

# Index

## • Numbers & Symbols •

802.11b/802.11i standards (IEEE), 157  
2600 – *The Hacker Quarterly* (magazine), 27

## • A •

- access controls
  - Linux systems, 203
  - Web servers, 285
- access points (AP), wireless networks
  - unauthorized, 158–160
  - vulnerabilities, 76, 148
- accounts, user
  - lockouts, 94
  - unused, 94
- Active Server Pages (ASP) script attacks, 289–290
- ActiveX controls malware attacks, 241–242
- Address Resolution Protocol (ARP)
  - poisoning/spoofing, 140–143
- ad-hoc mode (wireless LANs), 153
- admin account (NetWare), 231
- admin utilities (NetWare), 228
- AdRem NetWare management programs, 223
- Advanced EFS Data Recovery program (ElcomSoft), 101
- AES (Advanced Encryption Standard), 157
- African Whois (lookup) sites, 44
- AIM File Transfer security risks, 273
- AirJack wireless LAN security tool, 148
- AirMagnet wireless testing device, 150
- Aironet (Cisco) wireless card, 163
- AiroPeek (WildPackets) wireless LAN security tools
  - local airwave scans, 153–154
  - Monitor utility, 158–159
  - system analysis, 149
- AirSnort wireless LAN security tool
  - system analysis, 148
  - WEP-encryption cracking, 156
- airwaves, scanning local, 152–154
- Akin, Thomas (Southeast Cybercrime Institute), 259
- Akonix IM traffic-detection tools, 275–276
- all-in-one security-assessment tools, 170
- Amap application-detection software, 200–201
- anonymity, of hackers, protecting, 27–28
- antennas (wireless-network attacks), 150
- Antigen (Sybari Software) malware-prevention software, 254
- antivirus software, testing, 249–250
- AOL Instant Messenger security risks, 274
- AP (access points), wireless networks
  - default configurations, 162
  - unauthorized, 158–160
  - vulnerabilities, 148
- APNIC (Regional Internet Registry for Africa) lookup site, 44
- Apple Remote Access remote-connectivity software, 106
- application servers, security testing, 32
- Application Service Providers (ASPs), 33
- application-based attacks, 13–14
- approvals, written, importance of, 29–30, 323
- ARIN (Regional Internet Registry for North America) lookup site, 44
- ARP (Address Resolution Protocol)
  - poisoning/spoofing, 140–144
- ASP (Active Server Pages) script attacks, 289
- ASPs (Application Service Providers), 33
- assumptions, documenting, 36
- attachment attacks (e-mail), 260
- authentication
  - identifying requirements for, 48
  - weak, 84

authorization  
 importance of, 15, 29–30  
 tips for obtaining, 319–322  
 written approvals, 323

automated malware attacks, 243

automated scans (Web applications), 292–293

automated security assessments, 35, 311–312

automated-input attacks, 286–287

autoresponder attacks (e-mail), 262

AVERT Stringer (McAfee) antivirus program, 250–252

• **B** •

backdoor system access  
 for propagating malware, 244  
 using unsecured modems, 106

background checks, 60

banner-grabbing attacks  
 Netcat for, 130–131  
 telnet for, 130  
 testing for, 263–264

BBSs (bulletin board systems), 26

behavioral-analysis tools, 252–253

believability, 63

BigFix Patch Manager software, 213, 307

bindery contexts (NetWare), removing, 232–233

BIOS passwords, cracking, 100

black-hat (malicious) hackers, 10, 22, 24–25

BlackICE Web-application intrusion-prevention software, 295

BlackWidow Web-crawling tool  
 directory traversals, 284  
 function of, 42

blind assessments  
 versus knowledge assessments, 35  
 pros and cons, 40–41

bombs, e-mail, 258

bounced e-mail messages, 49

Browse rights (NetWare), 231–233

browsers, Web, scanning for information, 41

brute-force password attacks, 88

Brutus password-cracking software  
 cracking system passwords, 85  
 cracking Web logins, 282

buffer-overflow attacks, 208–209, 286

building infrastructure, 72–73

bulletin board systems (BBSs), 26

business goals, for ethical hacking plan, 30

• **C** •

Cain and Abel password-capture software, 85

Caldwell, Matt (GuardedNet, Inc.), 149

called IDs, 62

Antenna kits, 150

case studies  
 hacking e-mail, 259  
 hacking network infrastructures, 118  
 hacking Web applications, 281  
 hacking wireless networks, 149  
 malware attack, 238  
 physical security issues, 71  
 social-engineering attack, 57  
 war dialing, 107  
 Windows password vulnerabilities, 81

CERT/CC Vulnerability Notes Database  
 Web site, 49

CGI (Common Gateway Interface) script attacks, 289–290

Chappell, Laura (Protocol Analysis Institute), 118

CheckPoint firewall software, 295

Chirillo, John (*Hack Attacks Encyclopedia*), 12

chkconfig service (Linux), disabling, 203

Chknull password-cracking utility, 85

chkrootkit rootkit-detection tool, 254

Cisco LEAP protocol WERP keys, 156–157

Cisco routers, password vulnerabilities, 85

client applications, 32

Client Manager (Orinoco) wireless LAN security tool, 148

client operating systems, 32

Cobb, Chey (*Network Security For Dummies*), 101, 264, 308

code-injection attacks, 286–287

- COM ports, identifying, 111
- Common Gateway Interface (CGI) script attacks, 289
- Common Vulnerabilities and Exposures (CVE) Web site, 49, 300–301
- community of hackers, 26
- CommView for Wi-Fi (TamoSoft) wireless LAN-analyzer, 153
- comprehensive assessment tools, 37–38
- Computer Underground Digest* (magazine), 27
- computers. *See* physical-security attacks
- confidential information
  - and file sharing, 272–273
  - removing from Google Groups, 45
  - stealing off networks, 13
- configuration settings
  - Web servers, 285
  - wireless LANs, 162
- connection attacks (e-mail), 261–262
- console access (NetWare), 217
- contingency plans, 16, 35
- COPS file-monitoring program, 208
- copyrighted material, theft of, 26
- countermeasures, security. *See also*
  - security awareness training; security patches
  - Address Resolution Protocol protection, 143–144
  - autoresponder attack prevention, 262
  - awareness training, 56, 66–67, 92–93, 315–316
  - banner grab prevention, 131, 264
  - buffer-overflow attack prevention, 209
  - denial of service attack prevention, 145
  - disabling SMTP relays, 269
  - disabling unneeded services, 201
  - e-mail protections, 260–263, 269–272
  - firewall testing, 133
  - high-impact risks and responses, 305–306
  - instant messaging protections, 275–277
  - keystroke logging, 97–98
  - for Linux systems, 199, 210, 212–213
  - malware attack prevention, 253–254
  - NetBIOS attack prevention, 176–177
  - for NetWare systems, 220, 223–225, 228–234
  - Network File System protection, 207
  - network-analyzer attack prevention, 99–100, 139–140
  - network-infrastructure attack prevention, 146
  - null connection attack prevention, 184–186
  - ongoing ethical hacking, 311–312
  - operating system protection, 101–102
  - password protection, 91–94, 96–98, 100
  - port scanning prevention, 127–128
  - .rhosts and hosts.equiv file attack prevention, 205–206
  - remote procedure call protection, 178
  - script attack prevention, 290
  - SNMP attack prevention, 129
  - social-engineering attack prevention, 65–67
  - URL filter bypass prevention, 290–292
  - war dialing prevention, 114–115
  - Web directory traversal prevention, 285
  - Web-application attack prevention, 283, 289, 294–295
  - for Windows systems, 173–174
  - wireless LAN protection, 156–157, 159–160, 163
  - wireless workstation protection, 161–162
- Crack password-cracking software, 85
- crackers, defined, 10
- cracking passwords
  - brute-force attacks, 88
  - dictionary attacks, 87–88
  - documenting testing process, 34
  - inference attacks, 84
  - keystroke logging, 97–98
  - NetWare systems, 221–223
  - network analyzers, 98–100
  - in password-protected files, 95–97
  - password-reset programs, 100–101
  - shoulder surfing, 83
  - social-engineering attacks, 83
  - in systems with weak authentication, 84
  - tools for, 79, 85–87
  - weak storage systems, 98
  - on wireless LANs, 156
- crashing system during tests, 15

