

DCOM (Distributed Component Object Model), 356–360, 357–358

DDoS (Distributed Denial of Service) attacks, 80

de facto standards, 63

decision analysis, 5

dedicated hardware and software for VPN, 243

dedicated WAN link replacement, 238–240, 240

default settings

in .NET Security Policy, 376

templates for, 330

Default User Properties dialog box, 338, 338

defense in depth, 8, 21

defining alternatives, 9

definition in network usage policies, 458

delegated authentication in Kerberos, 366

delegation of authority in Active Directory, 318

demilitarized zones (DMZs), 150–151, 161

demodulators, 88

denial of service (DoS) attacks

buffer overflow, 432–433

Smurf, 434–435

teardrop, 195–197, 195, 433–434

translation rules for, 184

department communications, firewalls for, 114

dependencies checks, 401

DES (Data Encryption Standard), 222, 228

in IPsec, 372

keys in, 226

for passwd files, 388

Description field, 167

design review in SDLC, 24

desktop applications, support for, 316

desktop functionality in Active Directory, 318

desktop systems, virus protection for, 273–274

Destination Address screen, 251, 251

Destination Host/Network field

for AAA rules, 174

for access rules, 166

for filter rules, 179

Destination port, 170

Destination Unreachable value, 119

destinations, verifying, 219–220

development and acquisition in SDLC, 24

DHCP (Dynamic Host Configuration Protocol), 68–70, 187–188

DHCP Proxy service, 247

DHCP relay agent, 349

DHCP server, 349

dial backups, 288

dial-in modem pools, 114

dictionary files in brute force attacks, 436–437

DID (Direct Inward Dial) phone service, 417

differential backups, 296–297

Diffie, Whitfield, 223

Diffie-Hellman algorithm, 223, 372

digital certificate servers, 229

digital certificates, 331, 370–371

digital communications, 83–84, 84

digital signatures

in public key cryptography, 223, 370–371

in System Integrity Verifiers, 193

Digital Subscriber Line (DSL), 285

direct current (DC) circuits, 85

Direct Inward Dial (DID) phone service, 417

direction descriptors, 112

direction of flow in Snort, 207

Directory Auditing dialog box, 343, 344

Directory Permissions dialog box, 342–343, 342

Disable Registry setting, 339

disabling

EFS, 366

- inetd service, 409–410
- stand-alone services, 410–411
- disasters, 277
  - categories of, 278
  - documenting procedures for, 301
  - extreme, 299–301
  - from media, 278–280
  - network, 278–280
  - server. *See* server disasters
  - simulating, 300
  - topologies in
    - configuration files for, 288–289
    - LAN, 280–284, 282–283
    - single points of failure in, 286–288
    - WAN, 284–286
  - VSR for. *See* VSR (Veritas Storage Replicator)
- disconnected mode in IMAP, 75
- discovery
  - in LDP, 55
  - in network usage policies, 458
- disk duplexing, 292
- disk mirroring, 278, 291–292
- disk quotas, 328
- disk space for IDS, 192–193
- dispersion with fiber optic cable, 87
- disposal in SDLC, 28
- distance vector routing, 45
  - problems with, 48–50, 49
  - propagating information on, 45–48, 45
- distances in DSL, 285
- Distributed Component Object Model (DCOM), 356–360, 357–358
- Distributed Denial of Service (DDoS) attacks, 80
- distribution modes in LDP, 55
- DLCIs (Data Link Connection Identifiers), 98
- DMZs (demilitarized zones), 150–151, 161
- DNS (Domain Name Services), 70–72, 70
  - in Active Directory, 317
  - with NIDS, 199–200
  - in NT Server, 349
  - in PIX firewall, 164
  - port numbers for, 118
  - in Unix, 403
- DNS poisoning, 220
- dnsspoof tool, 431
- Do Not Dial the Initial Connection option, 251
- Do not display last logon name setting, 338
- Do Not Overwrite Events option, 345
- documentation of disaster procedures, 301
- domain controllers, 320–321
- Domain Name Services. *See* DNS (Domain Name Services)
- domain trusts, 321
- domains
  - in Unix, 386
  - whois command for, 416
  - in Windows 2000, 320–321

- DoS (denial of service) attacks
  - buffer overflow, 432–433
  - Smurf, 434–435
  - teardrop, 195–197, 195, 433–434
  - translation rules for, 184
- dropper programs, 260
- DSL (Digital Subscriber Line), 285
- dsniff tools, 431
- Dummy Net Driver Support? option, 399
- dumpster diving, 417
- duplexing, disk, 292
- dying gasps, 52
- dynamic filtering, 134
- Dynamic Host Configuration Protocol (DHCP), 68–70, 187–188
- dynamic information in SNMP, 78
- dynamic NAT, 171–172
- dynamic packet filtering firewalls, 60, 123
  - operation of, 123–128, 123–127
  - supported transports in, 128
  - for UDP traffic, 128
- dynamic rekeying, 372
- dynamic routing, 44
- dynamic rules, 171
- Dynamic section, 207

## E

- e-mail
  - IMAP for, 74–76
  - in network usage policies, 463
  - POP for, 73–74
  - SMTP for, 77–78
  - spoofed, 64–65, 64–65
  - in Unix, 405
  - viruses attached to, 272
- EAP (Extensible Authentication Protocol), 231
- ECC (Error Correction Code), 292–293
- Echo Reply value, 119
- echo requests
  - in ICMP, 119
  - in Smurf attacks, 434–435
- Echo service, 352
- Echo value, 119
- Edit Address Rule dialog box, 183
- Edit Host/Network dialog box, 171, 171
- .edu domain, 70
- EFS (Encrypting File System), 364–366, 365
- 802.11a standard, 94
- 802.11b standard, 283–284
- EISA, VLB, PCI and on Board Controllers? option, 400
- El Gamal algorithm, 193
- electromagnetic interference (EMI), 85–86, 85, 279
- embedded firewalls, 133
- Embryonic Limit option, 184
- emergency repair disks, SAM files on, 323

- employee productivity in network usage policies, 457
  - Enable Security option, 353
  - Enable SNMP updates setting, 337
  - enabling
    - packet filtering, 353, 353
    - profiles, 339
  - Encapsulating Security Protocol (ESP), 230, 372
  - Encrypt Contents to Secure Data option, 365–366
  - Encrypted Data Recovery Agents node, 366
  - encrypted passwords, crackers for, 436–437
  - Encrypting File System (EFS), 364–366, 365
  - encryption, 80, 215, 220–221
    - block cipher, 222–223
    - brute force attacks on, 225–226
    - cipher deficiencies in, 225
    - DES, 228
    - digital certificate servers, 229
    - government intervention in, 227
    - human error in, 224
    - IP Security, 229–230
    - Kerberos, 230–231
    - need for, 227–228
    - in OSPF password authentication, 53
    - in passwd files, 388
    - PPTP, 231
    - public/private crypto keys, 223
    - of radio wave transmissions, 88
    - RADIUS, 231–232
    - RSA, 232
    - security tokens, 233–234
    - SKIP, 234
    - SSH, 232
    - SSL, 232–233
    - stream cipher, 221–222
    - of viruses, 262, 270
    - in VPN. *See* VPN (virtual private networking)
    - weaknesses in, 224–227
  - encryption domains in VPN, 236–237
  - end-to-end leased line connectivity, 96
  - Enter Network Password dialog box, 159, 159
  - Enter Serial Number dialog box, 306, 307
  - Enterprise level, 375
  - Enterprise Server, 374
  - Entire Scheduled Starts option, 311
  - entities in Kerberos, 367
  - entropy of systems, 2
  - environments, 8
  - EQL (Serial Line Balancing) Support? option, 399
  - Error Correction Code (ECC), 292–293
  - eSoft InstaGate Pro firewalls, 150–151
  - ESP (Encapsulating Security Protocol), 230, 372
  - /etc/fstab file, 76
  - /etc/securetty file, 392–393
  - Ethernet (10 or 100Mbit): option, 399
  - Ethernet communications, 91–93, 92, 281
  - Ethernet frames, 31–32
    - data in, 32
    - frame check sequences in, 32
    - headers in, 32–35
    - preambles in, 32
  - event-based triggers, 15
  - Event Log node, 328
  - Event Log Settings dialog box, 344–345, 345
  - Event Viewer, 344–346, 345, 363
  - EventReporter, 346
  - events in NT Server, 344–346, 345, 363
  - everyone class, 382–383
  - evolvability in Systems Theory, 3
  - Exact Replica On Target option, 309
  - EXE files, 259
  - exec daemon, 404–405
  - executable files, 259
  - execute permission, 384
  - execution of infected files, 259
  - executive summaries, 24
  - exhaustive key searches, 225–226
  - Existing Replication Neighborhood option, 303
  - Explain tab, 328
  - exporting file systems, 76
  - Extensible Authentication Protocol (EAP), 231
  - Extensible Markup Language (XML), 374
  - extensible schema, 317
  - external connections, firewalls for, 114
  - external reviews, 23
- ## F
- Failover category, 187
  - false positives in virus monitoring, 269–270
  - Fast alerts in Snort, 205
  - FAT file system, 339
  - fault tolerance
    - RAID for, 291–293
    - redundant servers for, 293–294, 294
  - FCSs (frame check sequences), 32
  - FDDI (Fiber Distributed Data Interface) topology, 281–282, 282–283
  - FDDI Driver Support? option, 400
  - FEC (Forwarding Equivalency Class), 54
  - fiber optic cable, 86–88, 86, 279
  - file access events, auditing, 346
  - file requests in OSI Reference Model, 40–41, 41
  - file rights and permissions
    - in NT Server, 341–344, 342, 344
    - in Unix, 382–386
    - in Windows 2000, 364
  - file system
    - in NT Server, 339–344, 340–342
    - in Unix, 382–386
  - File System node, 329

