

# Index

## • Numerics •

802.11 encryption protocols, 161–162  
802.11i encryption protocols, 165

## • A •

Absinthe, 363  
Abuse.net SMTP relay checker, 355  
access control, 217  
access points (APs)  
  MAC address of, 156  
  network vulnerabilities and, 152  
  rogue wireless devices, 165  
account enumeration attacks, 257–260  
account lockout, 112  
Active Directory database, 93  
Acunetix Web Vulnerability Scanner, 278,  
  288, 290, 296, 363  
Address Resolution Protocol (ARP), 140  
Advanced Access Password Recovery,  
  307, 352  
Advanced Archive Password Recovery,  
  102–103, 358  
Advanced Encryption Standard (AES),  
  162, 165  
Advanced SQL Password Recovery,  
  304, 306, 352  
AES (Advanced Encryption Standard),  
  162, 165  
AfriNIC, 50, 353  
Aircrack, 154, 161, 365  
AirMagnet Handheld Analyzer, 155  
AirMagnet WiFi Analyzer, 154, 166,  
  168–169, 365  
Airodump, 161  
AirSnort, 365  
Akin, Thomas (Southeast Cybercrime  
  Institute), 251  
*allintitle* Google operator, 282  
Amap, 215  
Andrews, Chip (Special Ops Security),  
  305–306  
anonymity, 34  
Apache Web server, 209  
APNIC, 51, 353  
AppDetectivePro, 308, 352  
application attacks, 16  
Arcsight Logger, 331, 355  
ARIN, 51, 353  
ARP (Address Resolution Protocol), 140  
ARP spoofing. *See also* network  
  infrastructure attacks  
  countermeasures, 144  
  defined, 140  
  how it works, 140–141  
  using Cain & Abel, 141–143  
Arpwatch, 144, 356  
Asleap, 164, 365  
Asterisk, 68  
Athena FirewallGrader, 133  
attack tree analysis, 39  
attacks  
  account enumeration attacks, 257–259  
  application attacks, 16  
  ARP spoofing, 140–143  
  banner grabbing, 130–131, 255–257  
  brute-force attacks, 95–96  
  buffer overflows, 283–284  
  code injection, 287–289  
  database attacks, 303–309  
  denial of service attacks, 145–147  
  dictionary attacks, 94–95  
  directory reversal attacks, 280–283  
  dumpster diving, 15  
  e-mail attacks, 252–267  
  e-mail bombs, 252–255  
  e-mail header disclosures, 263  
  e-mail traffic capture, 264  
  encrypted traffic, 160–165  
  hidden field manipulation, 285–286  
  input filtering attacks, 283–291  
  instant messaging, 267–270, 287–289  
  keystroke logging, 103–104

