

Index

3Com, 165
 100 percent outsourced IT, 20
 802.11 wireless standards, 318
 802.11i, 347

A

ACID (Analysis Console for Intrusion Databases), 2,
 201, 246
 ADODB, 247
 analyzing alert data, 255
 archiving alerts, 258
 ARIN lookup, 256
 carefully using names, 259
 categorizing alerts, 253
 common IP destination addresses, 255
 configuration page, 251
 configuring, 250–251
 daily use, 256–257
 GD, 248
 graphing data, 257–258
 information on alert types, 253–254
 installing, 249–250
 introduction to using, 251–252
 IP source address, 255–256
 JpGraph, 247–248
 main page, 251
 narrowing search criteria, 252
 overall statistics on database, 251–252
 PHPLOT, 247
 reverse DNS lookup, 255–256
 Sam Spade search, 256
 sensitive data, 254
 service being attacked most, 256
 Snort sensors, 248
 sorting alerts, 254
 SQL databases, 247
 statistics on AG (alert group), 252
 summary information on database AG
 (alert group), 252
 tuning and managing NIDS, 253–254
 variables for configuring, 250–251
 Web servers, 247
 ACID database, maintaining, 258
 acid_conf.php file, 250
 Ad-hoc mode, 317

Adleman, Leonard, 282
 ADODB, 247
 ADODB Web site, 247
 AeroSniff, 335
 AES, 284
 Afind utility, 376
 AH (Authentication Header), 285–286
 AirCERT, 247
 Airjack, 343
 AirSnort, 335, 346
 Anomalous IDS (intrusion detection system),
 194–195
 Anonymous Internet access, 320
 Antennas, 324
 Anti-virus software, 7, 12
 AP (access point), 317–319
 Apache Web servers, xi, 22, 244–245
 NCC (Nessus Command Center), 267
 PHP, 261
 Apache Web site, 244
 AppleTalk, 164
 Application layer, 57, 121–122
 Application ports, 2
 Applications
 exposing systems to vulnerability, 121
 getting data, 57
 on high port numbers, 90
 port numbers, 88–89
 testing for security holes, 122
 Arcnet, 164
 ARIN lookup, 256
 Armed forces, 352
 ARP (Address Resolution Protocol), 59, 166
 Asymmetric cryptography, 281–282
 AT&T, 13
 Attacks
 coming through firewalls, 194
 filing criminal charges, 350–351
 repeated evidence of, 355
 Authentication, 284
 /autopsy directory, 369
 Autopsy Forensic Browser, 368–370
 Auto-rooters, 9
 Availability, 5
 Awk, 13

B

Back Orifice, 95
 Back Orifice 2000, 95
 Backups

- baseline database, 230
- current and vulnerability scanning, 158–159

 Bandwidth, 7–8
 Baseline database, 230
 Bastille, 29–30
 Bastille Linux, 2, 27–30
 Bastille Web site, 28
 BBSs (Bulletin Board Systems), 13
 Beacon broadcasts, 321
 Beale, Jay, 28
 Bell Labs, 13
 Binary files, replacing with trojanized versions, 226–227
 BIND (Berkeley Internet Naming Domain), xi

- security holes, 126
- version of, 116

 Bindinfo file, 116
 Bison scripting language, 168
 Bit-wise copy, 366
 Blaster worm, 6
 Blowfish, 284
 Bounce Scan, 105
 Breadth, 346
 Break-ins, 3
 Broadband, 7–8
 Broadcast traffic, 165–166
 Brute force attacks, 130, 283
 Brute force login, 141
 BSD license, 13, 21, 23
 BSD license Web site, 23
 BSD mailing list archive, 382
 BSD UNIX, xi
 BSDI, 23
 BSSID (Basic Station System ID), 318
 Buffer overflow, 89–90, 124, 128, 130
 Bug finder/beta tester, 385
 Business information security risks, 9–12
 Business processes and firewalls, 60–61

C

Carrier, Brian, 368
 Center for Internet Security Web site, 45
 CERT (Computer Emergency Response Team), 6, 247
 CERT Web site, 247
 CertServer Web site, 298
 CGI directory, 114

CGI programs and Nessus, 133
 CGI scripts, default location for, 144
 Cgi-bin directory, 117
 Chain of trust, 299
 Chains, 64
 chargen service, 129
 Chat rooms, 19
 Cheswick, Bill, 125
 chmod command, 67
 Chrooted jail, 29
 C.I.A., 4
 Cisco Aeronet wireless cards, 335
 Cisco routers, 124
 Civic action, 352
 Class action suits, 10
 Cloud Nine Communications, 10
 Code

- permission to release as open source, 265
- viewing, 18

 Code Red worm, 5, 9–10, 123, 196
 ColdFusion, 126
 Commercial software products, 16–18
 Communications

- encrypting all, 43
- securing important, 3

 Compile-time parameters, 98
 Compiling from source code, 97–98
 comp.os.linux.advocacy newsgroup, 382
 comp.os.unix.bsd.freebsd.misc newsgroup, 382
 comp.os.unix.bsd.openbsd.misc newsgroup, 382
 comp.sci.opensource newsgroup, 382
 Computer crimes, 5–9, 194
 Computer forensics careers, 351–352
 Confidentiality, 4–5
 Connection, setting up and closing down, 57
 Copyright violations, 11
 Coroner's Toolkit, 3, 356, 368
 Corporate secrets and data disclosure, 11
 Cost of open source software, 15
 CPAN (Comprehensive Perl Archive Network)

- system, 237

 CSI (Computer Security Institute), 5–7
 Curses toolkit, 28
 Custom applications and vulnerability scanning, 160
 Customer lists, 11
 Cypherspace Web site, 287

D

DALnet, 13
 Danyliw, Roman, 247

- Data
 - encryption, 279
 - format readable by receiving party, 57
 - managing with databases and Web servers, 241–264
 - Data link layer, 55–56, 164
 - Data loss, 9
 - Databases
 - administrative activity, 200
 - baseline attributes of files, 226–227
 - external access into, 126
 - hackers, 126
 - intrusion detection data, 247
 - managing security data, 241–264
 - daytime service, 129
 - dd, 293, 365–368, 372
 - DDOS (distributed denial of service) attack, 7–8
 - Decrypt file, 345
 - Decrypting files, 299
 - Deep Throat, 95
 - Department of Homeland Security, 352
 - DES (Data Encryption Standard), 283
 - Destination machine dropping packets, 31
 - DHCP broadcast traffic, 165
 - Dial-up connections, 7
 - Diffie, Whitfield, 281
 - dig command, 37–39
 - Digital certificates, 284–285
 - Disaster Recovery Plan, 9
 - discard service, 129
 - Discussion groups, 385–386
 - D-Link wireless cards, 335
 - DMZ interface, 60
 - DMZ (Demilitarized Zone) segment, 74
 - DNS (Domain Name Servers), 58
 - responsible for domain name, 37
 - security holes, 126
 - DNS cache poisoning, 126
 - DNS lookup request and ping (Packet Internet Groper), 31
 - DNS servers, 126, 129
 - Documenting security activities, 60
 - Domains, 37–39
 - DoS (Denial of Service) attacks, 10, 131
 - dport statements, 68
 - dports flag, 68
 - Drivers, installing, 335–337
- E**
- Early warning system, 2
 - Easy CD creator, 78
 - echo replies (ping responses), 60
 - Echo Reply ICMP message, 31
 - Echo Request ICMP message, 31
 - echo service, 129
 - Education and open source software, 18–19
 - Electronic Freedom Foundation, 306
 - Ellis, James, 281
 - EMACS, 66, 113–114
 - EMACS home page, 114
 - EMACS Quick Reference, 114
 - Embarrassment, 10
 - Employee policy issues, 12
 - Encrypted files, 3
 - Encrypting files
 - all communications, 43
 - GnuPG (GNU Privacy Guard), 298
 - PGP (Pretty Good Privacy), 291–292
 - Encryption, 57
 - asymmetric cryptography, 281–282
 - data, 279
 - FreeS/WAN, 306–312
 - GnuPG (GNU Privacy Guard), 295–301
 - OpenSSH, 301–305
 - PKE (public key encryption), 281–282
 - protocols, 280
 - Public Key cryptography, 281
 - reversing process, 293
 - shared secret, 281
 - symmetric cryptography, 281
 - types of, 281–282
 - VPNs (Virtual Private Networks), 305
 - Encryption algorithms, 283–284
 - Encryption applications, 284–286
 - Encryption protocols, 285–286
 - Encryption software, 287–295
 - Ephemeral port numbers, 88–89
 - ESP packets, 309
 - /etc/freeswan/ipsec.conf file, 310
 - /etc/pcmcia/config.opts directory, 336
 - /etc/ssh directory, 303
 - /etc/ssh file, 303
 - Ethereal, 2, 309
 - application server troubleshooting, 190
 - benefits, 183–184
 - capture options, 188
 - compiling, 185
 - display options, 189–190
 - graphical interface, 183
 - GTK development libraries, 184
 - information about packets, 185, 187
 - libpcap libraries, 184
 - Linux installation, 184–185
 - network optimization, 190