crawlers, Web, 284  
 criminal hackers, 24–25  
 cross-site scripting (XSS) Web-application attacks, 288  
 customer notification, importance of, 31  
 CVE (Common Vulnerabilities and Exposures) Web site, 49, 300–301  
 cyberterrorists, 23–24

## • D •

daemons (Linux), scanning, 195–199  
 database server testing, 32  
 DDoS (distributed DoS) attacks, 144  
 Debian Linux system updates, 213  
 Deep Freeze lock down program, 98  
 defaced Web pages, 25  
 delimited files, 182  
 deliverables, clarifying, 30  
 denial of service (DoS) attacks  
   defined, 13  
   indications of, 137–138  
   during testing, 15  
   types of, 144  
   using IM (instant messaging), 272  
 desktop auditing utilities, 276  
 DHAs (directory harvest attacks), 265  
 dictionary password attacks, 87–88  
 directional (wardriving) antennas, 150  
 directory-harvest attacks (DHAs), 265  
 directory-traversal attacks, 283–285  
 distributed DoS (DDoS) attacks, 144  
 DMZ/Shield Enterprise (Ubizen) intrusion-prevention software, 295  
 DNS queries, 43  
 documentation  
   of assumptions, 36  
   of test results and recommendations, 40, 303–304  
   of testing process, 34–35  
 domain-name information, 43  
 DOS debug program malware attacks, 243  
 DoS  
   defined, 13  
   indications of, 137–138  
   during testing, 15  
   types of, 144  
   using IM (instant messaging), 272

Draper, John (hacker), 22  
 drop ceilings, security risks, 72  
 dsniff network analyzer  
   analyzing UNIX systems, 135  
   e-mail packet sniffing, 270  
   malware attacks using, 242  
 dsrepair NLM (NetWare), 227  
 D-Tective reverse Whois service, 44  
 DumpSec vulnerability-assessment tool  
   operation system information, 48  
   security settings, 171  
   share permissions, 187  
   user and configuration settings, 182–183  
 dumpster diving  
   preventing, 74  
   risks from, 12, 61

## • E •

eBlaster (SpectorSoft)  
   keystroke-logging tool, 97  
   spyware, 241  
 Ecora  
   Enterprise Auditor IM traffic-detection tool, 276  
   Patch Manager patch-automation software, 307  
 Edgar Web site, 43  
 eDirectory (NetWare) directory service  
   disabling Public browse right, 231–233  
   vulnerabilities, 84  
 Eeye SecurellS intrusion-prevention software, 295  
 eicar test string, 249–250  
 802.11b/802.11i standards (IEEE), 157  
 ElcomSoft  
   Advanced EFS Data Recovery program, 101  
   password-cracking utilities, 95–96  
 elite hackers, 23  
 e-mail attacks  
   account enumeration, 265–266  
   anonymous addresses, 26  
   bounced messages, 49  
   e-mail bombs, 258  
   malware propagation, 243–244, 255, 270–271  
   using attachments, 260

- using autoresponders, 262
  - using connections, 260–261
  - e-mail packet sniffers, 270
  - e-mail servers
    - SMTP relay, 269
    - testing, 32
  - employees
    - security-awareness training, 56, 66–67, 92–93, 315–316
    - and social-engineering attacks, 55–56, 64
  - encryption
    - e-mail messages, 271
    - password databases, 101
    - for test results, 19
    - TKIP (Temporal Key Integrity Protocol), 157
    - user passwords, 82
  - Enforcer and L7 (Akonix) IM traffic-detection tools, 276
  - Enterprise Auditor (Ecora) IM traffic-detection tool, 276
  - enumerating (mapping out) networks, 46
  - Ethereal network analyzer, 17, 134
  - EtherPeek (WildPackets) network analyzer, 98–100, 134
  - ethical hacking. *See also* software and testing tools; testing process
    - ARP (Address Resolution Protocol) poisoning/spoofing, 140–144
    - automating application of, 311–312
    - benefits of, 31
    - collating data and test results, 299–301
    - cracking passwords, 82–91, 97–102
    - data analysis and recommendations, 20, 302–304
    - defined, 9–10
    - evaluating results, 20
    - footprinting, 41
    - goals, 10–12, 30–32
    - grabbing banner information, 130–131
    - identifying Web-based risks, 279–293
    - keeping up-to-date, 316
    - limits of, 324
    - Linux file attacks, 204–209
    - Linux system scans, 195–199, 211–212
    - malware intrusion scans, 244–253
    - NetWare system scans, 216–219
    - network analyses, 43–49, 134–140
    - network-infrastructure attacks, 117–121
    - obtaining sponsorship, authorization, 15, 29–30, 319–322
    - planning and preparation, 15–19
    - port scanning, 121–128
    - retesting, 20
    - scheduling tests, 30
    - similarity to beta testing, 39
    - similarity to malicious hacking, 39
    - SNMP scans, 129
    - social-engineering attacks, 56–59
    - stealthy versus open approaches, 40–41
    - system crashes, 15
    - timing of tests, 326
    - values, 14–15
    - war dialing, 105–115
    - Windows systems scans, 171–178
    - wireless LAN attacks, 148–163, 158–159
  - ettercap (Source Forge) network analyzer
    - ARP spoofing, 135, 141
    - malware attacks, 242
  - event-logging systems, 312–313
  - Exchange e-mail system, 84
  - EXPN command (SMTP), 265–266
  - external hacks, 36
  - external system scans, 47
- **F** ●
- FaceTime Communications IM traffic-detection tool, 276
  - false employees, dangers from, 55–56. *See also* social-engineering attacks
  - FedCIRC Incident Handling Checklist, 244–245
  - file names
    - illegitimate, 245
    - on Web servers, 284
  - file system. *See also* password attacks
    - file-sharing risks, 272–273
    - malware attacks using, 255–256
  - File Transfer Protocol (FTP)
    - vulnerabilities, 200
  - file-modification auditing programs, 208
  - file/print server testing, 32
  - financial information, scanning for, 60