File Transfer Protocol. *See* FTP (File Transfer Protocol)

files

- infection of, 259
- integrity checks for, 276

filesnarf tool, 431

filesystem IDS

- in NIDS, 204
- in System Integrity Verifiers, 193

filtering and filter rules

- audit events, 346–347
- dynamic packet filtering firewalls for, 123–128, 123–127
- hostile code, 132
- NIDS manipulation of, 201–202
- in PIX firewall, 161, 166, 175–179, 175–178
- by routers, 107
- stateful filtering firewalls for, 128–129
- static packet filtering firewalls for, 115–123, 115, 118–119
- in Windows NT, 353–356, 353–355

FIN flag

- in packet filtering firewalls, 126–127, 127
- in TCP flag field, 116–117

FIN scanners, 117, 425

Find command setting, 338

firewalls, 111

- address translation in, 142–145, 143
- in connection-oriented communications, 60
- definition of, 113
- deploying, 149–152, 149
- dynamic packet filtering, 123–128, 123–127
- with FTP, 67
- functions of, 133–134
- integration and access control in, 148
- for intrusion detection and response, 147–148
- logging and analysis for, 145–147, 146
- need for, 114
- vs. NIDS, 198
- PIX. *See* PIX firewall
- proxy servers. *See* proxy servers and clients
- selecting, 134–135
  - appliance-based, 141–142
  - server-based, 135–141
- stateful filtering, 128–129
- static packet filtering, 115–123, 115, 118–119
- third-party tools for, 148–149
- types of, 133
- for Unix, 397
- with VPN, 114, 147, 242–243

firmware, 142

fixed frequency signals, 88

flags

- in connection-oriented communications, 57
- in dynamic packet filtering firewalls, 124–126
- in IMAP, 74
- in static packet filtering firewalls, 115–117

flexibility in IPsec, 372

Flood Defender feature, 163

Flood Guard feature, 163

folder redirection, 327, 331

folders in IMAP, 75

footprints of viruses, 261

Forcibly Disconnect Remote Users setting, 333

forests in Active Directory, 317

formatting modules in Snort, 209

formulas for ciphers, 225

forwarding

- in PIX firewall, 161
- in Unix, 397

Forwarding Equivalency Class (FEC), 54

FragGuard feature, 163

Fragmentation Needed value, 120

fragmentation offset fields, 195–196, 434

fragmentation requests, 122

frame check sequences (FCSs), 32

frame relay technology, 96–98, 97, 285

frames

- Ethernet. *See* Ethernet frames
- vs. packets, 107

Framework Configuration tool, 376

FreeBSD operating system, 380–381

frequency

- and electromagnetic interference, 85
- of threats, 6, 8

From a Specified Range of Addresses option, 248

fstab file, 76

FTP (File Transfer Protocol), 66–67, 66–67

as clear text service, 218

passive, 67–68, 68

Telnet access to, 428

in Unix, 404

viruses in, 272

ftp.iana.org site, 359

Full alerts in Snort, 205

full backups, 295

Full Control access level, 341, 343, 364

full-duplex signals

- in FDDI, 281
- in T1, 96

Full Internal IPX Network? option, 398

functional requirements determination in SDLC, 23

functionality

- of components, 24
- of systems, 25

FunnyFile virus, 258

## G

gap analyses, 23

Gartner Research report, 277

gateways, 42, 130  
 General constraints, 13–14, 14  
 get command, 79  
 getnext command, 79  
 GIDs (Group IDs), 382  
 global address books, 73–74  
 Global Sign-On (GSO) product, 230  
 goals, 6  
 Good Times virus hoax, 264  
 .gov domain, 70  
 government, encryption intervention by, 227  
 grain of salt key, 388  
 great Internet worm, 265–266  
 grep command, 409, 411  
 group file, 382, 389–390  
 group folders in IMAP, 75  
 Group IDs (GIDs), 382  
 Group Policy tab, 366  
 groups  
   permissions for, 382–383  
   policies for, 140, 323–324, 338–339, 338  
     in Active Directory, 317  
     for .adm files, 327–328  
     for administrative templates, 325–327, 327  
     Computer Configuration node for, 325, 325  
     extensions for, 326–327  
     for folder redirection, 331  
     for Registry, 328  
     for scripts, 331  
     for security, 328–329  
     for security templates, 329–330  
     for software installation, 330–331  
     User Configuration node for, 325–326, 326  
   in Unix, 382, 385–386, 389–390  
 GSO (Global Sign-On) product, 230

## H

h-node systems, 352  
 half scanning, 425  
 handshaking  
   in connection-oriented communications, 57, 60  
   in FTP, 66–67  
 hardware firewalls, 133  
 hardware for VPN, 243  
 headers  
   in Ethernet frames, 32–35  
   information in, 420–421  
 Hellman, Martin, 223  
 Hepps, Jon, 265  
 heuristic virus scanners, 271–272  
 HHTTP Decode preprocessor, 208  
 hidden accounts  
   by 3COM, 267–268, 430  
   for attacks, 430

hidden node in WLANs, 284  
 Hide drives in My Computer setting, 339  
 Hide Network Neighborhood setting, 339  
 hiding  
   last logon names, 362  
   NAT, 144  
 HIDS (Host Intrusion Detection systems), 191  
 High Secure category, 330  
 hijacking, session, 218–219, 219, 431  
 Hisecdc.inf file, 330  
 Hisecws.inf file, 330  
 History Metrics category, 187  
 hives in Registry, 316  
 hoaxes, 18, 263–264  
 honeypots, 194–195  
 hops, 42, 46–47  
 host-based IDS, 202–203, 204  
 host descriptors, 112  
 Host Intrusion Detection systems (HIDS), 191  
 host names, DNS for, 70–72, 70  
 host scanning, 423  
 Host Unreachable value, 120  
 hostile code, filtering, 132  
 hosts, firewalls for, 114  
 hosts.allow file, 411–412  
 hosts.deny file, 411–412  
 hosts.equiv file, 405  
 hosts.lst file, 419–420  
 Hosts/Network tab, 185, 186  
 hot swappable RAID systems, 291  
 hotfixes in Active Directory, 319  
 Hotmail users, filter rules for, 177  
 HTTP (Hypertext Transfer Protocol), 72–73  
   as clear text service, 218  
   Telnet access to, 428  
   in Unix, 404  
   viruses in, 272  
 httpd process, 404  
 HTTPS (Secure Hypertext Transfer Protocol), 233  
 hubs, 99–100, 287

## I

IANA (Internet Assigned Numbers Authority), 63  
 IBSS (Independent Basic Service Set), 283  
 ICMP (Internet Control Message Protocol) traffic  
   in Snort, 207  
   static packet filtering firewalls for, 118–122, 119, 121  
 IDS (intrusion detection systems), 65, 191  
   firewalls for, 147–148  
   honeypots, 194–195  
   host-based, 202–203, 204  
   Log File Monitors, 193–194  
   NIDS. *See* NIDS (Network Intrusion Detection Systems)  
   System Integrity Verifiers, 193

- for teardrop attacks, 195–197
- types of, 191–192
- IDS Discussion List mailing list, 448
- IEFT (Internet Engineering Task Force) standards, 228
- IIS (Internet Information Server), 350
- IKE (Internet Key Exchange), 230
- ILOVEYOU worm, 132, 265
- IMAP (Internet Message Access Protocol), 74–76
  - as clear text service, 218
  - Telnet access to, 428
  - in Unix, 404
- implementation
  - in network usage policies, 459
  - in SDLC, 26
- Inclusion/Exclusion dialog box, 311
- incremental backups, 296
- incremental security templates, 329
- Independent Basic Service Set (IBSS), 283
- iNet Tools utility, 423–424, 423–424
- inetd.conf file, 407–409
- inetd process, 62
- inetd servers, 407–410
- InetPub directory, 350
- inetres.adm file, 328
- infection of files, 259
- information, 2
- Information Reply value, 120
- Information Request value, 120
- Information Theory, 2
- InfoSec News mailing list, 447
- infrastructure
  - in 802.11b networks, 283
  - in WiFi, 93
- initialization vectors (IVs), 222, 222
- initiation in SDLC, 22
- INND (InterNetNews daemon), 405
- inoculation for viruses, 260
- installing
  - PDM, 156–159, 157–158
  - PIX firewall, 154–161, 155
  - software, 330–331
  - VSR, 303–304, 303–304
- integration in firewalls, 134, 141, 148
- integrity checks for files, 276
- interception protection, 372
- Interface field
  - for AAA rules, 174
  - for access rules, 166
- Interface Graphs category, 188
- Interfaces category, 187
- interference, electromagnetic, 85–86, 85, 279
- internal attacks, 200
- International Standards Organization (ISO), 37
- Internet
  - for backups, 297
  - in network usage policies, 462–463
- Internet Assigned Numbers Authority (IANA), 63
- Internet Connection screen, 247, 247
- Internet Connection Sharing screen, 252, 252
- Internet Control Message Protocol (ICMP) traffic
  - in Snort, 207
  - static packet filtering firewalls for, 118–122, 119, 121
- Internet daemon (inetd) process, 62
- Internet Engineering Task Force (IEFT) standards, 228
- Internet Explorer Maintenance, 327
- Internet Information Server (IIS), 350
- Internet Key Exchange (IKE), 230
- Internet Message Access Protocol (IMAP), 74–76
  - as clear text service, 218
  - Telnet access to, 428
  - in Unix, 404
- Internet Protocol (IP) in Snort, 207
- Internet protocols in Active Directory, 318
- Internet Relay Chat (IRC), 80
- Internet Security Association and Key Management Protocol (ISAKMP), 373
- Internet worm, 265–266
- InterNetNews daemon (INND), 405
- InterNIC database, 416–418
- InterNIC site, diversions from, 220
- interoperability
  - in Active Directory, 318
  - in Kerberos, 367
- InterScan VirusWall product, 272
- interviews, 23
- Intrusion Detection category, 187
- intrusion detection systems. *See* IDS (intrusion detection systems); NIDS (Network Intrusion Detection Systems)
- IP (Internet Protocol) in Snort, 207
- IP: Accounting? option, 397
- IP Address Assignment screen, 247, 247
- IP addresses
  - bootp and DHCP for, 68–70
  - DNS for, 70–72, 70
  - in Snort, 207
  - in VPN, 239, 251
  - whois command for, 418
- IP: Aliasing Support? option, 397
- IP: Allow Large Windows? option, 398
- IP: Disable Path MTU Discovery? option, 397–398
- IP: Drop Source Routed Frames? option, 398
- IP: Firewall Packet Logging? option, 397
- IP: Firewalling? option, 397
- IP: Forwarding/Gateway? option, 397
- IP: Multicasting? option, 397
- IP: Optimize as Router Not Host? option, 397
- IP payload compression (IPcomp), 230