Ethereal, (*continued*)

- packet contents, 187
- packet stream data, 185–187
- RPM packages, 184
- saving output, 190
- starting capture session, 187–189
- tools, 189–190
- usage, 185–187
- Windows installation, 185

Ethereal Web site, 185

Ethernet, 164–166

Ethernet card, 165

Ethernet networks, 165–166

Ethernet sniffers, 164

Evidence file, 366

Exchange security problems, 125

Expect, 13

Extendibility, 15

F

Factoring large prime numbers, 282

Farmer, Dan, 368

Fault-tolerant network, 57

FBI Web site, 350

FBI's NIPC (National Infrastructure Protection Center), 5

Federal law enforcement, 352

Files

- access time listing, 376
- checking integrity, 231
- database of baseline attributes, 226–227
- decrypting, 299
- encrypted, 3
- GnuPG (GNU Privacy Guard), 298–299
- listing attributes, 377–378
- PGP encryption, 291–292
- securing important, 3
- signing with public key, 292–293
- wiping from hard disk, 293

Filters and firewalls, 60

FIN packet, 59

FIN Scan, 104

FIN/ACK packet, 59

finger, 39–41, 129

exploiting bug in, 124

Sam Spade for Windows, 48

security holes, 39

sending without username, 40

Firewall server, configuring securely, 2

Firewalls, 1, 12, 53–54

“allow all” statement, 62

attacks coming through, 194

attacks from within, 125

blocking offending IP addresses, 3

business processes, 60–61

“deny all” statement, 62

disallowing SYN packets, 59

DMZ interface, 60

double-checking rules, 194

echo replies (ping responses), 60

eliminating existing rules, 67

filters, 60

higher end, 54

ICMP-type packets, 60

implementing and testing, 61

interfaces, 59

Linux built-in, 59

low-end consumer-grade, 54

lptables, 62–70

lptables creation, 66–70

NAT, 309

Nessus server outside of, 159

reviewing and testing, 61

rules, 61–62

running Web server on, 71

shell scripts, 66–67

SmoothWall Express, 75–86

tprivate interface, 59

traffic on port 80, 89

trusted interface, 59

Turtle Firewall, 71–75

vendors, 54

vulnerable to attack, 2

vulnerable to normal OS-level exploits, 125

WAN interface, 59–60

weaknesses in, 124–125

Web server, 125

Windows XP, 86

Windows-based, 86

Firewall-wizards mailing list, 70

Flex scripting language, 168

Flush command, 67

Forensic analysis, 356–357

Forensic analysis tools

dd, 366–368

The Forensic Toolkit, 375–379

Fport, 357–360

Isof, 360–363

The Sleuth Kit/Autopsy Forensic Browser,
368–374

Forensic data, 354–355

Forensic evidence, copies of, 365

The Forensic Toolkit, 375–379

Forensic tools, 349–352

FORWARD chain, 67
 Fport, 357–360
 Franklin, Ben, 161
 Free Software Foundation, xi, 13, 21
 Free Software Foundation Web site, 384
 FreeBSD, 23
 FreeS/WAN, 306
 installing, 307–308
 IPsec, 308
 Linux, 307
 OE (Opportunistic Encryption) mode, 308
 opportunistic encryption, 307, 311–312
 parameters, 309
 peer-to-peer mode, 308–310
 road warrior mode, 308, 310–311
 starting, 307–308
 usage, 308–312
 FreeS/WAN Web site, 306
 Freshmeat Web site, 265, 383–384
 Frigido, Andrea, 71
 FTP and sudden surge in traffic, 194
 FTP servers, write access to anonymous users, 142

G

GCC (Gnu C Compiler), 21
 Gcc (Gnu C Compiler), 13, 98
 GD, 248
 GD Web site, 248
 Gencases file, 345
 get_port_state() NASL function, 157
 Gilmore, John, 306
 GNOME, 27
 GNU GPL (General Public License), 21–23
 GnuPG (GNU Privacy Guard), 295
 basic information of key, 300
 chain of trust, 299
 decrypting files, 299
 encrypting files, 298
 files, 298
 GPL license, 296
 installing, 296–297
 key edit mode, 300
 managing key trusts, 300–301
 OpenPGP standard, 296
 pass-phrases, 297
 printing fingerprint of key, 300
 public-private key pair creation, 297
 publishing public keys, 298
 revocation certificate, 297–298
 signing files, 299
 signing keys, 300

 simple symmetric cryptography, 298
 web of trust model, 299
 GnuPGreenware, 288
 Google, 129
 GPL (General Public License), 13, 15, 22–23, 277
 GPL Web site, 23
 GPS Clock Web site, 355
 GPSDrive, 343
 GPSDrive Web site, 343
 GPSMAP, 343
 grep, piping ps command into, 42
 GTK (Gimp Tool Kit), 135
 GTK Web site, 135

H

Hack 'a' Tack, 95
 Hackers, 7
 altering certain system files, 26
 automated and random attacks, 9
 bandwidth, 8
 blank or weak passwords, 128
 brute force hacking, 130
 buffer overflow, 89–90, 124, 130
 civil action, 352
 databases, 126
 DNS cache poisoning, 126
 DNS servers, 126
 DoS (Denial of Service) attacks, 10, 131
 finding passwords, 302
 finding tools on Internet, 130
 Hacker Ethics code, 8
 idle or unused accounts, 127
 information about users, 40
 information leaks, 129–130
 log-on habits and schedule, 40
 mail servers, 125
 manufacturer default accounts, 127–128
 mass Web site defacement binges, 10
 multiple entries into system, 123–124
 NetBIOS null sessions, 130
 point-and-click hacking tools or scripts, 8
 port scan, 130
 published and known security holes, 122–123
 replacing binary files with Trojanized versions, 226–227
 router or firewall weaknesses, 124–125
 Script Kiddies, 8–9
 sites with dedicated broadband access, 7
 snmpwalk, 128
 social engineering attack, 130
 storage lockers, 8