- find command (Linux), 207
- fingerprinting
  - Linux OS, 196–197, 294
  - Windows OS, 174
- Finjan Software Test Center Web site, 252–253
- Firewalk (Packet Factory) firewall-testing tool, 133
- Firewall Informer (BLADE Software) firewall-testing tool, 133
- firewalls
  - e-mail, 263, 271
  - Linux systems, 199
  - NetBIOS attacks, 177
  - testing, 32, 131–133
  - Web applications, 295
  - Windows systems, 173–174
- Flawfinder security-hole software, 295
- Fluke WaveRunner wireless testing device, 150
- footprinting, 41
- Fortres 101 for Windows lock-down program, 98
- fping ping utility (UNIX systems), 46
- FreeZip decompression tool, 89
- FTP (File Transfer Protocol)
  - vulnerabilities, 200
- FU rootkit, 240–241

## ● G ●

- GetPass login-decryption software, 85
- GFI Email Security Testing Zone, 250
- GFI LANguard Network Security Scanner
  - vulnerability-assessment tool
    - event logging, 312–313
    - firewall testing, 132
    - patch checking, 307
    - testing Linux systems, 195, 197–198
    - testing NetWare systems, 216, 218–219
    - testing Windows systems, 170, 172–173, 191
    - testing wirelessLANs, 149
    - uses for, 121
    - viewing share permissions, 188–189
- goals, ethical hacking, 10–12, 30–32

- Google search engine
  - Google Groups, 45
  - locating security tools using, 18
  - public information searches, 41–42
- government Whois (lookup) sites, 44
- Greenidea, Inc. Web site, 315

## ● H ●

- Hack Attacks Encyclopedia* (Chirillo), 12
- hacked Web sites, defacing of, 25
- hacker Web sites, 26
- hackers. *See also* ethical hacking
  - changing view of, 21–22
  - cyberterrorists, 24
  - elite hackers, 23
  - ethical versus malicious, 9–10
  - government agencies, 23
  - hacker community, 26
  - hackers for hire, 24
  - hacktivists, 23–24
  - importance of anonymity to, 27–28
  - intermediate hackers, 23
  - outsourcing, 312–315
  - personality profiles, 22–23
  - reasons for hacking, 24–26
  - script kiddies, 21, 23
  - work methods, 26–27
- The Hacker's Choice software
  - THC-Amap application-version-mapping tool, 195
  - THC-Scan war-dialing programs, 46, 109–110
- hacking tools. *See* software and testing tools
- hardening operating systems, 101, 308–309
- hardening servers, 264
- hardware. *See also* physical-security attacks
  - network, vulnerabilities of, 75–77
  - for wireless-network attacks, 150
- headers, e-mail, 269–270
- HFNetChk Pro (Shavlik Technologies)
  - patch-automation software, 307
- hidden field manipulation, 287–288
- high impact security vulnerabilities, 302

honeypots, 27  
Hoovers.com Web site, 42–43, 60  
host names, 46  
hosts.equiv file(Linux) attacks, 204  
Hyena security-assessment software, 191  
Hypertext Transfer Protocol (HTTP)  
  attacks involving, 14  
  vulnerabilities, 279–280

## • I •

ICAT Metabase list of password  
  vulnerabilities, 82  
IDSs (Intrusion Detection Systems), 33  
IEEE 802.11b standard, 157  
IM (instant messaging)  
  reducing risks from, 275–277  
  vulnerabilities from, 272–275  
IM Logic IM traffic-detection tool, 276  
inbound access (modems), 106  
individualism, 24  
inetd.conf service (Linux), disabling,  
  202–203  
inference password attacks, 84  
information-gathering attacks  
  banner grabs, 263–264  
  footprinting, 41  
  identifying vulnerabilities, 49–51  
  mapping the network, 43–45  
  penetrating security holes, 51–52  
  for social-engineering attacks, 60–62  
  system scans, 45–49  
  Web searches, 41–42  
information-security vulnerabilities  
  importance of identifying, 11–12  
  network-infrastructure attacks, 13  
  nontechnical attacks, 12  
  sharing system information, 45  
infrastructure vulnerabilities, 309  
input attacks (Web applications)  
  automated input, 286  
  code injection, 287  
  cross-site scripting (XSS), 287  
  hidden field manipulation, 287–288  
instant messaging (IM)  
  reducing risks from, 275–277  
  vulnerabilities from, 272–275

insurance, personal liability, 30  
intermediate hackers, 23  
internal hacks, 36  
internal system scans, 46–47  
Internet Relay Chat (IRC), 26. *See also*  
  instant messaging (IM)  
Internet vulnerabilities, 243. *See also* Web-  
  application attacks  
Internet Service Providers (ISPs), 33  
Interpact, Inc. Web site, 315  
intruder lockout, 94  
Intrusion Detection Systems (IDSs)  
  for Novell NetWare systems, 224–225  
  for service providers, 33  
IP addresses and host names  
  capturing using instant messaging, 272  
  scanning for, 46  
  viewing, 46  
IP Personality Web site, 294  
IRC (Internet Relay Chat), 26. *See also*  
  instant messaging (IM)  
ISO 177799 security framework, 30  
ISPs (Internet Service Providers), 33  
ITS4 security-hole software, 295  
ITsecurity.com security portal, 18  
IZArc decompression tool, 89

## • J •

Java applets, malware attacks using, 241  
JavaScript programs, malware attacks  
  using, 242  
John the Ripper password-cracking tool,  
  17, 85, 88–91

## • K •

Kerberos authentication system, 84  
KeyGhost keystroke-logging tool, 97  
KeyLogger Stealth software, 97  
keystroke logging, 97–98  
Kismet wireless LAN security tool  
  scanning local airwaves, 153  
  uses for, 148  
Knark for Linux rootkit, 240–241  
knowledge versus blind assessments, 35

## • L •

LACNIC (Latin American and Caribbean Internet Address Registry) lookup site, 44

LANGuard Network Security Scanner (GFI) vulnerability-assessment tool

- firewall testing, 132
- testing Linux systems, 195, 197–198
- testing NetWare systems, 216, 218–219
- testing Windows systems, 170, 172–173, 191
- testing wireless LANs, 149
- viewing share permissions, 188–189

LANs (local area networks). *See* wireless LANs (WLANs)

laptop computers

- resetting passwords, 100
- testing, 32

Latin American and Caribbean Internet Address Registry (LACNIC) lookup site, 44

LC4 password-cracking tool, 17, 85

LEAP protocol (Cisco), 157

legacy application configurations, 115

legal warnings, 131

Legion vulnerability-assessment tool, 171, 176

likeability, 62

Linux Security Auditing Tool (LSAT), 195

Linux systems

- buffer overflows, 208–209
- general security tests, 211–212
- hosts.equiv file attacks, 204–205
- malware attacks, 247–249
- Network File System attacks, 206–207
- operating system access, 102
- password storage locations, 87
- physical-security vulnerabilities, 209–210
- .rhosts file attacks, 204
- rogue file permissions, 207–208
- rootkits for, 240
- security patches, 212–213
- system vulnerabilities, 193–194
- tools for, 194–195