IP: PC/TCP Compatibility Mode? option, 397  
 IP: Reverse ARP? option, 397  
 IP Security (IPSEC), 229–230, 372–373  
 IP services, 348–352, 348, 350–351  
 IP: Tunneling? option, 397  
 IPcomp (IP payload compression), 230  
 IPSEC (IP Security), 229–230, 372–373  
 IPX protocol in Unix, 398  
 IPX Protocol? option, 398  
 IRC (Internet Relay Chat), 80  
 ISA Server, 140  
 ISAKMP (Internet Security Association and Key Management Protocol), 373  
 ISDN, 285, 288, 400  
 ISDN Support? option, 400  
 ISO (International Standards Organization), 37  
 isolation by bridges, 101  
 IVs (initialization vectors), 222, 222

## J

jabbering, 281  
 Java filtering, 164  
 Job Name dialog box, 309, 309  
 Jobs in VSR, 301, 303

## K

K-DUMP program, 368  
 Kashpureff, Eugene, 220  
 KDC (Key Distribution Center), 369  
 Kerberos, 230–231
 

- authentication service exchange in, 368–369
- client-server exchange in, 369
- ticket-granting service exchange in, 369
- in Windows 2000, 366–369

 Kerberos Authentication Service Requests, 369  
 Kernel Configurator dialog box, 402, 402  
 Kernel Daemon Configuration option, 402  
 kernel optimization for Unix, 393–394
 

- cleaning up work space, 401
- compiling kernel, 401–402
- configuring boot manager, 402
- configuring kernel, 394–401, 395–396
- dependencies checks, 401
- make for, 394
- network drive settings, 402–403, 402

 Kernel/User Network Link Driver? option, 398  
 Key Distribution Center (KDC), 369  
 key management, 370–371  
 Key Management Service (KMS), 371  
 Keyed Hashing for Message Authentication Code (KMAC), 372  
 keys
 

- encryption. *See* encryption
- in Registry, 316

KMAC (Keyed Hashing for Message Authentication Code), 372  
 Klez worm, 265  
 KMS (Key Management Service), 371

## L

l file type, 384  
 LOphT Heavy Industries site, 446  
 LOphTCrack utility, 436–437, 436  
 L2TP (Layer Two Tunneling Protocol), 231  
 Label Distribution Protocol (LDP), 55  
 Label field, 54  
 Label Switch Paths (LSPs), 54–55  
 label switching and MPLS, 53–56  
 LAN topologies, 280–284, 282–283
 

- Ethernet, 91–93, 92
- redundant routes in, 287
- wireless, 93–95

 laptop users, proxy clients for, 131  
 large environments, virus scanners for, 271  
 last logon name displays, 338, 362  
 layer 3 switching, 108–109  
 Layer Two Tunneling Protocol (L2TP), 231  
 LDAP (Lightweight Directory Access Protocol), 148, 318  
 LDP (Label Distribution Protocol), 55  
 lease periods in DHCP, 69  
 leased lines, 96, 284  
 LEDs (light-emitting diodes), 86, 155–156, 155  
 LegalNoticeCaption key, 362  
 LegalNoticeText key, 362  
 length
 

- cable, 279–280
- password, 332

 length fields
 

- in Ethernet header frames, 32
- in teardrop attacks, 195–196, 434

 levels
 

- in Bluetooth, 95
- for NT Server access, 341–343
- of risk in X-Force, 444

 LFMs (Log File Monitors), 193–194  
 liability in network usage policies, 457  
 light dispersion, 87  
 light-emitting diodes (LEDs), 86, 155–156, 155  
 light transmissions, 86–88, 86, 279  
 Lightweight Directory Access Protocol (LDAP), 148, 318  
 LILO boot manager, 402  
 Limit Memory to Low 16MB option, 396  
 line printer daemon (lpd), 350  
 Line Printer Remote (LPR), 350  
 Link Manager Protocol (LMP), 94  
 link state protocol (LSP) frames, 51  
 link state routing, 51
 

- convergence time with, 52

- in MPLS, 56
- propagating information on, 51
- routing failures in, 52
- security with, 52–53
- Linux operating system, 380, 394
  - kernel optimization for, 393–403
  - patches and updates for, 442
  - security checklist for, 453–455
  - server-based firewalls, 138–139
  - technical information for, 441
- List access level, 343
- List folder contents, 364
- LMP (Link Manager Protocol), 94
- Local Policies node, 328
- local profiles, 336
- Local Security Authority (LSA), 322
- locked accounts in passwd files, 387
- Lockout Duration setting, 333
- lockouts in NT Server, 333
- Log File Monitors (LFMs), 193–194
- Log On Locally right, 335
- Log section, 206
- log\_tcpdump formatting modules, 209
- logging. *See* logs and logging
- Logging category, 187
- logical connections, 11, 11
- logical networks, 42
- login daemon, 404–405
- logoff events, auditing, 346
- Logon Banner setting, 338
- logon banners, 338, 361–362
- logon events, auditing, 346
- logon names in RADIUS, 231
- logs and logging
  - for configuration files, 289
  - for firewalls, 145–147, 146
  - in IDS, 192
  - in network usage policies, 464
  - in NIDS, 204
  - in NT Server, 335, 344–346, 345, 363
  - in PIX firewall, 187
  - on remote systems, 203
  - in Unix, 396–397
- logto keyword, 208
- Long URL field, 179
- Love Bug virus, 257
- lpd (line printer daemon), 350
- LPR (Line Printer Remote), 350
- ls command, 383–384
- LSA (Local Security Authority), 322
- LSP (link state protocol) frames, 51
- LSPs (Label Switch Paths), 54–55

## M

- MAC (media access control) addresses
  - in bootp, 69
  - in Ethernet header frames, 33–34
  - in routers, 105
  - in switches, 103
- Mac operating system, server-based firewalls for, 135–136
- machine policies, 337–338, 337, 375, 377
- mail
  - IMAP for, 74–76
  - in network usage policies, 463
  - POP for, 73–74
  - SMTP for, 77–78
  - spoofed, 64–65, 64–65
  - in Unix, 405
  - viruses attached to, 272
- Mail Guard, 164
- mail headers, information in, 420–421
- mail slots for services, 61–62
- mail utility, 73
- mailing lists, 447–448
- mailsnarf tool, 431
- maintenance
  - of components, 25
  - in SDLC, 27–28
  - of systems, 25
  - for Unix, 414
- maintenance frames, 52
- make bzlilo command, 402
- make clean command, 401
- make config command, 394–395, 395
- make dep command, 401
- make menuconfig command, 395–396, 395
- Make New Connection Wizard, 250
- make xconfig command, 396, 396
- make zImage command, 401
- make zlilo command, 402
- man-in-the-middle attacks, 218–219, 219, 227–228, 430–432
- Manage Auditing and Security Logs right, 335
- Manage Global Address Pools dialog box, 181–182, 181
- management events, auditing, 346
- management information base (MIB), 78–79
- Managing Multiple Remote Access Servers screen, 248, 248
- mandatory profiles, 336
- Manifest, 375
- manual vulnerability checks, 427–429, 427
- many-to-one VSR model, 303
- maps in OSA, 13
- master boot sector replication, 260
- mathematical formulas for ciphers, 225
- Maximum Connection option, 184
- Maximum Password Age setting, 332
- Maximum Transfer Units (MTUs), 122, 397–398

media  
 problems from, 278–280  
 for transmissions, 89–90

media access control (MAC) addresses  
 in bootp, 69  
 in Ethernet header frames, 33–34  
 in routers, 105  
 in switches, 103

memory  
 for IDS, 192  
 for NT Server, 316  
 for Unix kernel, 396

memory-resident virus scanners, 271, 273–275

message classes in LDP, 55

message digests in OSPF, 53

messages. *See* mail

MetaFrame product, 243–244

MIB (management information base), 78–79

Microsoft  
 patches and updates for, 442  
 technical information for, 442  
 Trojan horses by, 267