- Hackers (*continued*)
- storing tools and other ill-gotten loot, 8
 - tracking down source or location of, 32
 - Trojan horses, 94
 - uncommon ports, 90
 - unneded services, 128–129
 - unsecured computers, 11
 - user and file management, 126–127
 - vulnerability scanner, 130
 - Web servers, 125
 - whois information, 130
 - zombies, 8
- Hard disks
- hidden data streams, 377
 - wiping files from, 293
- Hardening
- Linux, 28–30
 - security tool system, 27–44
 - Windows, 45–51
- Hardware
- NIDS requirements, 204
 - Snort, 203
 - Snort for Windows, 220–221
 - standard default logins and user accounts, 127
 - wireless LANs, 323–324
- Hash file, 373
- Hashes, 284, 356–357
- Healthcare, 11
- Hellman, Martin, 281
- Hermes chipsets, 323, 335
- Hewlett-Packard, 11
- Hfind utility, 376–377
- Hidden files and Windows, 376–377
- HIPAA (Health Insurance Portability and Accountability Act of 1996), 11
- Host unreachable ICMP message, 31
- Host-based intrusion detection, 225–231
- Hosts, 143–145, 148
- HP Open View, 199
- /htdocs/www.acid directory, 250
- /html directory, 114
- HTTP login forms, 141
- httpd process, 235
- Hunt utility, 378–379
- Hybrid cryptosystem, 289
- Hydra, 133, 141
- I**
- IANA (Internet Assigned Numbers Authority), 87–88
- IANA Web site, 88
- IBM, 20
- ICMP (Internet Control Message Protocol), 31
- ICMP-type packets and firewalls, 60
- .ida buffer overflow, 196–198
- Identity theft, 10
- Idle Scan, 105
- IDS (intrusion detection system), 193
- ACID (Analysis Console for Intrusion Detection), 201
 - analysis tools, 201
 - anomalous, 194–195
 - categories of alerts, 200
 - defining attacks, 193
 - empting hosts from examination, 200
 - false positives, 201
 - Kismet, 343–344
 - proper system configuration, 200–201
 - Snort, 201–216
 - Snort for Windows, 217–221
 - Snort Webmin Interface, 216–217
 - tuning, 201
- IEEE (International Electrical and Electronic Engineers), 165
- IIS (Internet Information Server) and cmd.exe attack, 196
- IIS Web server, 196–198
- Illicit services, 95–96
- Implementing secure wireless solution, 3
- Incident response plan, 353–354
- Incoming connections, blocking, 1
- Information leaks, 129–130
- Information security (info-security)
- availability, 5
 - business risks, 9–12
 - C.I.A., 4
 - confidentiality, 4–5
 - ignoring, 6
 - integrity, 5
- Infrastructure mode, 317
- Inline Snort, 202
- INN, xi
- Installer.sh file, 112
- Instant messengers, 12
- Integrity, 5
- Interdependence, 16
- Internal files, securing, 3
- Internal investigations, 352
- Internet, 123
- anonymous access, 320
 - broadband connections, 7–8
 - computer crimes, 7

- hackers, 7
- open source software, 13–14
- plain text, 279
- private address ranges, 70
- InternetMovies.com, 11
- Internic, 36
- Intrusion detection, host-based, 225
- Intrusion detection systems, 12
- Investigating break-ins, 3–4
- IP addresses, 56, 58
 - formats, 100–101
 - port scan, 130
 - space problem, 170
 - structure, 100, 102
 - traceroute (UNIX), 32–35
- IP masquerading and iptables, 70
- IP networks, 100, 102
- IP protocols
 - encrypting and verifying packets, 285
 - identifying version, 170–171
 - Snort, 222
- IPBlock, 48
- IPC (Inter-Process Communication) share, 127
- Ipchains, 59, 63–64
- Ipfwadm, 59, 63
- IPS (Intrusion Prevention Systems), 195–196
- IPsec, 306–307
 - AH (Authentication Header), 285–286
 - ESP packets, 309
 - FreeS/WAN, 308
 - transport mode, 286
 - tunnel mode, 286
 - VPN tunnel and encryption, 84–85
- ipsec.conf file, 308, 311
- IPv4 (IP version 4), 170, 285
- IPv4 packets, 171
- IPv6 (IP version 6), 170–171, 285
- IPX/SPX, 57
- ISAPI (Internet Server API), 196
- ISC Web site, 355
- ISO (International Standards Organizations), 54
- .iso image file, 78
- ISP complaints, 352

J

- Java Nessus Report Manager, 259
- John the Ripper, 312–314
- Joining open source movement, 384–387
- JpGraph, 247–248
- JpGraph Web site, 247

K

- Kazaa, 12
- KDE, 27
- Key rings, 290–291
- Keyserver Web site, 298
- Kismet, 328
 - capture session statistics, 341
 - configuration switches, 337–338
 - GPS support, 343
 - GPSMAP, 343
 - Hermes chipsets, 335
 - IDS, 343–344
 - installing, 337–338
 - interface settings, 340
 - key commands, 341–342
 - logging and interface options, 339
 - Network List section, 340–341
 - Prism II chipsets, 335
 - scrolling view of events, 341
 - wireless usage, 340–342
- Kismet Wireless, 184, 334–344
- kismet.conf file, 338, 344
- kismet_ui.conf file, 338
- Knowledge Base, 148

L

- L2TP (Layer Two Tunneling Protocol), 286
- LANalyser, 184
- Latency, 31
- LEAP, 345, 347
- Least privilege, 126–127
- Lex, 168
- Liability, 10–11
- libnasl file, 136
- Libpcap libraries, 135, 168, 184, 203
- Libpcap Web site, 135
- Linksys wireless cards, 335
- Linux, xi, 14, 22
 - AeroSniff, 335
 - AirSnort, 335, 344–346
 - built-in firewalls, 59
 - case sensitivity, 29
 - dd, 366–368
 - DMZ interface, 60
 - Ethereal installation, 184–185
 - FreeS/WAN, 307
 - Gcc (Gnu C Compiler), 98
 - GPSDrive, 343
 - hardening, 27–44
 - Ipchains, 59