- unauthorized scans, 195–199
- unnneeded services, 200–201

lock-down programs, 98

logged in NetWare server access, 217

logging

- e-mail, 271
- instant messages, 275
- system events, 40, 312–313

logic bombs, 242

logins

- insecure, 171, 280–282
- unauthorized, 224–225, 229

lookup sites (Whois lookups), 43–44

low impact security vulnerabilities, 302

LSAT (Linux Security Auditing Tool), 195

lsf tool (Linux)

- testing for malware intrusions, 248
- uses for, 201

## • M •

MAC (media access control) addresses

- vulnerabilities, 140, 151–152

Macintosh system lock-down programs, 98

magazines for hackers, 27

malicious hackers

- defined, 10
- monitoring for, 312–313

malware attacks

- automated, 243
- dangers from, 237–239
- defined, 237
- logic bombs, 242
- reporting, 253
- rootkits, 240–241
- spyware, 241
- testing systems for, 245–247
- Trojan houses, 239–240
- using e-mail, 243–244, 270–271
- using instant messages, 272
- using internal security tools, 242–243
- using programming interfaces, 241–242
- using vulnerable ports, 244
- viruses, 239–240
- worms, 240

*Malware: Fighting Malicious Code*  
(Skoudis), 238

malware-protection software, 253–254, 271

Man-in-the-Middle (MITM) attacks, 140

mapping networks

  Google Groups, 45

  Whois lookups, 43–44, 46

mapping null sessions, 179–180

Maven Security Consulting, Inc.

  Web site, 107

MBSA (Microsoft Baseline Security  
Analyzer) tool, 169–170, 190–191, 308

media access control (MAC) address  
  vulnerabilities, 140, 151–152

medium impact security  
  vulnerabilities, 302

messaging-system attacks

  banner grabbing, 263–264

  system vulnerabilities, 257–258

  using e-mail, 258–263

  using instant messaging, 272–275

  using Simple Mail Transfer Protocol,  
  265–272

Microsoft. *See also* Windows (Microsoft)  
  systems

  Baseline Security Analyzer (MBSA) tool,  
  169–170, 190–191, 308

  .NET application vulnerabilities, 241

  Software Update Services (SUS)  
  Server, 308

  Virtual PC system-scanning software, 46

military Whois (lookup) sites, 44

Minor Threat (ToneLoc software), 109

MITM (Man-in-the-Middle) attacks, 140

Mitnick, Kevin (hacker), 22

mobile device testing, 32. *See also* wireless  
  LANs (WLANs)

modems

  identifying COM port, 111

  physical placement, 115

  protecting against war dialing, 114–115

  unsecured, 46, 105–106

  vulnerability testing, 113–114

  for war dialing, 109–110

monitoring security events, 312–313

Mucho Maas (ToneLoc software), 109

## • N •

NAT (NetBIOS Auditing Tool) password-  
cracking tools, 85, 86

National Institute of Standards and  
Technology (NIST)

  ICAT Metabase Web site, 49

  operating system hardening practices,  
  101, 264, 308

National Security Agency

  operating system hardening practices,  
  264, 308

  Security Recommendation  
  Guidelines, 101

nbtstat NetBIOS attack program, 175

NCP packet signing (NetWare),  
  enabling, 230

NCPQuery enumeration software, 216

Nessus vulnerability-assessment tool  
  features, 50, 121

  firewall testing, 132

  malware attacks using, 242

  testing Linux systems, 195, 196–197

  testing Windows systems, 170

net use command, 247

net view command, 180–181

netbasic NLM (NetWare), 227

NetBIOS

  attacks on, 175–177

  blocking access to, 184

  vulnerability of, 13

NetBIOS Auditing Tool (NAT) password-  
cracking utilities, 85

Netcat banner-grabbing tool

  features, 130–131

  firewall testing, 132–133

  malware attacks using, 242

  network scanning, 120

Netcraft Web server-versioning tool, 48–49

netfilter/iptables Linux firewall, 199

NetScanTools Pro

  network scanning program, 120, 128

  ping tool, 46

NetScreen firewall software, 295

- netstat command
  - testing for malware intrusions, 245–248
  - testing Linux services, 201
- NetStumbler wireless LAN security tool
  - features, 148
  - scanning local airwaves, 152–153
  - testing unauthorized wireless LAN access points, 158
- NetWare Loadable Module (NLM)
  - password storage location, 223
  - rconsole attacks, 221
  - rogue programs, 225–229
- NetWare (Novell) systems
  - clear-text packets, 229–230
  - debugger, 243
  - intruder detection settings, 224–225
  - NCPQuery information, 219
  - Novell ConsoleOne access, 232–233
  - password testing, 85
  - port scanning, 217–219
  - Remote Console attacks, 221–223
  - rogue NLM programs, 225–229
  - server-console attacks, 224
  - system vulnerabilities, 215–216
  - testing tools, 216
- network cards
  - promiscuous mode, 135
  - testing for malware intrusions, 249
- Network File System (NFS) attacks, 205–206
- Network Mapper (NMap) port scanner
  - identifying host IP addresses, 46
  - limits of, 37–38
  - uses for, 17, 18
- network mapping
  - Google Groups, 45
  - Web site privacy policies, 45
  - Whois (lookup) sites, 43–44
- network scanning software, 120, 250–252
- Network Security For Dummies* (Cobb), 101, 264, 308
- Network Solutions Web site, 43
- Network Users (Optimum X)
  - login-scanning tool, 171
  - vulnerability-assessment tool, 183–184
- network-analyzer attacks
  - how they work, 134–140
  - packet sniffing, 98–100
  - running, 136–139
  - tools for, 17
- network-analyzer tools
  - capturing e-mail traffic using, 270
  - malware attacks using, 242
  - monitoring network traffic, 46
- network-infrastructure attacks
  - application-based attacks, 13–14
  - ARP (Address Resolution Protocol) poisoning/spoofing, 140–144
  - banner grabbing, 130–131
  - case study, 118
  - firewall vulnerabilities, 131–133
  - locations for, 36
  - network analyzers, 134–140
  - operating-system attacks, 13
  - password vulnerability, 85–86
  - port scanning, 46
  - scanning tools, 120
  - shares authentication, 48
  - Simple Network Management Protocol scans, 129
  - sniffers, 134–140
  - testing process, 32
  - vulnerability assessments, 119–121
- NFS (Network File System) attacks, 206–207
- Nikto Web-application-evaluation tool
  - automated scans, 292–293
  - features, 280
- NIST (National Institute of Standards and Technology)
  - ICAT Metabase Web site, 49
  - operating system hardening practices, 101, 264, 308
- NLM (NetWare Loadable Module)
  - password storage location, 223
  - rconsole attacks, 221–222
  - rogue programs, 225–229
- Nmap (Network Mapper) port scanner
  - features, 17–18, 46
  - limits of, 37–38
  - ping sweeps, 124
  - scanning systems using, 173
  - testing for malware intrusions, 250–251
  - testing Linux systems, 195, 198, 200–201
  - testing Windows systems, 169
  - using, 120, 126–127
- NMapWin port scanner, 46, 48, 120
- nontechnical attacks, 12
- not-logged in NetWare server access, 217