- MAC address spoofing, 143–144, 170–175
  - malware, 264
  - network infrastructure attacks, 15
  - nontechnical, 14–15
  - operating system attacks, 15
  - password cracking, 89–109
  - physical, 15
  - rainbow attacks, 96
  - rconsole attacks, 233–236
  - reasons for, 31
  - SMTP attacks, 257–265
  - SMTP relay attacks, 260–262
  - social engineering, 15
  - SQL injection, 287–289
  - storage system attacks, 309–313
  - styles of, 32
  - timing, 33
  - URL manipulation, 285
  - voice over IP, 270–276
  - vulnerability and, 33
  - auditing, security, 12
  - Auditory Professional, 269
  - authenticated scans, 205–206
  - authorization, 18
  - automated assessment, 56
  - Awareity MOAT, 362
- **B** •
- background checks, 49
  - BackTrack
    - capturing e-mail traffic address with, 258
    - firewall rulebase testing with, 133
    - Linux security testing with, 154, 209
    - network vulnerability testing with, 148
    - Web site, 355
  - banner grabbing. *See also* network infrastructure attacks
    - countermeasures, 131
    - defined, 130
    - overview, 130
    - telnet, 130–131
  - banners, 130, 255–257
  - Bastille Linux Hardening Program, 361
  - Beaver, Kevin (*Security On Wheels*), 360
  - believability in social engineering, 69
  - Berkeley Software Distribution (BSD)
    - r-commands, 218–220
  - BigFix Patch Management, 227, 325, 359
  - Bing search engine, 48, 353
  - BIOS passwords, 107, 358
  - BitLocker, 198
  - black hat hackers, 10
  - BlackKnightList, 95, 296
  - blank password, 101–102
  - Blast tool, 146, 356
  - Blaster worm, 181
  - blind assessment, 42, 47
  - blind SQL injection, 287
  - Bloover, 160
  - Bluejacking, 160, 351
  - BlueScanner, 160, 351
  - Bluesnarfer, 160, 351
  - BlueSniper rifle, 160
  - Bluetooth, 160, 351
  - BorderManager resources, 356
  - broadcast mode, 140
  - brute-force attacks, 95–96
  - Brutus
    - brute-force testing with, 296
    - password cracking with, 93
    - POP3 password cracking with, 265
    - Web site, 355, 358, 363
  - BTScanner for XP, 160, 351
  - buffer overflows, 223–224, 283–284
  - building infrastructure, physical security, 78–79
  - business phones, 68
  - buy-in, management, 339
    - ally and sponsor, 337
    - benefits of ethical hacking, 339
    - establishing credibility, 340
    - flexibility and adaptability, 341
    - getting involved in business, 339–340
    - practical advice, 337
    - speaking on management’s level, 340
    - value in efforts, 340–341
    - what-if-scenarios, 338
- **C** •
- Cain & Abel. *See also* software and testing tools
    - ARP spoofing with, 141–143

- capturing and recording voice traffic
    - with, 274–276
  - capturing e-mail traffic with, 264
  - cracking Oracle password hashes
    - with, 307
  - network analysis with, 105, 121, 135
  - password cracking with, 92, 304
  - Web site, 356, 358, 362
- Camasia Studio, 41
- Canary Wireless, 155
- cantenna, 155, 365
- CAPTCHA, 255, 297
- Car Whisperer, 160, 351
- Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) protocol, 175
- case studies
  - database hacking, 305–306
  - e-mail attacks, 251
  - messaging-system attacks, 251
  - network infrastructure attacks, 118
  - password cracking, 87
  - physical security, 77
  - social engineering, 63
  - Web application attacks, 279
  - wireless network attack, 153
- CCTV security camera, 27
- Center for Internet Security, 113, 321, 326, 361
- certifications, 352
- Certified Ethical Hacker (CEH), 12
- .cgi extension, 299
- CHAP Password Tester, 310, 361
- Chappell, Laura, 118
- Character Generator pot (NetWare), 232
- chargen, 123
- Checkmarx, 300, 361
- CheckPoint, 300
- chkconfig, 217
- chknul (password-cracking software), 92
- ChoicePoint, 49
- Chronology of Data Breaches, 338, 363
- CIFShareBF, 310, 361
- CipherTrust IronMail, 255
- Cisco Global Exploiter, 148–149
- civil liberties, 32
- Clear Channel Assessment attack, 175–176
- cleartext packets, 242
- client notification, 37
- closed-circuit television (CCTV), 81
- code injection, 287–289
- Common Vulnerabilities and Exposures, 55, 363
- CommView
  - denial of service testing with, 146
  - network analysis with, 106, 135
  - Web site, 357, 362
- CommView for Wi-Fi, 166–167, 365
- Computer Underground Digest, 354
- contingency plan, 18
- COPS, 223
- copy rooms, 81
- Counter Mode with Cipher Block Chaining Message Authentication Code (CCMP), 162
- countermeasures
  - account enumeration attacks, 257–260
  - ARP poisoning, 144
  - ARP spoofing, 144
  - banner attacks, 257
  - banner grabbing, 131
  - buffer overflows, 223–224
  - database attacks, 308–309
  - default configuration settings exploits, 177–178
  - default script attacks, 294
  - denial of service attacks, 146–147, 176
  - directory reversal attacks, 282–283
  - e-mail attachment attacks, 253
  - e-mail attacks, 266–267
  - e-mail bombs, 253–254
  - e-mail connection attacks, 253
  - e-mail header disclosures, 263
  - encrypted traffic attacks, 164–165
  - file permission attacks, 222–223
  - firewalls, 133–134
  - hosts.equiv file attacks, 219–220
  - input filtering attacks, 291
  - instant messaging vulnerabilities, 268–269
  - MAC address spoofing, 144, 175
  - missing patch exploitation, 205
  - NetBIOS, 190
  - Netware intruders, 238
  - NetWare Loadable Module, 241
  - network analyzers, 139–140
  - network infrastructure attacks, 135
  - NFS attacks, 221
  - null sessions, 194–195
  - packet capture, 242