Microsoft Baseline Security Analyzer, 319

Microsoft Cluster Server (MSCS), 293

Microsoft ISA firewalls, 150–151

Microsoft Management Console (MMC) plug-in, 245

Microsoft Network, Trojan horses on, 267

Microsoft Network Security Hotfix checker, 319

Microsoft Security Bulletin, 319

Microsoft Security Notification Service, 319

Microsoft TCP/IP Properties dialog box, 353

.mil domain, 70

MIME (Multimedia Internet Mail Extensions), 73, 78

Minimum Password Age setting, 332

Minimum Password Length setting, 332

mirroring, 278, 291–292

Miscellaneous Graphs category, 188

MMC (Microsoft Management Console) plug-in, 245

mobile users, proxy clients for, 131

models and terminology in systems analysis, 10–16, 11–15

modems and modem pools  
 in connection-oriented communications, 57  
 firewalls for, 114  
 VPN for, 237–238

modification protection, 372

Modify permission, 364

module-path entry, 391–392

module-type entry, 391–392

Monitor tab, 311, 312

monitoring  
 in attacks, 426–427, 426  
 clear text, 217–218  
 with Network Monitor, 351, 351  
 in PIX firewall, 187–189, 188  
 for Unix, 414

monitoring ports in switches, 103–104

Moore's Law, 27

Morris, Robert, 265–266

mount points in Unix, 382

mounting file systems, 76

MPLS (Multiprotocol Label Switching), 53–56

MSCS (Microsoft Cluster Server), 293

msg keyword, 208

msgsnarf tool, 431

MTUs (Maximum Transfer Units), 122, 397–398

Multi-String Editor dialog box, 358, 358

Multicast category, 187

multicasting, 187, 397

multihoming, 404

multimaster replication, 318

Multimedia and telephony protocols, 164–165

Multimedia Internet Mail Extensions (MIME), 73, 78

multimode fiber optic cable, 87

multiple access in CSMA/CD, 91

multiple collisions in CSMA/CD, 91

Multiprotocol Label Switching (MPLS), 53–56

mutation by viruses, 263, 270

mutation engines, 263

mutuality in Systems Theory, 2

myth of total security, 17–19

## N

names  
 domain. *See* DNS (Domain Name Services)  
 in Unix, 382  
 for VPN connections, 253

NASA, 21

NAT (network address translation)  
 for access rules, 171, 171  
 with DCOM, 359–360  
 in firewalls, 142–145, 143  
 with FTP, 67–68  
 in PIX firewall, 162, 171–172, 171–172, 182–184, 182–183  
 with VPN, 239  
 in WiFi, 93

National Security Agency (NSA), 227

National Security Institute (NSI) site, 446–447

NBAR (Network-Based Application Recognition), 130

NBNS (Net BIOS Name Server), 352

NCP (NetWare Core Protocol), 59

NCP Filesystem Support? option, 401

NE2000/NE1000 Support? option, 400

negative publicity considerations in network usage policies, 458

Nelson, Michael, 357–358

Net BIOS Name Server (NBNS), 352

.NET operating system, 140–141, 374–377

Net Unreachable value, 120

NetBIOS over IP service, 77, 165

- Netcat product
  - port scans fooled by, 356
  - VPN compromised by, 238
- NetIQ Security Analyzer, 319
- NetIQ Security Manager, 319
- NETLOGON share, 339
- nets in IRC, 80
- Netscape, encryption keys in, 226
- NetWare Core Protocol (NCP), 59
- network addresses
  - protocols in, 42
  - translation of. *See* NAT (network address translation)
- Network Aliasing? option, 396
- network analyzers, 216–217, 216–217
- Network-Based Application Recognition (NBAR), 130
- Network Connection Type screen, 250, 250
- Network Connection Wizard, 250–252, 250–252
- Network Device Support? option, 399
- network driver settings for Unix, 402–403, 402
- Network File System (NFS), 76
  - in connectionless communications, 59–60, 59
  - in Unix, 401, 406
- Network Firewall? option, 396
- Network Information Services (NIS), 386
- network interface cards (NICs), 281
- Network Intrusion Detection Systems. *See* NIDS (Network Intrusion Detection Systems)
- network layer, 38, 40–42
- network management in network usage policies, 460
- Network Monitor Agent, 351
- Network Monitor tool, 351, 351
- Network News Transfer Protocol (NNTP), 76–77
- network profiles, 336
- Network Properties dialog box, 348
- network protocols for routers, 105, 107
- network services, 60–65, 64
  - in access control policies, 112
  - bootp and DHCP, 68–70
  - DNS, 70–72, 70
  - FTP, 66–68, 66–68
  - HTTP, 72–73
  - IMAP, 74–76
  - IRC, 80
  - NetBIOS over IP, 77
  - NFS, 76
  - NNTP, 76–77
  - POP, 73–74
  - in probing networks, 423
  - SMTP, 77–78
  - SNMP, 78–79
  - SSH, 79
- network time protocol (NTP), 406
- network translation. *See* NAT (network address translation)
- network transmissions. *See* transmissions
- network usage policies. *See* security policies
- networking for Unix, 414
- Networking Support? option, 396
- networks, disasters in, 278–280
- New Job Wizard, 308–309, 308–309, 311, 311
- New Server Wizard dialog box, 305–307, 305–307
- news servers, 77, 405
- newsgroups
  - for attack prevention, 448
  - in network usage policies, 463
  - in NNTP, 76–77
- nexus.exe file, 346
- NFS (Network File System), 76
  - in connectionless communications, 59–60, 59
  - in Unix, 401, 406
- NFS Filesystem Support? option, 401
- NICs (network interface cards), 281
- NIDS (Network Intrusion Detection Systems), 192–193
  - attacks against, 198–200, 199
  - data manipulation detection by, 197
  - filter rule manipulation by, 201–202
  - fusion of, 204–205
  - limitations of, 195–202, 199
  - session disruption by, 200–201
  - Snort. *See* Snort NIDS
  - for teardrop attacks, 195–197, 195
- Nimda worm, 132, 265
- NIS (Network Information Services), 386
- nmbd daemon, 406
- NNTP (Network News Transfer Protocol), 76–77
- No Access access level, 341, 343
- No Changes on Target option, 309
- node addresses, 33–35, 34–36
- noise
  - in digital circuits, 83–86, 84–85
  - server problems from, 290
- non-routable protocols, 42
- nondestructive testing, 301
- None alert setting, 206
- nonrepudiation, 370
- nonresident replicating viruses, 259
- Novell
  - patches and updates for, 443
  - technical information for, 442–443
- NSA (National Security Agency), 227
- NSI (National Security Institute) site, 446–447
- nsi.org site, 447
- NT file system (NTFS)
  - in NT Server, 339
  - viruses in, 261
- NT Server, 315–316
  - auditing in, 343, 344, 346–347, 347
  - DCOM with, 356–360, 357–358
  - Event Viewer in, 363

- file system in, 339–344, 340–342
  - IP services for, 348–352, 348, 350–351
  - last logon names with, 362
  - logging in, 344–346, 345, 363
  - logon banner for, 361–362
  - packet filtering with, 353–356, 353–355
  - page files in, 363–364
  - policies and profiles in, 335–339, 336–338
  - ports used in, 360–361
  - Registry changes for, 361–364
  - security patches for, 347–348
  - user accounts in. *See* users and user accounts
  - virtual memory support in, 316
- NTBugtraq mailing list, 448
- Ntconfig.pol file, 339
- NTFS (NT file system)
- in NT Server, 339
  - viruses in, 261
- NTP (network time protocol), 406
- ## O
- Oakley Key Determination, 373
- object access events, auditing, 346
- object-based policies, 317
- Object-Behavior Model (OBM), 10, 14
- object classes, 11, 11
- Object-Interaction Model (OIM), 10
- object-level security, 318
- Object-Oriented Systems Analysis (OSA), 10–16, 11–15
- Object-Relation Model (ORM), 10–16, 11–15
- Object RPC, 356
- objectives in systems analysis, 6–9
- objects, 11–12, 11
- OBM (Object-Behavior Model), 10, 14
- ocfiles.inf file, 330
- ocfilesw.inf file, 330
- offline mode
- in IMAP, 74
  - in POP, 73
- OIM (Object-Interaction Model), 10
- on-demand virus scanners, 271, 273–275
- one-time pads, 222, 224
- one-to-many VSR model, 303
- one-to-one VSR model, 302
- one-way encryption, 388
- one-way trusts, 321
- online mode
- in IMAP, 74
  - in POP, 73
- open level in Bluetooth, 95
- Open Shortest Path First (OSPF)
- password authentication in, 52–53
  - security in, 218
- Open System Interconnection. *See* OSI (Open System Interconnection) Reference Model
- OpenBSD operating system, 138
- OpenView, 148–149
- operating systems, virus protection for, 274–275
- operation and maintenance in SDLC, 27–28
- operators in IRC, 80
- optimizing Unix kernel, 393–394
- cleaning up work space, 401
  - compiling kernel, 401–402
  - configuring boot manager, 402
  - configuring kernel, 394–401, 395–396
  - dependencies checks, 401
  - make for, 394
  - network drive settings, 402–403, 402
- optional flag, 392
- Options field, 179
- .org domain, 70
- organizations in systems analysis, 10
- ORM (Object-Relation Model), 10–16, 11–15
- OS X server-based firewalls, 135
- OSA (Object-Oriented Systems Analysis), 10–16, 11–15
- OSI (Open System Interconnection) Reference Model, 37–38, 39
- application layer, 39–40
  - data link layer, 38
  - file requests in, 40–41, 41
  - network layer, 38, 42
  - physical layer, 38
  - presentation layer, 39
  - receiving data in, 41–42
  - session layer, 39
  - transport layer, 38
- OSPF (Open Shortest Path First)
- password authentication in, 52–53
  - security in, 218
- Other ISA Cards? option, 400
- out-of-band processing, 116
- output modules in Snort, 212
- overflow of buffer attacks, 432–433
- overhead in transmissions, 84
- owner permissions, 382–383
- ownership
- in NT Server, 344
  - in Unix, 385–386
- ## P
- p-node systems, 352
- packet analyzers
- and link state routing, 52
  - in man-in-the-middle attacks, 430
- packet filtering
- dynamic, 123–128, 123–127
  - stateful, 128–129, 161
  - static, 115–123, 115, 118–119
  - in Windows NT, 353–356, 353–355
- packet forwarding, 161
- Packet Storm vulnerability engine, 444–445