- Linux (*continued*)
 - Ipfwadm, 59
 - Kismet Wireless, 334–344
 - iptables, 59, 63
 - Isof, 360–363
 - NCC (Nessus Command Center), 267
 - Nessus installation, 135–136
 - Nmap installation, 97–99
 - Prism2Dump, 335
 - RPM for Perl modules, 237
 - RPM (RedHat Package Manager) format, xvi
 - scanning commands, 364
 - tools, xvi
 - tprivate interface, 59
 - trusted interface, 59
 - /var/log directory, 234
 - VPNs (Virtual Private Networks), 306
 - WAN interface, 59–60
 - Webmin service, 71
 - WEPCrack, 335
 - wireless drivers, 335
 - wlan-ng drivers, 336
 - Linux messages file, 234–235
 - Linux-WLAN Web site, 336
 - Local law enforcement, 351
 - Log files, 234
 - failed login attempts, 235
 - monitoring, 3, 236–241
 - reviewing, 363–365
 - security information, 235
 - UNIX, 363–364
 - Windows, 363
 - Log2db.pl script, 114
 - Logic errors, 160
 - Logins
 - configurations, 141
 - failed attempts, 235
 - Loss of customers, 10
 - Loss of productivity, 12
 - iptables, 59, 62
 - accepting fragmented packets, 67
 - command line, 63
 - commands, 64–65
 - current rule set, 63
 - “deny all” statement, 67
 - domain as only allowable port, 69
 - dropped packets, 69
 - eliminating existing rules, 67
 - firewall creation, 66–70
 - flushing other chains, 67
 - HTTP and Web traffic, 68
 - ICMP packets, 69
 - incoming connections only on certain ports, 68
 - incoming traffic based on inside connections, 68
 - installing, 63–64
 - IP masquerading, 70
 - NAT (Network Address Translation), 70
 - port scans, 93
 - preventing users from protocol use, 68–69
 - scripts, 63
 - setting up logging, 69
 - smurf attack, 68
 - specifications, 65–66
 - spoofing, 67–68
 - tables, 64–66
 - UDP packets, 69
 - usage, 64–66
 - Isof (LiSt Open Files), 360–363
- ## M
- m multiport, 68
 - MAC (Media Access Control) addresses, 55–56, 166
 - BSSID (Basic Station System ID), 318
 - hosts, 145
 - MAC Addresses Web site, 56
 - Mail servers
 - hackers, 125
 - security holes, 2
 - Mail system testing, 142
 - Mailing lists, 19, 386
 - open source software, 382
 - support, 17
 - Major Domo, xi, 386
 - Make install command, 98
 - Makefile, 98
 - Malicious software, 9
 - Malware, 9
 - Managing key trusts, 300–301
 - Mandrake Linux
 - EMACS, 113
 - tools, xvi
 - Manufacturer default accounts, 127–128
 - MapPoint, 324, 331–333
 - MASQUERADE flag, 70
 - MD5 hashing algorithm, 284, 356–357
 - Merkle, Ralph, 281
 - Metcalfe, Bob, 165
 - Microsoft RPC (Remote Procedure Call)
 - vulnerabilities, 6
 - MINIX, 13–14
 - Monitoring log files, 236–241
 - Morris, Robert, 124

Morris worm, 124
MySQL, 207

- commands, 243–244
- configuring Snort for, 248–249
- /etc/ld.so.conf file, 242
- install script, 242
- locking down, 243
- NCC (Nessus Command Center), 267
- NPI (Nessus PHP Interface), 259
- ownership and file permissions, 242
- /scripts directory, 242
- security, 243
- starting as daemon, 243
- user and group, 242
- user name and password, 243

MySQL databases, 220

- admin user, 243
- NPI (Nessus PHP Interface), 260

MySQL server, 242–243, 261
MySQL Web site, 242

N

Napster, 12
NASA Web site, 355
NASL (Nessus Attack Scripting Language), 15, 133, 156–158
NAT (Network Address Translation), 70, 309
National Security Agency Web site, 45
.nbe format, 260
NCC (Nessus Command Center), 2–3, 145, 265

- adding targets, 274–276
- adding users, 273
- admin user and password combination, 271
- Apache, 267
- automating scans, 266
- database interface for Nessus results, 266–267
- database schema with tables, 269
- GPL, 277
- group administrators option, 273
- group management feature, 273
- installing, 270–272
- Linux, 267
- logical layout, 269
- login page, 272
- main screen, 272
- management platform for Nessus scanning, 266
- managing users, target files, and schedules, 273
- modular and expandable, 272–273
- MySQL, 267, 270
- Nessus interface, 266
- Nessus server and client, 270

Perl, 267, 270
PHP-compliant Web server, 270
platforms, 267
project elements, 268
Schedule Management screen, 276
scheduling database, 266
scheduling scan, 276–277
Sourceforge page, 269
symbolic link, 271
system administrator option, 273
Target Management screen, 274
usage, 272–273
User Management screen, 273
user name and password, 273
Web interface for setting Nessus options, 267
Web site, 269
Nero, 78
NesQuick, 259
Nessus, 2, 131

- auto-install script, 135–136
- auto-installer script remotely running, 135
- automatic scheduled scan of network, 145
- avoiding pattern-matching NIDS, 143
- brute force login, 141
- certificate for SSL communications, 137
- CGI programs, 133
- CGI scripts default location, 144
- client-server architecture, 132–133
- database creation, 262
- documentation, 135
- exporting scans into NIP, 263
- extensive install process, 135
- flexibility, 138
- Ftp writable directories, 142
- hosts by MAC address, 145
- HTML, 134
- Hydra, 133
- integration with other tools, 133
- KB (Knowledge Base) tab, 147–149
- Knowledge Base, 134, 147–149
- LaTeX, 134
- Linux installation, 135–136
- listing previously run sessions, 147
- login, 141
- login page, 138
- mailing lists, 134–135
- medium- to large-size networks, 259
- multiple report formats, 134
- NASL (Nessus Attack Scripting Language), 15, 133
- new hosts, 148

Nessus (*continued*)

- NIDS (Network Intrusion Detection System), 142–143, 199
- Nikto, 133
- Nmap, 133, 140
- NNTP (Network News) server, 142
- number of simultaneous tests, 143–144
- open source project, 133
- ping remote host, 140–141
- plain text, 134
- Plugins tab, 139
- port range, 143
- port scanner, 133, 145
- Preferences tab, 139
- prerequisites, 135
- reading targets from file, 146
- record of targets and settings, 146
- retesting hosts, 148
- reusing Knowledge Base, 148
- reverse DNS lookup, 144
- robust support network, 134–135
- sample scanning configurations, 155–156
- saving sessions without data, 147
- Scan Options tab, 143–145
- scanning without being connected to client, 145
- security scan data and database reports, 3
- server-side options, 139–143
- setting up, 137
- smart testing, 133–134
- SMTP settings, 142
- status of scan, 148–149
- Target Selection tab, 145–147
- testing, 142
- testing every host, 148
- testing on every host, 144
- testing SSL services, 141
- two different parts generating data, 260
- UID (User ID numbers) range, 141
- unsafe checks, 144–145
- unscanned ports as closed, 143
- user accounts, 137
- User tab, 147
- user-created scripts, 156–158
- vulnerability tests depth, 132
- Web mirroring, 142
- Whisker, 133, 142
- Windows domain test, 142
- XML, 134
- zone file for domain, 146

Nessus mailing list, 134

Nessus server

- logging into, 138
- outside firewall, 159
- users, 147

Nessus Web site, 158

nessus-announce mailing list, 134

Nessus-core file, 136

nessus-cvs mailing list, 134

nessusd daemon, 42

nessus-devel mailing list, 134

Nessus-libraries file, 136

nessus-php directory, 262

Nessus-php index file, 263

nessusphp.inc file, 262

Nessus-plugin-ins file, 136

Nessus.rc text file, 150

NessusWX, 149

- client-side settings, 150–151
- Comments tab, 152
- installing, 150
- interface, 150
- MySQL support, 150
- Options tab, 152
- PDF files, 150
- Plugins tab, 152
- Port scan tab, 152
- report manipulation, 150
- reporting formats, 150
- reports, 154
- scan configurations (sessions), 151
- Scan Status screen, 153–154
- server-controlled settings, 150
- session profile, 151–154
- Session Properties window, 152
- user interface, 150

Net Security SVCS Web site, 269

NetBEUI, 57

NetBIOS, 57, 130

NetBSD, 23

NetBus, 95

netfilter.org Web site, 63

NetIQ, 234

Netmasks, 100, 102

NetPatrol, 234

Netscape, 283

NetScreen, 54

NetStumbler, 20, 184, 323

- converting output to MapPoint, 331–333
- data fields, 326–327
- installing, 325
- listing access points, 325