Novell NetWare  
 clear-text packets, 229–230  
 debugger, 243  
 intruder detection settings, 224–225  
 NCPQuery information, 219  
 Novell ConsoleOne access, 232–233  
 password testing, 85  
 port scanning, 217–219  
 Remote Console attacks, 221–223  
 rogue NLM programs, 225–229  
 server-console attacks, 224  
 system vulnerabilities, 215–216  
 testing tools, 216  
 NTAAccess password-resetting  
 program, 101  
 NTFSDOS Profession password-cracking  
 utilities, 85  
 null session attacks (Windows), 179–184

## • 0 •

Oechslin, Philippe (Swiss Federal Institute  
 of Technology), 81  
 office layout, risks associated with, 74–75  
 omnidirectional antennas, 150  
 open ports, scanning for, 48  
 open source software  
 hacking tools, 37–38  
 PasswordSafe encryption tool, 92  
 OpenSSH (Linux) vulnerability testing, 196  
 operating systems  
 access limits, 101  
 fingerprinting, 174  
 hardening, 264, 303, 308–309  
 rootkits attacks, 240–241  
 vulnerabilities, 48–49, 198–199  
 operating-system attacks, 13  
 organizational (end-user) password  
 vulnerabilities, 80–81  
 Orinoco Registry Encryption/Decryption  
 (Lucent) program, 161  
 outbound access (modems), 106  
 outcomes, identifying before starting  
 hacking process, 30  
 outsourcing  
 ethical hacking, 313–315  
 security monitoring, 312–313

## • p •

Pandora  
 NetWare hacking suite, 229–230  
 password-cracking tool, 85  
 password attacks  
 brute-force attacks, 88  
 cracking tools, 85–87  
 dictionary attacks, 87–88  
 how they work, 86  
 inference attacks, 84  
 keystroke logging, 97–98  
 locations for, 36  
 network analyzers, 98–100  
 recognizing, 79–80  
 resetting programs, 100–101, 226–227  
 shoulder surfing, 83–84  
 social-engineering attacks, 83–84  
 success of, 82  
 Trojan horses, 94  
 password vulnerabilities  
 authentication systems, 84  
 Novell NetWare systems, 221–223  
 organizational end-users, 80–81  
 passwords in limbo, 100  
 privacy issues, 64  
 protecting against, 79, 91–94  
 storage issues, 87, 92, 98  
 Windows shares, 177  
 password-protected files, 95–97  
 Patch Manager (Ecora) patch-automation  
 software, 307  
 patches, security  
 automated, 307–308  
 for e-mail attacks, 271  
 for Linux systems, 212–213  
 managing, 306–307  
 for NetWare systems, 220, 234  
 for Windows systems, 188–190, 308  
 PatchManager (Big Fix) patch-automation  
 software, 307  
 pcAnyware remote-connectivity  
 software, 106  
 penetration testing, 10, 34  
 perimeter e-mail protection, 263  
 personal liability insurance, 30

- personnel
    - security-awareness training, 56, 66–67, 92–93, 315–316
    - and social-engineering attacks, 55–56, 64
  - PestPatrol Web site
    - Auditor’s Edition scanning tool, 251–252
    - catalog of pests, 245
    - war-dialing programs, 109
  - PGP (Pretty Good Privacy) encryption
    - for password databases, 92
    - using, 19
  - phone line vulnerabilities, 114–115
  - PhoneSweep
    - telephone line-scanning program, 114
    - war-dialing software, 46
  - phone-switch software, accessing, 62
  - PHRACK* (magazine), 27
  - physical-security attacks
    - common, 69–71
    - on Linux systems, 209–210
    - network components and computers, 75–77
    - versus social-engineering attacks, 55
    - types of, 12
    - using buildings and offices, 71, 74–75
    - using utility systems, 73–74
    - on wireless LANs, 160
  - Ping of Death DoS attacks, 144
  - ping tool
    - scanning systems using, 46
    - using from external location, 47
  - planning and preparation, 15–19
  - port scanning
    - commonly hacked ports, 122–123
    - indications of, 139
    - information provided by, 121–122, 124–125
    - mapping programs, 246
    - NetWare systems, 217–219, 227
    - number assignments, viewing, 48
    - for open ports, 46–47
    - ping sweeps, 124
    - tools for, 46
  - portals, security, 18
  - PortSentry intrusion-prevention software, 199
  - Prescan tool (ToneLoc), 108
  - Pretty Good Privacy (PGP) encryption
    - for password databases, 92
    - using, 19
  - privacy
    - and civil liberty, 26
    - need for, during hacking process, 19
    - policies, vulnerabilities from, 45
    - respecting, during hacking process, 14–15
  - Procomm Plus remote-connectivity software, 106
  - programming interface vulnerabilities, 241–242
  - PromiscDetect network-analyzer attack detector, 140
  - promiscuous mode, 135
  - propagation of malware
    - automated, 243
    - backdoor access, 244
    - using e-mail, 243–244, 255, 270–271
    - using instant messaging, 272
  - property, physical, protecting, 69–70
  - protocols, identifying, 47
  - ps malware-intrusion testing tool, 248–249
  - public information, locating, 41–43
  - pwdump, pwdump2 password-cracking tools, 17, 85, 88–91
- *Q* •
- QualysGuard (Qualys) vulnerability-assessment tool
    - features, 50
    - testing Linux systems, 195, 198–199
    - testing Windows systems, 170
- *R* •
- RAS (remote access servers), 105
  - RATs (remote-access Trojans), 138, 239–240
  - RATS security-hole software, 295
  - RC4 encryption algorithm, 155
  - Rconj NetWare-management program, 223
  - rconsole (Remote Console, NetWare) attacks, 221–223
  - reconnaissance missions
    - banner grabs, 263–264
    - footprinting, 41