- packet-switched technologies, 96, 285
- packets vs. frames, 107
- padding in Ethernet frames, 32
- page files, 363–364
- PAM (Pluggable Authentication Module), 391–392
- pam.conf file, 391–392
- Parameter Problem value, 119
- Participation constraints, 13, 13
- Pass section in Snort, 206
- passfilt.dll file, 334
- passive FTP (PASV FTP), 67–68, 68
- passive monitoring
  - in attacks, 426–427, 426
  - of clear text, 217–218
- Passport, 375
- passwd file, 382, 386–389
- password crackers, 436–437, 436
- Password Uniqueness setting, 332–333
- passwords
  - in Active Directory, 318
  - in Kerberos, 230, 369
  - in link state routing, 52–53
  - in network usage policies, 460–461
  - in NT Server, 332–334
  - in PAM, 391–392
  - for PIX firewalls, 159–160
  - in RADIUS, 231
  - in security tokens, 233–234
  - in Unix, 386–389
- PASV FTP (passive FTP), 67–68, 68
- PAT (port address translation), 145, 180, 182
- patches
  - for NT Server, 347–348
  - for Unix, 413
  - vendor information for, 439–443
- path definitions in MPLS, 53
- PC/TCP protocol stack, 397
- PCI BIOS Support option, 396
- PDM (PIX Device Manager)
  - configuring, 159–161, 159–160
  - installing, 156–159, 157–158
- PDM Log category, 187
- PDM Users category, 188
- Perfect Forward Secrecy (PFS), 373
- performance
  - disabling services for, 409
  - of firewall-based VPN, 242
  - in layer 3 switching, 108
  - with RAID, 293
- permanent virtual circuits (PVCs)
  - in ATM, 98–99
  - in frame relay, 96–97
- Permission View tool, 376
- permissions
  - in NT Server, 339–344, 340–342
  - in Unix, 382–386
  - for virus protection, 261, 268, 274–275
  - in Windows 2000, 364
- persistence of Registry settings, 328
- personal identification numbers (PINs), 373
- personal Internet-based accounts, 463
- PFS (Perfect Forward Secrecy), 373
- PHF CGI attacks, 197
- phone numbers, whois command for, 417
- Phrack* Magazine home page, 447
- physical access attacks, 437–438
- physical layer, 38, 40
- physical location, whois command for, 417
- piconets in Bluetooth, 94
- PIF files, infection of, 259
- Ping of death, 202
- Ping packets in Smurf attacks, 434–435
- Ping scanning, 423, 423
- PINs (personal identification numbers), 373
- PIX Administration category, 187
- PIX Device Manager (PDM)
  - configuring, 159–161, 159–160
  - installing, 156–159, 157–158
- PIX firewall, 150–151, 153–154
  - access control in, 162–163
  - ASA in, 161–162
  - attack-specific protection in, 163–165
  - configuring, 161–165, 165
    - AAA rules in, 172–175, 172–173
    - Access Rules tab, 166–172, 167–171
    - filter rules in, 175–179, 175–178
    - Hosts/Network tab, 185, 186
    - monitoring in, 187–189, 188
    - Systems Properties tab, 186–187, 186
    - translation rules in, 179–187, 179–183
    - VPN for, 185, 185
  - installing, 154–161, 155
  - NAT in, 162, 171–172, 171–172, 182–184, 182–183
- PKI (Public Key Infrastructure), 370–371
- PKI-enabled applications, 371
- planning VSR, 302–303
- platform independence in VPN, 237
- PLIP (Parallel Port) Support? option, 399
- plug gateways, 130
- Pluggable Authentication Module (PAM), 391–392
- Pocket and Portable Adapters? option, 400
- point to point topologies, 95–96
- Point-to-Point Tunneling Protocol (PPTP), 231
- policies
  - in Active Directory, 317
  - group. *See* groups
  - and profiles, 335–339, 336–338

- security. *See* security policies
- User Manager
  - for accounts, 331–334
  - for users, 334–335, 334
- policy analysis, 5
- policy change events, auditing, 346
- polling in SNMP, 79
- polymorphic mutation, 263, 270
- POP (Post Office Protocol), 73–74
  - network analyzer view of, 216–217, 216–217
  - Telnet access to, 428
  - in Unix, 404
- port address translation (PAT), 145, 180, 182
- port numbers
  - in address translation, 144
  - in DNS, 118
  - in Snort, 207
- port scanners, 117
- port scanning
  - in packet filtering, 354–356, 354–355
  - in probing networks, 424–425, 424
- Port Unreachable value, 120
- portable features, 80
- ports
  - for DCOM, 357–359
  - for FTP, 66–67
  - for PIX firewall, 158, 158
  - for services, 61–62
  - well known, 63–65
  - for Windows services, 360–361
- Portscan preprocessor, 208
- POSIX file system, 382
- Post Office Protocol (POP), 73–74
  - network analyzer view of, 216–217, 216–217
  - Telnet access to, 428
  - in Unix, 404
- power problems, UPSs for, 290–291
- PPoE Client category in PIX firewall, 188
- PPP (Point-to-Point) Support? option, 399
- PPTP (Point-to-Point Tunneling Protocol), 231
- preambles in Ethernet frames, 32
- preinstallation checklist for Unix, 412
- Premium level service, 56
- preprocessors in Snort, 208–209, 212
- Prescan option, 309
- presentation layer, 39–40, 42
- previewing in IMAP, 75
- PRI ISDN, 288
- Printer Ports dialog box, 350, 350
- printing, TCP/IP, 350, 350
- privacy issues
  - in public key cryptography, 370
  - in security policies, 464
- private addressing. *See* addresses
- private data in access control policies, 113
- private keys, 365
- probing networks
  - FIN scanning for, 425
  - host and service scanning for, 423
  - Ping scanning for, 423, 423
  - port scanning for, 424–425, 424
  - TCP half scanning for, 425
  - traceroute command for, 421–422, 421–422
- problem scope, 6
- process, 1
  - security as, 17
    - myth of total security, 17–19
    - risk mitigation, 19–22
    - SDLC. *See* SDLC (System Development Life Cycle)
    - vigilance in, 28–29
- process monitoring for viruses, 269–270, 276
- process tracking events, auditing, 346
- processors
  - for IDS, 192
  - NT Server support for, 316
  - RISC, 108
- production honeypots, 194
- productivity in network usage policies, 457
- profiles
  - enabling, 339
  - and policies, 335–339, 336–338
  - in Windows 2000, 323
- promiscuous modes, 91–93, 92, 95
- Properties dialog box, 158, 158
- proprietary VPN, 241
- prosecution of virus creators, 258
- protection specifications development, 23–24
- Protocol Unreachable value, 120
- protocols, 36–37
  - clear text, 218
  - with DCOM, 357–358, 357–358
  - non-routable, 42
  - for proxy servers, 130
  - for routers, 105, 107
  - in Snort, 207
- proxy objectives, 7
- proxy servers and clients, 129, 134
  - benefits of, 130–131
  - configuring, 130
  - for filtering hostile code, 132
  - liabilities of, 131
  - operation of, 129–130, 129
  - transparent, 131–132
- PSH flag
  - in packet filtering firewalls, 125
  - in TCP flag field, 116
- public analysis of ciphers, 225
- public data in access control policies, 113

- public key algorithms, 223
- public key certificate services, 370–371
- Public Key Infrastructure (PKI), 370–371
- Public Network screen, 250, 250
- public/private key encryption, 223, 371
- publicity in network usage policies, 458
- published applications, 331
- PVCs (permanent virtual circuits)
  - in ATM, 98–99
  - in frame relay, 96–97

## Q

- Qchain utility, 319
- Qfecheck.exe program, 319
- QoS (Quality of Service)
  - in access control policies, 113
  - in MPLS, 56
- Quote of the Day service, 352

## R

- R commands, 405
- r permission, 384–385
- radiation, electromagnetic, 85–86, 85, 279
- Radio Network Interfaces? option, 399
- radio wave transmissions, 88–89
- RADIUS (Remote Access Dial-In User Service), 231–232
  - with firewalls, 148
  - for VPN connection, 249
- RAID (redundant array of inexpensive disks) protection, 291
  - RAID 0, 291
  - RAID 1, 291–292
  - RAID 2, 292
  - RAID 3 and RAID 4, 292
  - RAID 5, 293
- Randomize Sequence Number section, 184
- RC4 encryption, 226
- read rights and permissions
  - in NT Server, 341, 343
  - in Unix, 384
  - in Windows 2000, 364
- Read & Execute permission, 364
- readsm.exe utility, 436
- Reboot TARGET option, 307
- recommendations in specifications, 24
- recoverability in Internet backups, 297
- recovering from server disasters, 298–299
- Red Hat Linux, 394
- Redirect value, 119
- Redirect Datagram for the Host value, 121
- Redirect Datagram for the Network value, 121
- Reduced Instruction Set Computer (RISC) processors, 108
- redundancy
  - for LAN routes, 287
  - for servers, 293–294, 294