- networks detected, 326, 328
 - options, 329
 - polling for access points, 328
 - saving sessions, 331
 - signal graph, 328
 - usage, 325–328
 - wireless network card status, 328
- NetStumbler Web site, 322
- Network architecture
- application layer, 57
 - data link layer, 55–56
 - network layer, 56
 - OSI Reference Model, 54–57
 - physical layer, 55
 - presentation layer, 57
 - session layer, 57
 - transport layer, 56–57
- Network card and promiscuous mode, 168
- Network interface hardware, 55–56
- Network layer, 56
- Network protocols, 57
- Network sniffers, 2, 61, 163–164
- baseline for network, 167
 - Ethereal, 183–191
 - getting permission for, 166
 - network topology, 166–167
 - ports, 166–167
 - routers, 166
 - Tcpdump, 167–181
 - tight search criteria, 167
 - WinDump, 181–182
- Network Solutions, 36
- Network Solutions Web site, 37
- Network unreachable ICMP message, 31
- Network use policy, 60
- Network Worms, 94
- Networks
- accounts with blank passwords, 128
 - baseline, 2, 167
 - checking external exposure, 119
 - communication with secondary identification, 56
 - dropping packets, 31
 - fault-tolerant, 57
 - information about, 31
 - inventory of, 93–94
 - mapping needed services, 61
 - monitoring system activity, 199
 - NIDS placement, 210–211
 - plain text inter-system communications, 43
 - scanning from inside and out, 2
 - scanning with permission, 158
 - topology, 166–167
 - tracking troublemakers, 36–37
 - watching for suspicious activity, 2
- Network/server optimization, 94
- Newsgroups, 381–382
- NeWT, 150
- NICs (network interface cards), 318, 335–337
- NIDS (Network Intrusion Detection System), 2, 142–143, 163, 194
- attacks and suspicious activity from internal sources, 194
 - cmd.exe attack, 196
 - database authentication activity, 200
 - false positives, 198–200
 - hardware requirements, 204
 - .ida buffer overflow, 196–198
 - long authentication strings, 199–200
 - Nessus, 199
 - network monitoring system activity, 199
 - network vulnerability scanning/port scanners, 199
 - Nmap, 199
 - placement of, 210–211
 - signatures, 196–198
 - sorting and interpreting data, 2
 - Trojan horse or worm-like behavior, 199
 - tuning and managing with ACID, 253–254
 - user activity, 199
- Nikto, 133
- Nimda worm, 9–10, 123, 196, 199
- NIST (National Institute of Standards and Technology), 284
- Nlog, 94
- add-ons, 115–116
 - CGI directory, 114
 - checking external network exposure, 119
 - hunting for illicit/unknown Web servers, 118
 - installing, 112, 114
 - organizing and analyzing output, 112–117
 - scanning for least common services, 117–118
 - scanning for servers running on desktops, 118–119
 - Trojan horses, 119
 - usage, 114–115
 - user-created extensions, 116–117
 - viewing database file, 114–115
- Nlog directory, 112
- Nlog Web site, 112
- Nlog-bind.pl file, 117
- Nlog-bind.pl script, 116
- Nlog-config.ph file, 117

Nlog-dns.pl file, 116
Nlog-finger.pl file, 116
Nlog.html file, 114
Nlog-rpc.pl file, 116
Nlog-search.pl file, 117
Nlog-smb.pl file, 116
Nmap, 2, 96, 135
 Bounce Scan, 105
 carefully selecting scan location, 110
 checking external network exposure, 119
 code, 97
 color coding ports, 111
 command line interface, 97, 103
 compiling from source, 98
 downloading files, 97
 ease of use, 97
 FIN Scan, 104
 Idle Scan, 105
 illicit/unknown Web servers, 118
 IP addresses formats, 100–101
 least common services, 117–118
 Linux installation, 97–99
 log file, 114
 miscellaneous options, 107–109
 Nessus, 133, 140
 network discovery options, 106
 NIDS (Network Intrusion Detection System),
 199
 NULL Scan, 104
 options, 96–97
 output, 110–112
 PingSweep scan, 104
 regularly running scans, 110
 RPC Scan, 105
 running as service, 107, 110
 saved logs formats, 112
 scan types, 103
 scanning networks, 100
 starting graphical client, 99
 SYN scan, 103
 TCP Connect scan, 103
 timing, 106–107, 110
 Trojan horses, 119
 UDP Scan, 104
 Windows installation, 99–100
 Windows Scan, 105
 XMAS Scan, 104
 X-Windows, 97
NMapWin, 99–100
NMS (Network Monitoring System), 199
NNTP (Network News) server, 142

Norton, 293
Norton Ghost, 365, 372
NPI (Nessus PHP Interface), 259
 analyzing Nessus data, 263–264
 dataflow, 269
 directory for files, 262
 flow of data, 260
 importing Nessus scans, 263
 installing, 261–263
 logical parts, 260
 manipulating scan data, 264
 MySQL, 259–261
 .nbe format, 260, 263
 .nsr format, 263
 PHP, 259
 PHP-enabled Web server, 260
 queries, 263–264
 usage, 263–264
Nslookup, 47
nsr script, 262–263
nsr-php script, 261–262
NTP (Network Time Protocol), 355
NULL Scan, 104

O

OE (Opportunistic Encryption) mode, 308
Official name registrars, 36
One-way functions, 282
Open ports and security, 2
Open Source Initiative Web site, 384
Open source movement
 bug finder/beta tester, 385
 discussion groups and supporting other users,
 385–386
 joining, 384–387
 providing resources to project, 386–387
Open source operating systems, 27
Open source projects, 264
 broader need for, 265
 NCC (Nessus Command Center), 266–277
 patronizing companies supporting open source
 products, 387
 permission to release code as open source, 265
 providing resources to, 386–387
Open source security tools, xix–xxi
Open source software, xi, 12
 100 percent outsourced IT, 20
 advantages, 15–19
 BSD license, 13, 21, 23
 chat rooms, 19
 cost, 15