- identifying vulnerabilities, 49–51
  - mapping the network, 43–45
  - penetrating security holes, 51–52
  - for social-engineering attacks, 60–62
  - system scans, 45–49
  - Web searches, 41–42
- Recording Industry Association of America (RIAA) copyright lawsuits, 26
- Red Hat Linux system updates, 213
- red teams, 31
- reformed hackers, hiring, 315
- Regional Internet Registry for Africa (APNIC) lookup site, 44
- Regional Internet Registry for North America (ARIN) lookup site, 44
- Register Fly Web site, 43
- relays (SMTP), vulnerabilities, 266
- remote access servers (RAS), 105
- Remote Console (rconsole, Novell NetWare) attacks, 221–223
- Remote password-cracking software, 216
- remote procedure call (RPC) enumeration, 177–178
- remote-access services, 48
- remote-access Trojans (RATs), 138, 239–240
- repeat dial tones, 106
- reports, 302–304. *See also* documentation
- resetting passwords
  - cautions about, 100–101
  - in NetWare systems, 226–227
- results, test data, evaluating, 20, 302–304
- reverse Whois services, 44
- Rhoades, David (Maven Security Consult, Inc.), 107
- .rhosts files (Linux), attacks on, 204
- RIAA (Recording Industry Association of America) copyright lawsuit, 26
- RIPE Network Coordination Centre lookup site, 43–44
- risks, evaluating and ranking, 300–302
- Rkdet rootkit-detection tool, 254
- robots.txt file, searching for, 283–284
- Rogue Aware (Akonix) IM traffic-detection tool, 275–276
- rogue modems, 13
- root passwords, cracking, 82
- rootkits
  - detection tools, 254
  - uses for, 240–241
- routers, testing, 32
- RPC (remote procedure call) enumeration, 177–178
- Rpcdump port scanning tool, 171, 178
- r-services (Linux) vulnerabilities, 198, 200

## • S •

- SAM (Security Account Manager)
  - database, 87
- Sam Spade for Windows network scanning program, 43, 109, 120, 267
- sandboxes, 241
- SANS Institute
  - operating system hardening practices, 101, 264, 308
  - Top 20 Internet Security Vulnerabilities consensus list, 50
- SATAN (Security Administrator Tool for Analyzing Networks), 18, 38
- scanning local airwaves, 152–154
- scans, system
  - banner grabbing, 263–264
  - information obtained from, 47–49
  - penetrating security holes, 51–52
  - using network analyzers, 46–47
  - using port scanners, 46–47
  - using unsecured modems, 46
- screen captures, as documentation, 40
- script attacks (Web applications), 289–290
- script kiddies, 21, 23
- scripting program vulnerabilities, 241–242
- SearchSecurity.com security portal, 18
- SeattleWireless Hardware Comparison Web page, 150
- SEC filings Web site, 60
- second dial tones, 106, 110
- SecureIIS (Eeye) Web-application intrusion-prevention software, 295
- Security Account Manager (SAM)
  - database, 87
- Security Administrator Tool for Analyzing Networks (SATAN), 18
- Security Awareness, Inc. Web site, 315

- security awareness training, 56, 66–67, 92–93, 315–316
- security holes, 26–27, 36, 51–52
- security infrastructure, assessing and enhancing, 309
- security measures. *See also* security awareness training; security patches
  - Address Resolution Protocol protection, 143–144
  - autoresponder attack prevention, 262
  - awareness training, 56, 66–67, 92–93, 315–316
  - banner grab prevention, 131, 264
  - buffer-overflow attack prevention, 209
  - denial of service attack prevention, 145
  - disabling SMTP relays, 269
  - disabling unneeded services, 201
  - e-mail protections, 260–263, 269–272
  - firewall testing, 133
  - high-impact risks and responses, 305–306
  - instant messaging protections, 275–277
  - keystroke logging, 97–98
  - for Linux systems, 199, 210, 212–213
  - malware attack prevention, 253–254
  - NetBIOS attack prevention, 176–177
  - for NetWare systems, 220, 223–225, 228–234
  - Network File System protection, 207
  - network-analyzer attack prevention, 99–100, 139–140
  - network-infrastructure attack prevention, 146
  - null connection attack prevention, 184–186
  - ongoing ethical hacking, 311–312
  - operating system protection, 101–102
  - password protection, 91–94, 96–98, 100
  - port scanning prevention, 127–128
  - .rhosts and hosts.equiv file attack prevention, 205–206
  - remote procedure call protection, 178
  - script attack prevention, 290
  - SNMP attack prevention, 129
  - social-engineering attack prevention, 65–67
  - URL filter bypass prevention, 290–292
  - war dialing prevention, 114–115
  - Web directory traversal prevention, 285
  - Web-application attack prevention, 283, 289, 294–295
  - for Windows systems, 173–174
  - wireless LAN protection, 156–157, 159–160, 163
  - wireless workstation protection, 161–162
- security patches
  - automated, 307–308
  - for e-mail attacks, 271
  - for Linux systems, 212–213
  - managing, 306–307
  - for NetWare systems, 220, 234
  - for Windows systems, 188–190, 308
- security policies, 66
- security portals, 18
- security seals, 30
- security vulnerabilities, ranking, 300–301
- SecurityFocus.com security portal, 18
- SecurityProfiling Syspdate patch-automation software, 307
- security-testing tools, overview, 18–19, 37–38. *See also* software and testing tools
- self-replicating viruses and worms, 239–240
- semidirectional antennas, 150
- sendmail security vulnerabilities, 200
- server-console (NetWare)-attacks, 224
- servers
  - identifying software used by, 48
  - viewing operating systems, applications, 32
- services
  - unneeded, disabling, 199, 272
  - in use, identifying, 47
- setpwd NLM (NetWare), 226
- setspass NLM (NetWare), 226
- setspwd NLM (NetWare), 226
- shares (Windows) attacks, 176, 186–189
- Shavlik technologies HFNetChk Pro patch-automation software, 307
- shoulder surfing, 83
- Sima, Caleb (SPI Dynamics, Inc.), 281
- Simple Mail Transfer Protocol (SMTP)-based attacks
  - account enumeration attacks, 265–266
  - banner grabs, 263–264
  - e-mail header disclosures, 269–270
  - e-mail relays, 266–269
  - types of, 14