- reflexivity in Systems Theory, 3
- regedt32 tool, 316
- Registry
  - for DCOM, 357–358, 357
  - group policies for, 328–329
  - for NT Server, 316, 361–364
  - persistence of settings in, 328
  - in Windows 2000, 324
  - on workstations, 362–363
- Registry node, 329
- relationships, 11–13, 13–14
- release notes, 155
- remote access
  - with Network Monitor tool, 351, 351
  - in network usage policies, 462
- Remote Access Dial-In User Service (RADIUS), 231–232
  - with firewalls, 148
  - for VPN connection, 249
- Remote Client Protocols screen, 246, 246
- remote encryption domains, 236
- Remote Installation Services (RIS), 327–328
- Remote Procedure Calls (RPCs)
  - DCOM for, 356
  - RPC Configuration service for, 351
- remote systems, logs on, 203
- Remove Find command setting, 338
- Remove folders from Settings setting, 338
- Remove Run command setting, 338
- repair directory, SAM files in, 322, 436
- repetition with recursion, 22
- Replace Permissions on Existing Files option, 342
- Replace Permissions on Subdirectories option, 342
- replication
  - in Active Directory, 318
  - by viruses, 258–260
  - in VSR, 308–313, 308–313
- Replication Management Server (RMS), 302
- Replication Neighborhood, 302–304
- Replication Options dialog box, 309, 309
- Replication Pairs dialog box, 310
- Replication Rules dialog box, 310–311
- Replication Schedule dialog box, 311
- Replication Servers Select A Source Server dialog box, 310
- Replication Servers Select A Target Server dialog box, 310
- Replication Service Agent (RSA), 302
- Request to Send/Clear to Send (RTS/CTS) protocol, 284
- required flag, 392
- requisite flag, 392
- research honeypots, 194
- reservations in MPLS, 56
- Reset Count After setting, 333
- resident replicating viruses, 259
- resources
  - conservation of, 22
  - in network usage policies, 457

restart events, auditing, 346

Restricted Groups node, 329

Reverse Path Forwarding (Unicast RPF), 163

reviews

- in network usage policies, 459
- in SDLC, 24–25

rights events, auditing, 346

rights in NT Server, 334–335, 334

Rijndael block cipher, 228

RIP (routing information protocol), 42

- in distance vector routing, 45
  - problems with, 48–50, 49
  - propagating information on, 45–48, 45
- for Internet Protocol service, 351

RIPv2 in PIX firewall, 164

RIS (Remote Installation Services), 327–328

RISC (Reduced Instruction Set Computer) processors, 108

risk levels in X-Force, 444

risks

- assessment and analysis of, 7–8, 23
- in Internet backups, 297
- mitigating, 19–22, 457–458
- in systems analysis, 6–9

Ritchie, Dennis, 380

Rivest, Ron, 232

RJ45 connectors, 99

RMS (Replication Management Server), 302

RMS Retrieval dialog box, 303, 303

roaming profiles, 336

roles in access control policies, 113

root accounts in Unix, 383, 393

root names servers, 70–71

Router Advertisement value, 119

router-based VPN, 243

Router Selection value, 119

router switching, 108–109

routers, 42–43, 43, 105

- vs. bridges and switches, 107–108
- for dial backups, 288
- example, 105–107, 106
- network protocols for, 105, 107

routes, redundant, 287

Routing and Remote Access (RRAS), 245, 246, 249, 249

Routing and Remote Access Server Setup Wizard, 245–248, 246–248

Routing category, 187

routing failures in link state routing, 52

routing information protocol (RIP), 42

- in distance vector routing, 45
  - problems with, 48–50, 49
  - propagating information on, 45–48, 45
- for Internet Protocol service, 351

routing loops, 50

routing tables, 43–44

- for distance vector routing, 45–51, 45
- for link state routing, 51–53

- and MPLS, 53–56
- for static routing, 44–45

RPC Configuration service, 351

rpc.statd daemon, 138

RPCs (Remote Procedure Calls)

- DCOM for, 356
- RPC Configuration service for, 351

RRAS (Routing and Remote Access), 245, 246, 249, 249

RSA (Replication Service Agent), 302

RSA encryption, 232

RST flag, 116–117

RSVP-TE LDP, 55

RTS/CTS (Request to Send/Clear to Send) protocol, 284

Rudnyi, Evgenii, 322

Rule dialog box, 310–311, 310

rule headers, 206

rules

- NIDS manipulation of, 201–202
- in PIX firewall. *See* PIX firewall
- in Snort, 206–209, 213

Run command setting, 338

Run only allowed Windows applications setting, 339

Run setting, 337

## S

Sadmin worm, 20

SAG (segmentation and reassembly), 98

salt key, 388

SAM (Security Account Manager), 322–323

Samba programs, 77, 406

SANS (System Administration, Network, and Security) site, 446

SAs (security associations), 373

satellite transmissions, 89

saving network configuration files, 288–289

scalability in Active Directory, 318

scalable virus protection, 271

scaling domain trusts, 321

scanners

- virus, 271–275
- vulnerability, 428–429, 429

SCard COM, 374

scatternets in Bluetooth, 94

schema partitions, 320

scope

- defining, 6
- in network usage policies, 459

scripts

- filtering with proxies, 132
- and group policies, 326, 331
- limitations of, 321

SCSPs (Smart Card Service Providers), 374

SDLC (System Development Life Cycle), 22

- accreditation in, 27
- certification in, 25

- component and code review in, 24–25
- conceptual definition, 22–23
- design review in, 24
- development and acquisition in, 24
- disposal in, 28
- functional requirements determination in, 23
- implementation in, 26
- operation and maintenance in, 27–28
- protection specifications development in, 23–24
- system test reviews in, 25
- search engines for attacks, 420–421, 420
- secret keys
  - algorithms for, 223
  - in cryptography, 370
- Secure Category, 330
- Secure Hypertext Transfer Protocol (HTTPS), 233
- Secure Shell (SSH), 79, 232
  - for access rules, 167, 169–170
  - spoofing with, 431–432
  - for translation rules, 180
- Secure Shell Sessions category, 187
- Secure Sockets Layer (SSL), 157, 232–233
- Securedc.inf file, 330
- securetty file, 392–393
- Securaws.inf file, 330
- SecurID cards, 233, 233
- security
  - in connection-oriented communications, 60
  - in distance vector routing, 50–51
  - group policies for, 328–329
  - in link state routing, 52–53
  - as process, 17
    - myth of total security, 17–19
    - risk mitigation, 19–22
    - SDLC. *See* SDLC (System Development Life Cycle)
    - vigilance in, 28–29
  - in static routing, 44–45
  - as transmission medium issue, 90
- Security Account Manager (SAM), 322–323
- Security Alert dialog box, 159, 159
- Security Analyzer, 428–429, 429
- security associations (SAs), 373
- security equivalency in Unix, 405
- Security Identifiers (SIDs), 321–322, 322
- security levels in PIX firewall, 161
- security patches
  - for NT Server, 347–348
  - for Unix, 413
  - vendor information for, 439–443
- security policies
  - development process in, 458–459
  - incidents in, 464
  - Internet access policy in, 462–463
  - network management in, 460
  - password requirements in, 460–461
  - privacy and logging in, 464
  - remote network access in, 462
  - risk mitigation in, 457–458
  - scope in, 459
  - total cost of ownership in, 457
  - virus protection policy in, 461
  - in Windows .NET, 375–377
  - workstation backup policy in, 461
- Security tab, 340–341, 342
- security templates, 329–330
- security through obscurity, 200
- security tokens, 233–234, 233
- SecurityFocus vulnerability engine, 445
- segmentation and reassembly (SAG), 98
- Select Computer dialog box, 345, 345
- Select Host/Network dialog box, 168–169, 168
- Select Network Service dialog box, 348, 348
- Select The Destination Computer dialog box, 306, 306
- Select The Destination Path dialog box, 306, 306
- selection methodology in specifications, 24
- Sendmail program, 405
- sensitive information
  - as media issue, 89–90
  - in network usage policies, 458
- sensors, 192, 198–200
- sequence numbers in Ethernet frames, 32
- serial line balancing, 399
- server-based firewalls
  - Linux, 138–139
  - Mac, 135–136
  - .NET, 140–141
  - Unix, 136–138
  - Windows 2000, 140
  - Windows NT, 139–140
- server disasters, 290
  - ASPs for, 298
  - backups for, 295–297
  - clustering for, 294–295
  - RAID for, 291–293
  - recovering from, 298–299
  - redundant servers for, 293–294, 294
  - UPSs for, 290–291
- Server Group field, 174
- server rooms as attack targets, 90
- servers
  - disasters in. *See* server disasters
  - news, 77
  - proxy. *See* proxy servers and clients
  - verifying, 219–220
  - for VPN, 245–249, 246–249
- Service dialog box, 169, 169
- Service field
  - for access rules, 167
  - for filter rules, 179
- Service for AAA rules, 174