- documentation, 18
 - education, 18–19
 - extendibility, 15
 - GPL (General Public License), 13, 15, 21–23
 - hashes, 284
 - history, 13–14
 - interdependence, 16
 - Internet, 13–14
 - licenses, 21–23
 - Linux, 14
 - mailing lists, 19, 382
 - not fitting needs, 19–20
 - patches, 16
 - product life span, 18
 - reputation, 19
 - resources, 381–384
 - restrictive corporate IT standards, 20
 - scripting languages, 15
 - security, 4, 15–16
 - security software company, 19–20
 - support, 16–18
 - UNIX, 13
 - viewing code, 18
 - Web sites, 382–384
 - Windows, 20–21
 - OpenBSD, 23
 - OpenSSH, 301–305
 - OpenSSH Client, 43–44
 - OpenSSH server, 302–304
 - OpenSSL, 135
 - OpenView, 234
 - Operating system tools
 - Bastille Linux, 28
 - dig, 37–39
 - finger, 39–41
 - OpenSSH Client, 43–44
 - ping (Packet Internet Groper), 30–32
 - ps, 41–42
 - traceroute (UNIX), 32–37
 - tracert (Windows), 32–37
 - whois, 35–37
 - Opportunistic encryption, 307, 311–312
 - Oracle, 207
 - ORiNOCO wireless cards, 335–336
 - OS (operating system), 25
 - attacks on, 26
 - hardening, 27–44
 - identifying, 31
 - securing, 27
 - security features, 26
 - OSI Reference Model, 54–57, 121–122
- P**
- Packets, 58
 - delivery address for, 170
 - latency, 31
 - logging, 205
 - moving between points, 56–57
 - number of hops before dying, 32
 - suspicious, 205–206
 - virtual path, 32
 - Pass-phrases, 289, 297
 - Password crackers, 312–314
 - Password files, testing, 312–314
 - Password hash file, 314
 - Passwords, 7, 127–128, 141
 - Patches, 16, 124
 - pcap library, 168
 - PCMCIA drivers, 335
 - Peer-to-peer file transfer software, 95–96
 - Peer-to-peer mode, 308–310
 - Perl
 - NCC (Nessus Command Center), 267
 - Swatch, 237
 - Perl Curses and TK modules, 28
 - PGP (Pretty Good Privacy), 3
 - adding keys to public key ring, 291
 - chain of trust, 299
 - Decrypt/Verify function, 293
 - deleting, 290
 - Encrypt and Sign function, 293
 - Encrypt function, 291–292
 - encrypting files, 291–292
 - features, 288
 - Freespace Wipe, 293
 - generating public/private key pair, 289
 - hybrid cryptosystem, 289
 - improper use of, 289
 - installing, 289
 - key pairs creating and revoking, 291
 - key rings, 290–291
 - options, 293–295
 - pass-phrase, 289–290, 292
 - PGP Options dialog box, 293–295
 - PGPKeys section, 290–291
 - PGPMail, 290
 - pouring file, 290
 - private key, 290
 - reversing PGP encryption process, 293
 - securing file, 290
 - shared secret encryption, 292
 - Sign function, 292–293
 - web of trust model, 299

PGP (*continued*)

- Wipe function, 293
 - wiping original file, 292
- PGP Freeware, 288, 290
- PGP Web site, 298
- PGPMail, 290
- PHP
- Apache Web server, 261
 - buffer overflows, 126
 - color graphs, 247–248
 - httpd.conf configuration file, 246
 - manipulation libraries, 248
 - NPI (Nessus PHP Interface), 259
 - setting up, 245–246
 - Web-based applications, 245
- PHP Web site, 246
- PHP-enabled Web server, 260
- PHPLOT, 247
- Physical layer, 55, 164
- Physical media, 55
- Physical threat, 7
- Pico, 113
- ping (Packet Internet Groper), 30–32
- Sam Spade for Windows, 47
 - Windows, 45
- PingSweep scan, 104
- PKE (public key encryption), 281–283, 289
- Plain text, 279
- Plugging holes, 2
- Plug-ins, 139
- plug-ins-writers mailing list, 134
- Port 80, 89
- Port forwarding, 304–305
- Port numbers, 88–89
- TCP headers, 172
 - Trojan horses, 94
- Port scan, 130
- Port scanners, 61
- differences between, 90
 - identifying operating system, 91–92
 - network inventory, 93–94
 - network/server optimization, 94
 - Nlog, 112–117
 - Nmap, 96–112
 - overview, 90–92
 - spyware, Trojan horses, and network worms, 94
 - TCP fingerprinting, 91–92
 - unauthorized or illicit services, 95–96
 - when to use, 93
- Port scans, 93

Ports

- network sniffing, 166–167
 - scanning. *See* port scanners
 - unscanned as closed, 143
 - verifying suspicious open, 110–111
- PostgreSQL, 207
- Presentation layer, 57
- Primitives, 175
- Prism II chipsets, 323, 335
- Prism2Dump, 335
- Private keys, managing, 290–291
- Private line connections, 7
- Processes, listing, 41–42, 45
- Product life span, 18
- Promiscuous mode, 168
- Property masks, 228
- Protocols and encryption, 280
- ps command, 41–42
- Public Key cryptography, 281, 302
- Public key servers, 298
- Public keys
- managing, 290–291
 - publishing, 298
 - signing files with, 292–293
 - validating, 291
- Public servers, 2
- Public-private key pair, 297
- Publishing public keys, 298
- PuTTY, 49–51
- Pwlib, 28
- Python, 13

Q

- qotd (quote of the day) service, 129

R

- RangeLan wireless cards, 335
- RC4, RC5, and RC6, 284
- RedHat Linux, 14, 26, 28
- Remote host, pinging, 140–141
- Remote systems
- information on users, 40
 - securely logging into, 43–44
- Remote terminal access, 302
- Reputation, 19
- Resources for open source software, 381–384
- Restrictive corporate IT standards, 20
- Reverse DNS lookup, 144, 255–256
- Revocation certificate, 297–298
- revoke.asc file, 298
- RFC Editor Web site, 170

- Rijndael, 284
 - Rivest, Ronald, 282, 284
 - Road Warrior mode, 308, 310–311
 - Roesch, Martin, 202
 - Roots Web mailing list, 382
 - Routers
 - finger, 39
 - network sniffing, 166
 - Telnet, 125
 - weaknesses in, 124–125
 - RPC Scan, 105
 - RPM (RedHat Package Manager) format, xvi
 - RPMFind Web site, 237, 335
 - RSA, 282–283
- S**
- sa account, 128
 - Sam Spade for Windows, 47–48
 - ACID (Analysis Console for Intrusion Databases), 256
 - installing, 46
 - PuTTY, 49–51
 - testing IP address or hostname, 46
 - Samba and potential security holes, 30
 - Samspade.org Web site, 46
 - Schneier, Bruce, 284
 - SCP, 302
 - Script Kiddies, 8–9
 - Scripting languages, 15
 - Search engines, 129–130
 - Secure wireless solution, implementing, 3
 - Securely logging into remote systems, 43–44
 - Securing
 - files, 290
 - important files and communications, 3
 - perimeter, 1–2
 - Security, xi–xii
 - early warning system, 2
 - hardware and software, 12
 - height cost of, 12
 - implementing secure wireless solution, 3
 - important files and communications, 3
 - investigating break-ins, 3–4
 - management system for security data, 2–3
 - MySQL, 243
 - open source software, 4, 15–16
 - plugging holes, 2
 - securing perimeter, 1–2
 - unauthorized or illicit services, 95–96
 - Security holes
 - BIND (Berkley Internet Naming Domain), 126
 - buffer overflow, 89–90
 - identifying, 122–131
 - logic errors, 160
 - major Internet outages, 123
 - not enough time or staff, 123
 - patches, 16, 123
 - potential, 161
 - published and known, 122–123
 - unaware of problem, 123
 - Web servers, 125
 - Windows, 16
 - Security policies for employees, 160–161
 - Security software company, 19–20
 - Security tool system, hardening, 27–44
 - Sed, 13
 - Sendmail, xi, 22, 125
 - Servers
 - investigating break-ins, 3
 - message logs, 234
 - port scanning, 94
 - rebooting at strange times, 235
 - running on desktop, 118–119
 - time syncing, 354–355
 - Services
 - account and password for, 141
 - attacked most, 256
 - brute force login, 141
 - illicit, 95–96
 - listing running, 94
 - mapping out needed, 61
 - running Nmap as, 107, 109
 - running Snort as, 215–216
 - searching for, 42
 - turning off, 45
 - unauthorized, 95–96
 - unknown running, 42
 - unnneeded, 128–129
 - Session layer, 57
 - Session profile, 151–154
 - Sessions, logging, 50
 - Sfind utility, 377
 - SFTP, 302
 - SGI Web site, 355
 - Shamir, Adi, 282
 - Shared secret encryption, 281
 - Shell scripts, 66–67
 - Shells, 67
 - Shmoo Web site, 322, 336
 - SID (Security ID), 142
 - Signatures, 193, 196
 - signed.doc file, 299
 - Signing files and GnuPG (GNU Privacy Guard), 299–300