- Simple Network Management Protocol (SNMP) attacks, 129
- Skoudis, Ed (security expert and author), 238
- Slackware Linux system updates, 213
- SMAC MAC-spoofing software, 142–143
- SMTP
  - account enumeration attacks, 265–266
  - banner grabs, 263–264
  - e-mail header disclosures, 269–270
  - e-mail relays, 266–269
  - types of, 14
- smtpscan banner-grabbing software, 264
- Smurf DoS attack, 137–138, 144
- SNARE intrusion-prevention software, 199
- sniffdet network-analyzer attack detector, 140
- SNMP (Simple Network Management Protocol) attacks, 129
- social-engineering attacks
  - behaviors associated with, 62–64
  - case study, 57
  - cracking passwords, 83
  - deceptive practices, 63–65
  - defending against, 65–67
  - defined, 12, 55–56
  - and ethical hacking, 56–59
  - versus physical-security attacks, 55
  - system reconnaissance, 43, 60–62
- software and testing tools
  - banner grabbing, 264
  - behavioral-analysis, 252–253
  - capturing e-mail traffic, 270
  - cautions when using, 38
  - choosing correctly, 325
  - desirable features, 38
  - e-mail header disclosures, 269–270
  - e-mail malware propagation, 243–244
  - firewall testing, 132
  - instant message monitoring, 275–276
  - keystroke logging, 97
  - Linux security testing, 195, 213
  - Linux service assessments, 200–201
  - MAC spoofing, 142–143
  - NetWare security testing, 216, 229–230
  - network analyzers, 134–135
  - null session attacks, 179–180
  - password-cracking utilities, 85–87, 95–96
  - rootkit detection, 254
  - spyware scanning, 250–252
  - testing SMTP relays, 266–267
  - vulnerability assessment, 50–51, 280
  - war dialing, 108–111
  - Windows security testing, 168–171
  - Wired Equivalent Privacy encryption cracking, 156
  - wireless LAN security testing, 148–149
- software, malicious
  - automated, 243
  - dangers from, 237–239
  - defined, 237
  - logic bombs, 242
  - reporting, 253
  - rootkits, 240–241
  - spyware, 241
  - testing systems for, 245–247
  - Trojan houses, 239–240
  - using e-mail, 243–244, 270–271
  - using instant messages, 272
  - using internal security tools, 242–243
  - using programming interfaces, 241–242
  - using vulnerable ports, 244
  - viruses, 239–240
  - worms, 240
- Spector Pro (SpectorSoft)
  - keystroke-logging tool, 97
  - spyware, 241
- SPI Dynamics
  - Web site URL, 65
  - WebInspect application-evaluation tool, 280
- spider programs, 284
- Spies Among Us* (Winkler), 57
- Spitzner, Lance, Web site, 27
- sponsorship for ethical hacking
  - importance of obtaining, 15
  - tips for obtaining, 319–322
  - written approvals, 323
- spyware, 241
- startup files, testing for malware
  - intrusions, 247–248
- stealthy versus open hacking approaches, 40–41
- A Step-by-Step Guide to Computer Attacks and Effective Defenses* (Skoudis), 238
- strangers, responding to with caution, 67, 75

- SuperScan port scanner
    - features, 17, 125–126
    - identifying malware intrusions, 250–251
    - limits of, 37
    - ping sweeps and port scanning, 46, 120
    - testing Linux systems, 195, 195–196
    - testing NetWare systems, 216, 218
    - testing Windows systems, 170–173
  - SUS (Microsoft Software Update Services) Server, 308
  - SuSE/Novell Linux system updates, 213
  - switches, in Google searches, 42
  - SYN flood DoS attacks, 144
  - SYSKEY encryption tool, 101
  - system auditing feature (NetWare), 233–234
  - system crashes, 14–15
  - system login files, 88
  - system scans
    - information obtained from, 47–49
    - IP addresses and host names, 46
    - Linux systems, 195
    - network analyzers for, 46–47
    - penetrating security holes, 51–52
    - port scanners for, 46–47
    - unsecured modems, 46
    - Windows systems, 171–173
  - SysTrust security seal, 30
  - SysUpdate patch-management tool, 213
  - SysUpdate (SecurityProfiling) patch-automation software, 307
- T ●
- tablet PCs, testing, 32
  - tarpitting, 262
  - TCP port scans, 125–128
  - TCP Wrappers access-control tool, 203
  - tcpcon NLM (NetWare), testing, 227–228
  - TCP/IP communications
    - NetWare parameter settings, 234
    - protocol vulnerabilities, 13
  - technical password vulnerabilities, 82
  - Techno Security Web site, 71
  - telephone system vulnerabilities, 61–62, 106
  - telnex tool
    - banner grabbing, 130
    - SMTP relay testing, 267–269
    - security vulnerabilities, 200
  - Temporal Key Integrity Protocol (TKIP)
    - encryption, 157
  - testing. *See also* ethical hacking; software and testing tools
    - capturing clear-text packets, 229–230
    - choosing test systems, 32–33
    - crashing system during, 15
    - for DoS attacks, 145
    - for e-mail header disclosures, 269–270
    - for firewall vulnerabilities, 132–133
    - goals for, 30–32
    - IM (instant messaging) security, 274–275
    - for insecure Web logs in, 280–282
    - Linux security, 195–201
    - locations for, 36
    - logging and documenting, 40
    - for malware intrusions, 244–253
    - for NetBIOS attacks, 174–176
    - NetWare security systems, 216–224
    - process of, 19
    - results from, 19–20, 299–301
    - retesting, 20, 324
    - for rogue file permissions, 207
    - for rogue NLMs, 226
    - for share permissions, 187–189
    - for SMTP relays, 266–267, 266–269
    - timing and timelines for, 33–36, 326
    - for unauthorized access points, 158–159
    - for unprotected shares, 187–189
    - for URL filter bypasses, 290–292
    - for vulnerable malware ports, 244
    - Web directory security, 283–284
    - Windows system security, 171–173, 180–184, 189–191
  - TFN (Tribe Flood Network) DoS attacks, 144
  - Tiger Linux security-auditing tool, 195, 211–212
  - tiger teams, 31
  - Timbuktu for Apple remote-connectivity software, 106
  - timing and timelines, 33–36, 326
  - TippingPoint Technologies firewall software, 295
  - TKIP (Temporal Key Integrity Protocol)
    - encryption, 157
  - toneloc command, 112

ToneLoc (Minor Threat, Mucho Maas)  
 Phun-Pak Prescan utility, 108  
 war-dialing program, 108–111  
 tone.log file (ToneLoc program), 112  
 tools, security. *See* software and testing tools  
 traffic  
 e-mail, monitoring, 270  
 instant messaging, monitoring, 275–276  
 network, restricting, 127–128  
 wireless, 154, 155–156  
 Tribe Network (TFN) DoS attacks, 144  
 Trinoo DoS attacks, 144  
 Tripwire file-monitoring program, 208  
 Trojan horse attacks  
 features, 239–240  
 password-cracking, 94  
 tester software, 244–245  
 types of, 245  
 using instant messaging, 272  
 TrueActive spyware, 241  
 trust  
 and ethical hacking, 14  
 and social-engineering attacks, 62–63  
 2600 – *The Hacker Quarterly* (magazine), 27

• U •

Ubizen DMZ/Shield Enterprise Web-application intrusion-prevention software, 295  
 unauthorized logins (Novell NetWire), 229  
 UNIX systems  
 cracking passwords on, 90  
 e-mail packet sniffers, 270  
 MAC-address spoofing, 142  
 network-analyzer attack detectors, 140  
 for operating system access, 102  
 password-storage locations, 87  
 ping utilities, 46  
 rootkits for, 240–241  
 network analyzer attacks, 134–135  
 wireless LAN security tools, 148  
 unlimited attack approach, 16, 35  
 unneeded services  
 disabling, 272  
 security vulnerabilities, 200–201

URL filter bypasses, 290–292  
 U.S. government, hacking by, 23  
 U.S. Patent Office Web site, 43  
 user accounts  
 password protection strategies, 92–94  
 unused, eliminating, 94  
 user IDs for Web logins, viewing, 280–282  
 utilities, physical, protecting, 73–74