- Service Groups, 170
- service independence of VPN, 235, 237
- service name entry, 391–392
- services
  - in disaster recovery, 278
  - network. *See* network services
  - Unix, 137
- services file, 61–63, 407
- session disruption, 200–201
- session hijacking, 218–219, 219, 431
- session keyword, 208
- session layer, 39–40, 42
- Session Message Block (SMB) systems, 401
- sessions in PAM, 391
- set command, 79
- Set Module Options dialog box, 402, 402
- setup security.inf file, 330
- shadow passwords, 388–389
- Shamir, Adi, 232
- Shannon, Claude E., 2
- share permissions, 339–341, 340–341
- Shared Documents Properties dialog box, 340–341, 340, 342
- Shared tab, 340, 340
- Sharing setting, 337
- Shipley, Peter, 418
- Shock, John, 265
- “Shockwave Rider, The” (Brunner), 265
- Show Advanced User Rights option, 334
- shutdown events, auditing, 346
- Shutdown from Authentication Box setting, 338
- sid2user utility, 322, 322
- SIDs (Security Identifiers), 321–322, 322
- signature files in virus scanners, 270–271
- signatures
  - in public key cryptography, 223, 370–371
  - in System Integrity Verifiers, 193
- Simple Key Management for Internet Protocols (SKIP), 234
- Simple Mail Transfer Protocol (SMTP), 77–78
  - as clear text service, 218
  - Telnet access to, 428
  - in Unix, 405
- Simple Network Management Protocol (SNMP), 78–79, 352
  - as clear text service, 218
  - in NIDS, 204
  - in NT Server, 337
- Simple Network Markup Language (SNML), 209
- Simple TCP/IP services, 352
- simulating disasters, 300
- single-mode fiber optic cable, 87
- single points of failure in networks, 286–287
  - redundant LAN routes for, 287
  - WAN dial backups for, 288
- SIVs (System Integrity Verifiers), 193
- 62.5/125 cable, 86
- size of Event Viewer logs, 344
- SKIP (Simple Key Management for Internet Protocols), 234
- SLIP (Serial Line) Support? option, 399
- SM modes in Bluetooth, 95
- small footprints of viruses, 261
- Smart Card Service Providers (SCSPs), 374
- SmartCards, 373–374
- Smb alerts, 206
- SMB Filesystem Support? option, 401
- SMB (Session Message Block) systems, 401
- SMB Win95 Bug Workaround? option, 401
- smbd daemon, 406
- SMC cards, 400
- SMTP (Simple Mail Transfer Protocol), 77–78
  - as clear text service, 218
  - Telnet access to, 428
  - in Unix, 405
- Smurf attacks, 434–435
- SNML (Simple Network Markup Language), 209
- SNMP (Simple Network Management Protocol), 78–79, 352
  - as clear text service, 218
  - in NIDS, 204
  - in NT Server, 337
- SNMP management stations, 78
- snort.conf file, 211
- Snort NIDS, 205–206
  - configuring, 211–212
  - example, 213
  - hardware requirements in, 210–211
  - NIDS placement in, 210, 211
  - rules in, 206–209, 213
  - suggestions for, 213–214
- social engineering
  - attacks, 417
  - viruses, 263–264
- Socket alerts, 205
- sockets for services, 61–62
- SOCKS software, 130
- software
  - group policies for, 330–331
  - for VPN, 243
- software firewalls, 133
- Software Settings, 325–326
- Solaris/sadmind.worm, 20
- SonicWALL PRO 300 firewalls, 150–151
- Source Host/Network field
  - for AAA rules, 174
  - for access rules, 166
  - for filter rules, 179
- source ports
  - for access rules, 170
  - in address translation, 144
- Source Quench value, 119
- Source Route Failed value, 120

- source route frames, 398
- source servers in VSR, 301
- space-based transmissions, 89
- Space Travel game, 379–381
- Spade (Statistical Packet Anomaly Detection Engine) preprocessor, 208
- spam on newsgroups, 77
- Special Access access level, 343
- specific hosts in access control policies, 112
- speed in Internet backups, 297
- spoofing, 64–65, 64–66
  - with Echo service, 352
  - in man-in-the-middle attacks, 430–432
  - in Smurf attacks, 434–435
- spread spectrum signals, 88
- rttool, 302
- SSH (Secure Shell), 79, 232
  - for access rules, 167, 169–170
  - spoofing with, 431–432
  - for translation rules, 180
- sshitm tool, 431
- SSL (Secure Sockets Layer), 157, 232–233
- Stack field, 54
- stackable hubs, 287
- stand-alone services, disabling, 410–411
- Standard Server, 374
- standards
  - de facto, 63
  - in VPN, 241–242
- star topologies, 282
- state tables, 123
- stateful filtering, 128–129, 161
- stateless keyword, 208
- states of objects, 14
- static access rules, 171
- static filtering, 134
- static information in SNMP, 78
- static NAT, 144–145
- static packet filtering firewalls, 115, 115
  - for ICMP traffic, 118–122, 119, 121
  - TCP flag field in, 115–117, 115
  - for UDP traffic, 117–118, 118
- static routing, 44–45
- stations in 802.11b networks, 283
- Statistical Packet Anomaly Detection Engine (Spade) preprocessor, 208
- Status applet, 302
- stealth by viruses, 262
- Stoll, Clifford (*The Cuckoo's Egg*), 194
- Storage Replication Console dialog box, 304, 305
- Storage Replicator RSA option, 304
- Storage Replicator Setup dialog box, 304, 304
- Storm Watch feature, 444
- stream cipher encryption, 221–222
- Stream4 preprocessor, 208
- StreamFind utility, 261
- striping, 292–293
- structure in Active Directory, 317
- su command, 390
- sub-goals, 6
- subdomains, 71
- subnets, 42
  - with NIDS, 198–200, 199
  - whois command for, 418
- sufficient flag, 392
- Sun Microsystems
  - patches and updates for, 443
  - technical information for, 443
- sunsolve.sun.com site, 443
- Support Audio via ISDN? option, 401
- Support Generic MP (RFC 1717)? option, 401
- support.novell.com site, 443
- Support Synchronous PPP? option, 400
- SVCs (switched virtual circuits), 98–99
- switched environments, IDS for, 203, 204
- switched virtual circuits (SVCs), 98–99
- switches, 102–105, 103
  - vs. routers, 107–108
  - routing by, 108–109
  - for VLANs, 104–105
- symbols, 2
- SYN attacks
  - Flood Defender for, 163
  - operation of, 433
- SYN flag
  - in connection-oriented communications, 57–58, 60
  - in packet filtering firewalls, 124–126
  - in TCP flag field, 116–117
- synchronizing VSR jobs, 311, 312
- synchronous PPP, 400
- Syslog alerts, 205
- syslogd client, 346
- System Administration, Network, and Security (SANS) site, 446
- system capacity for VPN, 239
- system configuration for Unix, 412
- System Development Life Cycle. *See* SDLC (System Development Life Cycle)
- system events, auditing, 346–347, 347
- System Graphs category, 188
- System Integrity Verifiers (SIVs), 193
- system logs in NIDS, 204
- system messages in NIDS, 205
- System Policy Editor, 324, 336, 336
- System Properties tab
  - for AAA rules, 172
  - for filter rules, 176
- System Services node, 329
- system test reviews, 25
- systems analysis, 1
  - data in, 9–10

- introduction to, 1–6, 3
- models and terminology in, 10–16, 11–15
- objectives, constraints, risks, and costs in, 6–9
- organizations in, 10
- problem scope in, 6
- technology in, 10
- users in, 10

Systems Properties tab, 186–187, 186

Systems Theory, 2–3, 3

## T

T1 lines, 96, 284

TACACS+ (Terminal Access Controller Access Control System), 148

Talk service, 406

tape backups, 295–297

target servers in VSR, 301

targets as objectives, 6

TCO (total cost of ownership)  
with firewalls, 148

in network usage policies, 457

TCP (Transmission Control Protocol)

in LDP, 55

in PIX firewall, 162

in Snort, 207

TCP flag field, 115–117, 115

TCP half scanning, 425

TCP/IP Networking? option, 396

TCP/IP printing, 350, 350

TCP/IP Security dialog box, 353–355, 354

TCP/IP services, 352

TCP Wrapper, 411–412

tcpd daemon, 411

tcpkill tool, 431

tcpnice tool, 431

teardrop attacks

NIDS for, 195–197, 195

operation of, 433–434

technology in systems analysis, 10

Telnet

as clear text service, 218

in connection-oriented communications, 57–58, 58

for PIX firewalls, 160, 160

vs. SSH, 79

in Unix, 407

for vulnerability checks, 427–429, 427

Telnet Console Sessions category, 187

templates, 325–327, 327, 329–330

Terminal Access Controller Access Control System (TACACS+), 148

terminal logging for configuration files, 289

Terminal Services, 243

terrestrial transmissions, 89

testing

cable, 280

nondestructive, 301

VPN, 253–256, 253–255

TFTP (Trivial File Transfer Protocol), 157, 289

TGSs (Ticke-Granting Servers), 367

TGT return packets, 368

TGTs (Ticket-Granting Tickets), 367

third-party support, 443–444

for firewalls, 148–149

vulnerability databases for, 444–445

Thompson, Ken, 379–380

3COM Cards? option, 399

3COM company

back door accounts by, 267–268, 430

patches and updates from, 440

technical information from, 440

3DES encryption, 157

Ticke-Granting Servers (TGSs), 367

ticket-granting service exchange, 369

Ticke-Granting Tickets (TGTs), 367

tickets in Kerberos, 367

time division of T1 lines, 96

Time Exceeded value, 119

time reference servers, 406

time restrictions in access control policies, 112

time servers, 406

time to live (TTL) setting, 54, 71–72

timeouts in FTP, 68

Timestamp value, 120

Timestamp Reply value, 120

timestamps

in ICMP, 120

in Kerberos, 369

virus modification of, 261

token cards, 233–234, 233

Token Ring Driver Support? option, 400

Token Ring networks, 400

top-level domains, 70–71

topologies

ATM, 98–99

configuration files for, 288–289

frame relay, 96–98, 97

LAN, 90, 280–284, 282–283

Ethernet, 91–93, 92

redundant routes in, 287

wireless, 93–95

single points of failure in, 286–288

WAN, 95–96, 284–286

wireless, 99

Torvalds, Linus, 380–381

total cost of ownership (TCO)