- Simovits Web site, 359–360
- Simple symmetric cryptography, 298
- Slash notation, 100, 102
- Slashdot Web site, 383
- The Sleuth Kit/Autopsy Forensic Browser, 356
 - adding hosts, 371–372
 - adding images, 372–373
 - analysis types, 374
 - analyzing data, 374
 - Autopsy Forensic Browser, 369
 - Case Gallery, 371
 - creating and logging into case, 370–371
 - evidence locker, 369
 - features, 369
 - hash file, 373
 - installing, 369
 - usage, 369–370
- SmoothWall Corporate Server, 75, 78
- SmoothWall Express, 75
 - additional applications, 85–86
 - additional connection types support, 77
 - admin default user name, 80
 - auto-detecting NICs (network interface cards), 79
 - bootable CD-ROM disk, 78
 - dedicated machine, 77
 - DHCP client and server, 76–77, 79
 - graphs and reports, 77
 - hardware requirements, 77
 - hostname, 79
 - installing, 78–80
 - intrusion detection, 77
 - opening screen, 80
 - passwords, 80
 - patches, 83
 - setting up network types, 79
 - setup mode, 79
 - shutting down, 83
 - versus* SmoothWall Corporate, 78
 - SSH and Web access to firewall, 77
 - VPN support, 76
 - Web caching server, 77
 - Web interface user account, 80
 - Web proxy server, 77
 - zones, 79
- SmoothWall firewall, 80–81, 83–84
- SmoothWall Web site, 78
- SMTP, 142
- Smurf attack, 68
- SNA, 57
- Sniffer, 184
- Sniffer Pro, 184
- SNMP (Simple Network Management Protocol), 127–128
- snmpwalk, 128
- Snort, 2, 15, 201, 343
 - alert header, 222
 - alert modes, 206–207
 - alert options, 222–223
 - anomalous activity detection, 202
 - command line, 203
 - configuring for maximum performance, 207–209
 - customizing rule sets, 209
 - database output, 207, 209
 - decoders and preprocessors, 208
 - default snort.conf configuration file, 205
 - disabling rules, 211–215
 - features, 203
 - hardware, 203
 - home network, 207
 - IDS mode, 203
 - installing, 203
 - internal servers setup, 208
 - intrusion detection mode, 205–206
 - IP protocols, 222
 - logging packets, 205
 - logging suspicious packets, 205–206
 - MySQL, 248–249
 - open source and portable, 203
 - output modules configuration, 208–209
 - packet logging mode, 203–205
 - packet sniffer mode, 203–204
 - resources, 202
 - rule classes file names, 211–215
 - running, 203
 - sample custom rules, 224–225
 - securing database, 254
 - as service, 215–216
 - signature-based, 202
 - SMB output option, 206
 - snort.conf configuration file, 207–209, 248
 - Space module, 202
 - Syslog output option, 207, 209
 - Unified output module, 209
 - using names carefully, 259
 - /var/log/snort directory, 205
 - writing custom rules, 221–225
- Snort for Windows, 217–221
- Snort Web site, 221
- Snort Webmin Interface, 216–217
- Social engineering attack, 130

Software and wireless LANs, 323–324
 SonicWALL, 54, 347
 Source code
 compiling from, 97–98
 modifications, 22
 Sourceforge Web site, 237, 265, 382–383
 Space module, 202
 Spoofing, 67–68
 Spyware, 94
 SQL databases, 247
 SQL servers, 128
 SQL Slammer worm, 123–124, 126, 128
 SSH (secure shell), 43–44, 302
 SSH client and Windows, 50–51
 SSH server, 302–304
 sshd process, 302
 sshd_config file, 303
 SSID (Station Set Identifier), 318–321
 SSL (Secure Socket Layer), 286, 302
 SSL services, testing, 141
 Stacheldraht, 95
 Stallman, Richard, 13
 State, 59
 Storage lockers, 8
 StumbVerter, 331–333
 Sub7, 95
 Support, 16–16
 Supporting other users, 385–386
 Swatch (Simple Watcher or Syslog Watcher), 3
 action statements, 240–241
 bad logins, 236
 command options, 238
 configuration file, 239–241
 configuring, 238–239
 as daemon or as cron job, 236
 Date::Calc Perl module, 237
 Date::Format Perl module, 237
 Date::HiRes Perl module, 237
 default config file, 238
 FTP, SSH, or Telnet usage, 237
 installing, 237–238
 log file options, 239
 Perl, 237
 running, 238–239
 scanning UNIX messages file, 239
 Snort or Nessus messages, 236
 swatchrc file, 239–241
 swatchrc.monitor, 239
 swatchrc.personal file, 239
 system crashes, 236
 system reboots, 236

 text editor usage, 237
 watchfor statement, 240
 Symmetric cryptography, 281, 302
 SYN packet, 59
 SYN scan, 103
 -syn statement, 68
 SYN/ACK packet, 59
 Syslog server, 207
 System files, modifications to, 2257
 System V, 13
 Systems, listing processes, 41–42

T

Tables, 64–66
 Tampering with records, 12
 tar -zxvf command, 112
 Targets, 274–276
 TCB (Trusted Computing Base), 25
 TCP (Transmission Control Protocol), 56–57
 establishing session, 172
 three-way handshake, 59
 TCP Connect scan, 103
 TCP fingerprinting, 91–92
 TCP Flags, 172–173
 -tcp flags, 68
 TCP headers, 172–173
 Tcpcdump, 167, 309
 allowable primitive combinations, 176–179
 comments, 170
 destination address, 170
 example, 169
 examples, 180–181
 expressions, 175–179
 installing, 168
 options, 173–175
 parts of IP stack, 173
 ported over to Windows platform, 181–182
 primitives, 175
 qualifiers, 176
 running, 169–170
 source IP address of packet, 170
 TCP sequence number, 173
 TCP/IP packet headers, 170–175
 timestamp, 170, 173
 Tcpcdump Web site, 168
 TCP/IP
 ARP (Address Resolution Protocol) request, 59
 becoming standard, 57–58
 communication phases between network nodes,
 58–59
 communications having state, 59