• V •

VBScripts, malware attacks using, 242  
 viruses, 240  
 Vision (Foundstone)  
 port-mapping software, 246–247  
 system-analyzer software, 169  
 Visual Basic, VBScript vulnerabilities, 242  
 VLAD the Scanner Linux security-auditing tool, 212, 195  
 VMware Workstation system-scanning software, 46  
 voice-mail systems, vulnerabilities, 106  
 VPN services, identifying, 48  
 VRFY command (SMTP), 265–266  
 vulnerability-assessment tools. *See also*  
 GFI LANguard Network Security Scanner vulnerability-assessment tool  
 DumpSec, 48, 171, 182–183, 187  
 Legion, 171, 176  
 Network Users (Optimum X), 183–184  
 QualysGuard, 50, 170, 195, 198–199  
 Walksam, 171, 183  
 vulnerable systems, criteria for identifying, 33

• W •

Walksam vulnerability-assessment tool, 171, 183  
 WANRemote RAT attacks, 138  
 war dialing  
 attack process, 106–108  
 case study, 107  
 configuring programs for, 110–111  
 defined, 105  
 dialing-in process, 110–113  
 documenting testing process, 34  
 information gathering stage, 108–109

- war dialing (*continued*)
  - modems for, 109
  - protecting against, 114–115
  - scanning modems, ports, 46–47
  - software tools, 109
- wardriving (directional) antennas, 150
- weak authentication, 84
- weak passwords, 88
- Web access (NetWare), 217
- Web browsers, obtaining system information from, 41
- Web login-cracking tools, 281
- Web pages, defaced, 25
- Web servers
  - configuration settings, 285
  - identifying software versions, 48
  - testing configurations, 32
  - testing directory security, 283–284
- Web site privacy policies, information from, 45
- Web sites
  - antivirus software testing, 250
  - banner-grabbing software, 264
  - behavioral-analysis tools, 252
  - Cantenna kits, 150
  - decompression tools, 89
  - defaced Web pages, 25
  - default system passwords, 100
  - dictionary word lists, 88
  - ElcomSoft password-cracking utilities, 95
  - FedCIRC Incident Handling site, 244–245
  - fingerprint-changing tools, 294
  - firewall testers, 133
  - hacker community sites, 26
  - hacker magazines, 27
  - hardening practices information, 101, 264
  - ICAT Metabase list of password vulnerabilities, 82
  - INM traffic-detection tools, 275–276
  - keystroke logging tools, 97
  - Lance Spitzner's, 27
  - Linux security tools, 195, 199, 213
  - lock-down programs, 98
  - logging resources, 312–313
  - MAC-spoofing software, 142–143
  - malware-protection software, 254
  - NetWare management programs, 223
  - password-cracking tools, 85, 282
  - password-resetting program, 101
  - patch-automation applications, 307
  - port-mapping software, 246
  - port-number assignment listings, 48
  - Pringles-can design antenna, 150
  - rconsole attack information, 223
  - Security Accounts Manager (SAM)
    - database, 87
    - security training vendors, 315
    - service-disabling utilities, 202–203
  - SMTP relay information, 266–267, 269
  - SNMP scanners, 129
  - for understanding specific malware attacks, 245
  - for understanding system vulnerabilities, 49–50
  - war-dialing programs, 109
  - Web-application security tools, 280, 295
  - Web-crawling tools, 284
  - Whois (lookup) sites, 43–44
  - Windows security tools, 169–171, 181, 183, 190
  - Wired Equivalent Privacy encryption
    - cracking tools, 156
  - wireless hardware information, 150
  - wireless LAN security tools, 148–149, 151
- Web-application attacks
  - assessment tools, 17
  - automated scans, 292–293
  - cracking Web logins, 280–283
  - directory traversals, 283–285
  - input attacks, 285–289
  - types of, 279–280
  - URL filter bypasses, 290–292
    - using default scripts, 289–290
- Web-crawling utilities, 42
- WebInspect (SPI Dynamics) Web-application-evaluation tool, 280, 17, 292–293
- Web-server security features, 294
- WebTrust security seal, 30
- Wellenreiter wireless LAN security tool, 148
- WEP (Wired Equivalent Privacy)
  - encryption, 155–156, 161
- WepAttack wireless LAN-cracking tool, 156
- WEPCrack password-cracking tool, 156
- WhatIsMyIP.com Web site, 46
- Whister Web-application-assessment tool, 17

- white-hat hackers, 10. *See also* ethical hacking
  - Whois lookup tools, 43–44, 109
  - Wi-Fi Protected Access (WPA), 157
  - WiFiMaps Web site, 151
  - WiGLE wireless LAN database Web site, 151–152
  - WildPackets EtherPeek network-analysis program, 120–121
  - Wiles, Jack (The Training Co.), 71
  - Win Sniffer password capture software, 85
  - Windows (Microsoft) systems
    - cracking passwords on, 89–90
    - e-mail packet sniffers, 270
    - lock-down programs, 98
    - MAC-address spoofing, 142–143
    - malware infection detectors, 245–247
    - NetBIOS attacks, 174–177
    - network-analyzer attacks, 134–135, 140
    - null session attacks, 179–186
    - operating system vulnerabilities, 101–102, 167–168
    - password resetting program, 101
    - password vulnerabilities, 81, 87
    - ping utilities, 46
    - remote procedure call enumeration, 177–178
    - rootkits for, 240–241
    - security tools, 148–149, 168–171
    - share permission vulnerabilities, 187–189
    - system scanning process, 171–174
  - Windows Registry
    - blocking access, 184–185
    - examining for malware attacks, 247
  - Windows Resource Kit security tools, 170
  - Windows Script Host (WSH) malware attacks, 242
  - Windows Server 2003
    - enhanced security, 179, 184
    - share permissions, 187
  - Windows System Information tool, 111
  - Windows Task Manager, 246
  - Windows 2000/NT
    - null connection attacks, 185–186
    - security-testing tools, 171
    - share permissions, 186–187
    - unprotected shares, 188–189
  - Windows Update security patches, 188–190, 308
  - Windows workstation security
    - enhancements, 188
  - Windows XP security enhancements, 188
  - Winfo NT security-testing tool, 171, 181–182
  - Winkler, Ira (social engineer, author), 57
  - WinNuke DoS attacks, 144
  - Wired Equivalent Privacy (WEP)
    - encryption, 155–156, 161
  - wireless access points, testing, 32
  - wireless LANs (WLANs)
    - ad-hoc mode, 153
    - configuration vulnerabilities, 162–163
    - hacking tools and hardware, 148–158
    - physical-security attacks, 160
    - reconnaissance missions, 151–154
    - types of, 154–155
    - unauthorized access points, 158–160
    - unencrypted traffic, 155–157
    - vulnerabilities, 13, 147–148
  - Wired Equivalent Privacy encryption, 155–156
    - wireless workstations, 161–162
  - working ethically, 14
  - workstations
    - testing, 32
    - wireless, 161–162
  - worms, 94, 240
  - Wotsit's Format Web site, 245
  - WPA (Wi-Fi Protected Access), 157
  - WSH (Windows Script Host) malware attacks, 242
- X •
- xinetd configuration tool, replacing, 203
  - XSS (cross-site scripting) Web-application attacks, 288
- Y •
- Yahoo! Finance Web site, 42–43, 60
- Z •
- zombie computers, 28, 65