with firewalls, 148

in network usage policies, 457

traceroute command, 421–422, 421–422

Traceroute value, 120

- traffic engineering, 55–56
- traffic isolation
  - by bridges, 101
  - in MPLS, 56
- training for systems, 25
- transitions in OSA, 14–15, 14–15
- Translate The DNS Replies That Match The Date option, 183
- translation, address
  - NAT. *See* NAT (network address translation)
  - PAT, 145, 180, 182
- Transmission Control Protocol (TCP)
  - in LDP, 55
  - in PIX firewall, 162
  - in Snort, 207
- transmissions, 83
  - bound and unbound, 87–89
  - clear text, 215–218, 216–217
  - digital, 83–84, 84
  - electromagnetic interference in, 85–86, 85
  - fiber optic cable for, 86–88, 86
  - media for, 89–90
- transmitting in the clear, 216
- transparent proxies, 131–132
- transport layer, 38, 40–41
- transport specific dynamic packet filtering, 128
- traps in SNMP, 79
- trees in Active Directory, 317
- triggers in OSA, 14–15, 14–15
- Triple DES standard, 226, 228
- Tripwire filesystem IDS, 193
- Trivial File Transfer Protocol (TFTP), 157, 289
- Trojan horses, 267–268
- troubleshooting, MAC addresses in, 33
- trust management in Kerberos, 367
- trusted devices in Bluetooth, 95
- trusted hosts daemons, 404–405
- trusts, domain, 321
- ttl keyword, 208
- TTL (time to live) setting, 54, 71–72
- tunneling
  - in Unix, 397
  - in VPN, 237
- turnkey firewall systems, 133
- twisted pair cabling, 86, 279
- two-way trusts, 321
- type fields
  - in Ethernet header frames, 32
  - in ICMP, 118–122
  - dynamic packet filtering firewalls for, 128
  - filtering, 355
  - in PIX firewall, 162
  - in Snort, 207
  - static packet filtering firewalls for, 117–118, 118
  - TCP Wrappers for, 411
  - for TFTP, 289
- UIDs (User IDs), 382
- unbound transmissions, 87–89
- Unicast RPF (Reverse Path Forwarding), 163
- unidirectional trusts, 321
- uninterruptible power supplies (UPSs), 290–291
- unit ID numbers for security tokens, 233
- Unix operating systems, 379
  - account administration in, 386–393
  - bootp server in, 403
  - DNS server in, 403
  - file system in, 382–386
  - FTP server in, 404
  - group files in, 389–390
  - history of, 379–381
  - HTTP server in, 404
  - IMAP and POP3 servers in, 404
  - inetd servers in, 407–410
  - kernel optimization for, 393–403, 395–396
  - login and exec daemons in, 404–405
  - mail servers in, 405
  - news servers in, 405
  - NFS servers in, 406
  - passwd files in, 386–389
  - permissions in, 382–386
  - root logon limitations in, 393
  - SAMBA tools in, 406
  - security checklist for, 412–414
  - server-based firewalls, 136–138
  - stand-alone services in, 410–411
  - Talk in, 406
  - TCP Wrappers in, 411–412
  - Telnet servers in, 407
  - time servers in, 406
  - virus protection for, 275–276
- unshielded twisted-pair cabling, 86, 279
- untrusted devices in Bluetooth, 95
- upper layer communications, 80–81
- upper port numbers, 63, 65
- UPSs (uninterruptible power supplies), 290–291
- URG flag, 116
- uricontent keyword, 208
- URL Filtering in PIX firewall, 164, 177, 187
- urlsnarf tool, 431
- Use VJ-Compression with Synchronous PPP? option, 400
- user behavior in NIDS, 205
- User Configuration node, 325–326, 326
- User Datagram Protocol (UDP). *See* UDP (User Datagram Protocol)

## U

### UDP (User Datagram Protocol)

- in connectionless communications, 59, 59
- for DHCP and bootp, 70

User IDs (UIDs), 382  
 User level, 375  
 User Licenses category, 188  
 User Manager policies  
   for accounts, 331–334  
   for users, 334–335, 334  
 User Must Log On in Order to Change Password setting, 333  
 user policy, 377  
 user rights, 334–335, 334, 346  
 User Rights Policy dialog box, 334, 334  
 user2sid utility, 322, 322  
 users and user accounts, 321  
   in access control policies, 112  
   in PAM, 391  
   in systems analysis, 10  
   in Unix, 386–393  
   in Windows 2000  
     policies for, 331–335, 334. *See also* groups  
     profiles for, 335–339, 336–338  
     SAM in, 322–323  
     SIDs in, 321–322, 322  
 uuencode program, 78  
 uuencode program, 78

## V

valid subnets, whois command for, 418  
 value of data as transmission medium issue, 89  
 vampire worms, 265  
 variables in Snort, 206, 212  
 VBScript scripts, 132  
 vendor information for attack prevention, 439–443  
 verification  
   of destinations, 219–220  
   in distance vector routing, 50–51  
 Veritas Storage Replicator (VSR), 301–302  
   configuring, 304–307, 305–308  
   installing, 303–304, 303–304  
   planning, 302–303  
   replication in, 308–313, 308–313  
 Vernam cipher, 221–222  
 vigilance, 28–29  
 Virtual Local Area Network (VLAN) technology, 104–105  
 virtual memory, NT Server support for, 316  
 Virtual Network Computers (VNCs), 243–244  
 virtual private networking. *See* VPN (virtual private networking)  
 Virtual Wide Area Networks (VWANS), 53  
 virus domains, 271  
 viruses, 19  
   access control for, 268  
   anti-virus countermeasures by, 262  
   application-level scanners for, 272  
   attribute manipulation by, 261  
   bombs, 263  
   checksum verification for, 268–269  
   concealment of, 261–263  
   deploying protection for, 272, 273  
   desktop system protection from, 273–274  
   encryption of, 262, 270  
   heuristic scanners for, 271–272  
   hoaxes, 18  
   in network usage policies, 461  
   polymorphic mutation by, 263, 270  
   process monitoring for, 269–270  
   replication by, 258–260  
   server protection from, 274–275  
   small footprints of, 261  
   social engineering, 263–264  
   statistics on, 257–258  
   stealth by, 262  
   vs. Trojan horses, 267  
   UNIX system protection from, 275–276  
   virus scanners for, 270–272  
   worms, 264–266  
 VLAN (Virtual Local Area Network) technology, 104–105  
 Vmyths.com page, 264  
 VNCs (Virtual Network Computers), 243–244  
 von Bertalanffy, Ludwig, 3  
 VPN (virtual private networking), 235  
   alternatives to, 243–244  
   authentication in, 241  
   client configuration for, 250–253, 250–253  
   dedicated hardware and software for, 243  
   diagrams of, 244, 245  
   encryption in, 241  
   firewalls for, 114, 147, 242–243  
   for modem pool replacement, 237–238  
   operation of, 235–237, 236  
   in PIX firewall, 185, 185  
   preparation for, 244  
   router-based, 243  
   selecting, 240–242  
   server configuration for, 245–249, 246–249  
   standards in, 241–242  
   system capacity for, 239  
   testing, 253–256, 253–255  
   for WAN link replacement, 238–240, 240  
 VPN Connection Graphs category, 188  
 VPN Statistics category, 188  
 VPN tab, 185, 185  
 VSR (Veritas Storage Replicator), 301–302  
   configuring, 304–307, 305–308  
   installing, 303–304, 303–304  
   planning, 302–303  
   replication in, 308–313, 308–313  
 vulnerability checks in attacks, 427–429, 427, 429  
 vulnerability databases, 444–445  
 VWANS (Virtual Wide Area Networks), 53

**W**

- w permission, 384–385
- waking up applications, 62
- WANK (Worms Against Nuclear Killers) worm, 266
- WANs (wide area networks), 95–96, 284–286
  - dial backups for, 288
  - VPN for, 238–240, 240
- war dialers, 418
- WatchGuard Firebox 2500 firewalls, 150–151
- Web Server, 374
- Web sites
  - for attack prevention, 446–447
  - in network usage policies, 463
- webmitm tool, 431–432
- webspay tool, 431
- well known ports, 63–65
- well known SIDs, 322
- WEP (Wired Equivalency Privacy), 93
- Western Digital/SMC Cards? option, 400
- white box view, 4
- whois utility, 416–418
- wide area networks (WANs), 95–96, 284–286
  - dial backups for, 288
  - VPN for, 238–240, 240
- WiFi standard, 93
- Windows 2000 operating system, 364
  - Active Directory for, 317–319
  - domain structure in, 320–321
  - Encrypting File System in, 364–366, 365
  - file permissions in, 364
  - IPsec in, 372–373
  - Kerberos in, 366–369
  - public key certificate services in, 370–371
  - security checklist for, 451–453
  - server-based firewalls, 140
  - SmartCards in, 373–374
- Windows Desktop environment, 139
- Windows Internet Name Service (WINS), 352
- Windows Media Player (WMP), 132
- Windows .NET, 140–141, 374–377
- Windows NT operating system, 139–140, 353–356, 353–355. *See also*
  - NT Server
- Windows Scripting Host (WSH), 331
- Windows services, ports for, 360–361
- Windows Settings, 325
- Windows Update, 318
- WinFrame product, 243–244
- Winlogon key, 362
- WINS (Windows Internet Name Service), 352
- winsock.dll file, 130–131
- Wired Equivalency Privacy (WEP), 93
- wireless LANs, 93–95
- wireless topologies, 99
- wiring closets, 90
- WLAN (802.11b) networks, 283–284
- WMP (Windows Media Player), 132
- workstations
  - in network usage policies, 461
  - securing Registry on, 362–363
- worms, 264–265
  - Internet, 265–266
  - vampire, 265
  - WANK, 266
- Worms Against Nuclear Killers (WANK) worm, 266
- write rights and permissions
  - in Unix, 384
  - in Windows 2000, 364
- write term command, 289
- WSH (Windows Scripting Host), 331
- wu-ftpd package, 138
- www.3com.com site, 440
- www.aionline.com site, 446
- www.atstake.com site, 446
- www.cert.org site, 446
- www.cisco.com site, 440
- www.linux.org site, 441
- www.march.co.uk site, 261
- www.microsoft.com site, 357, 442
- www.novell.com site, 442
- www.ntbugtraq.com site, 322
- www.phrack.org site, 447
- www.security.gatech.edu site, 457

**X**

- X.509 standard, 229
- X-Force IDS Discussion List mailing list, 448
- X-Force vulnerability database, 444
- x permission, 384–385
- xforce.iss.net site, 444
- xlates, 161
- XML (Extensible Markup Language), 374
- XML Digital Signature (XMLDSIG) specification, 374
- xml formatting modules, 209

**Y**

- Yankee Group study, 286
- Yellow Pages, 386
- Ylonen, Tatu, 232

**Z**

- zombies in IRC, 80
- zone transfers, 419–420
- zones, 42