- TCP/IP (*continued*)
 - fault-tolerant network, 57
 - headers, 170–175
 - IP address, 58
 - packets, 58
 - TCP three-way handshake, 59
 - TCP/IP networks, 56
 - TCP/IP packet, layout of, 170
 - TCP/UDP port numbers, 87
 - Telnet, 302
 - routers, 125
 - scanning ports, 90–91
 - Terminal program, 43
 - Text editors, 112–114
 - Time, 48
 - Token Ring, 164
 - Tools
 - Mandrake Linux 9.1, xvi
 - RPM (RedHat Package Manager) format, xvi
 - searching Web for, 265
 - Windows 2000 Pro, xvi
 - Windows XP Pro, xvi
 - Torvalds, Linus, xi, 14
 - Tprivate interface, 59
 - Trace and Sam Spade for Windows, 48
 - traceroute (UNIX), 32–37
 - tracert (Windows), 32–37
 - Traffic signatures, 193
 - Transport layer, 56–57
 - Transport mode, 286
 - Trin00, 95
 - Trinity, 95
 - TripleDES, 283–284
 - Tripwire
 - baseline attributes database, 226–227
 - commercial and open source versions, 226
 - configuring, 227–230
 - cron job, 231
 - /etc/tripwire directory, 227
 - file integrity, 231
 - ignore flags, 229
 - initializing baseline database, 230
 - installing, 227
 - license agreement, 227
 - policy file, 227–231
 - property masks, 228
 - RPMs, 227
 - site and local pass phrases, 227
 - template property masks, 229
 - updating database, 231
 - Trojan horses, 9, 94–95
 - database of, 359
 - NIDS (Network Intrusion Detection System), 199
 - nlog, 119
 - nmap, 119
 - port numbers, 94
 - uncommon ports, 90
 - Trusted interface, 59
 - Trusted zone, 73
 - TTL (Time to Live) setting, 32
 - Tunnel mode, 286
 - Turbo Linux, 14
 - Turtle Firewall, 1, 63–64, 71–75
 - Turtle Firewall Web site, 72
 - twagent, 226
- U**
- UDP (User Datagram Protocol), 57
 - UDP Scan, 104
 - UIDs (User ID), 141
 - Unauthorized services, 95–96
 - Universities, 13
 - University of California at Berkeley, 13
 - UNIX, 14
 - C compiler built in, 97
 - case sensitivity, 29
 - dd, 365–368
 - Ethereal, 183–191
 - John the Ripper, 313
 - log files, 363–364
 - lsf, 360–363
 - Open Source software, 13
 - scanning commands, 364
 - The Sleuth Kit/Autopsy Forensic Browser, 368–374
 - Snort, 201–216
 - text editors, 113–114
 - tools, xvi
 - universities, 13
 - unixODBC, 207
 - Unsafe checks, 144–145
 - Untrusted zone, 73
 - USENET, 13
 - USENET newsgroups, 381–382
 - /user/local/etc directory, 338
 - Users
 - adding to NCC, 273
 - least privilege, 126–127
 - listing logged-on, 40–41

- Nessus server, 147
 - remote system information about, 40
 - SUID (Security ID), 142
- /usr/local/bin directory, 303
- /usr/local/etc/ssh directory, 303

V

- /var/log directory, 234
- Verification and hashes, 284
- VeriSign, 36, 285
- vi, 66, 113
- VIA Web site, 355
- Viruses, 9
- Vogt, Jens, 99
- VPN encryption, 347
- VPN tunnel, 84–85
- VPNs (Virtual Private Networks), 2, 305
 - Linux, 306
 - SmoothWall firewall, 83–85
- Vulnerability scanners, 12
 - attacks in progress or already happened, 161
 - current backups and, 158–159
 - custom applications, 160
 - excessive scanning, 159
 - hackers, 130
 - location of Nessus server, 159
 - logic errors, 160
 - minimal impact on other employees, 159
 - Nessus, 131–141
 - NessusWX, 149–154
 - scanning with permission, 158
 - security policies for employees, 160–161
 - testing applications for security holes, 122
 - undiscovered vulnerabilities, 160

W

- WAN interface, 59–60
- War dialing, 321
- War driving, 321–322
- Web
 - login strings, 199–200
 - searching for tools on, 265
- Web of trust, 291, 299
- Web servers
 - ACID (Analysis Console for Intrusion Databases), 247
 - allowing dangerous commands, 142
 - alternate ports, 118
 - buffer overflow, 130
 - bugs, 125
 - firewalls, 125
 - hackers, 125
 - hunting for unknown/illicit, 118
 - managing security data, 241–264
 - NetBIOS null sessions, 130
 - security holes, 2, 125
 - testing integrity, 142
- Web sites, 7–8
 - open source software, 382–384
 - whois information, 130
- Web-based applications, 245
- Webmin interface, 72
- Webmin RPM, 63–64
- Webmin Snort, 218–219
- Webmin Web site, 63
- Well-known port numbers, 88
- WEP (Wired Equivalent Privacy), 319–321, 344, 346
- WEPCrack, 335, 344
- WhatsUp Gold, 199
- Whisker, 133, 142
- Whois, 35–37, 48
- Wi-Fi, 316–319
- Windows, 26
 - broadcast traffic, 165
 - default guest account, 127
 - Ethereal, 183–191
 - exposing network configuration information, 129
 - The Forensic Toolkit, 375–379
 - Fport, 357–360
 - guides for, 45
 - hardening, 45–51
 - hidden files, 376–377
 - installing Ethereal, 185
 - installing Nmap, 99–100
 - IPC (Inter-Process Communication) share, 127
 - John the Ripper, 313
 - listing processes running, 45
 - log files, 363
 - NessusWX, 149–154
 - NetStumbler, 324–331
 - network-aware services, 45
 - Norton Ghost, 365
 - NULL session capabilities, 378–379
 - open source software, 20–21
 - ping, 45
 - poor security by default, 127
 - Sam Spade for Windows, 46–49
 - security holes, 16
 - Services window, 45
 - Snort for Windows, 217–221
 - SSH client, 50–51
 - StumbVerter, 331–333

- Windows (*continued*)
 - traceroute, 45
 - WinDump, 181–182
 - Windows 2000 Pro, xvi
 - Windows Scan, 105
 - Windows Small Business Server 2000, 26
 - Windows XP
 - firewalls, 86
 - insecurities, 26
 - Windows XP Pro, xvi
 - Windows-based firewalls, 86
 - WinDump, 181–182
 - WinDump-specific commands, 182
 - WinPcap, 100
 - WinPcap libraries, 168, 185, 220
 - Wireless cards, 323
 - Wireless LANs
 - 802-11-specific vulnerabilities, 320–321
 - access to wireless PCs, 320
 - accessing with wireless access point, 320
 - AirSnort, 344–346
 - anonymous Internet access, 320
 - antennas, 324
 - auditing perimeter, 347
 - beacon broadcasts, 321
 - dangers, 319–321
 - default SSIDs, 320–321
 - eavesdropping, 319–320
 - external antenna, 330
 - hardware, 323–324
 - improved encryption protocol, 347
 - informing others of access to, 330
 - Kismet Wireless, 334–344
 - moving access points, 347–348
 - NetStumbler, 324–331
 - optimal conditions for auditing, 330
 - overview, 316–319
 - permission to access, 329
 - properly configuring, 348
 - security perimeter, 316
 - software, 323–324
 - StumbVerter, 331–333
 - training staff about, 348
 - treating as untrusted, 347
 - unencrypted communications, 321
 - unsecured, 322
 - VPN encryption, 347
 - war dialing, 321
 - war driving, 321
 - WEP (Wired Equivalent Privacy), 319–321, 346
 - Wi-Fi, 316–317
 - wireless cards, 323
 - wireless perimeter, 329–330
 - Wireless network node, 318
 - Wireless networks
 - security assessment, 322
 - testing security, 3
 - Wireless PCs, access to, 320
 - wlan-ng drivers, 336
 - Worms, 6, 9
 - accounts with blank passwords, 128
 - NIDS (Network Intrusion Detection System), 199
 - wtmp, 3
 - /www subdirectory, 262
 - /www/htdocs directory, 249
- X**
- XMAS Scan, 104
 - X-Windows, 27, 29
- Y**
- Yacc, 168
- Z**
- Zimmerman, Phil, 286–287
 - Zombies, 8