- countermeasures (*continued*)
  - password cracking, 109–114
  - physical security attacks, 224–225
  - physical security problems, 176–177
  - port scanning, 127–128
  - .rhost file attacks, 219–220
  - rogue NLM attack, 241
  - rogue wireless devices, 170
  - SMTP relay attacks, 263
  - SNMP scanning, 130
  - social engineering, 72–74
  - storage system attacks, 313
  - system scans, 212
  - unnneeded services, 216–217
  - unsecured login mechanisms, 297
  - Voice over IP, 276
  - vulnerable wireless workstations, 177–178
  - wireless network attacks, 158–159
- Counterpane, 331
- Crack, 358
- crackers, 10
- cracking tools, 20
- cracklib, 114
- crashing system during tests, 17
- criminal hackers, 10, 28
- cross-site scripting (XSS), 290
- CWE/SANS Top 25 Most Dangerous Programming Errors, 363
- CxAudit, 300
- CxDeveloper, 300–301
- cyberterrorists, 29

## • D •

- daemons, 209
- Data Thief tool, 305
- database attacks. *See also* storage system attacks
  - best practices for minimizing risks, 308–309
  - case study, 305–306
  - finding databases on network, 304–306
  - overview, 303
  - password cracking, 306–307
  - scanning for vulnerabilities, 307–308
  - testing tools, 303–304
  - tools, 352

- daytime, 123
- .db file, 311
- .dbf file, 311
- Debian Linux Security Alerts, 359
- Debian Package System, 227
- Deep Freeze, 104, 361
- defaced Web pages, 31, 364
- default configuration settings, 178
- default script attacks, 292–293
- deliverables, 19
- denial of service (DoS) attacks.
  - See also* network infrastructure attacks
  - countermeasures, 146–147
  - defined, 145
  - distributed, 145
  - Ping of Death, 145
  - Queensland, 175–176
  - SYN floods, 145
  - testing, 146
  - WinNuke, 145
- dictionary attacks, 94–95
- dictionary files, 358
- Digital Hotspotter, 155, 168, 365
- directional antenna, 155
- directory reversal attacks
  - countermeasures, 282–283
  - crawlers, 280–281
  - defined, 280
  - Google, 281–282
- distributed denial of service (DDoS) attacks, 145
- D-Link DWL-650 wireless NIC, 175
- DNS (Domain Name System), 123
- DNSstuff.com, 50, 353
- dnstools.com, 353
- .doc file, 311
- .docx file, 311
- Dogwood Management Partners Security Posters, 362
- Domain Name System (DNS), 123
- doors, 79–80
- Draper, John (Captain Crunch), 27
- drop ceilings, 80
- dsniff program, 140, 357
- dsrepair (NetWare Loadable Module), 239
- DumpSec utility, 55, 192, 364
- dumpster diving, 15, 67

## • E •

- eBlaster (keystroke-logging software), 104
- echo, 123
- Echo port (NetWare), 232
- Ecora Patch Manager, 326, 359
- eDirectory, 229
- Effective File Search, 310, 361
- EICAR Anti-Virus test file, 356
- EICAR test string, 265
- Elcomsoft Advanced Archive Password Recovery, 102–103
- Elcomsoft Distributed Password Recovery, 92, 306, 352, 358
- Elcomsoft System Recovery, 108–109, 359
- Elcomsoft Wireless Security Auditor (EWSA), 154, 162–163, 365
- e-mail attacks. *See also* messaging-system attacks
  - banners, 255–257
  - case study, 251
  - e-mail bombs, 252–255
  - guidelines against, 266–267
  - overview, 16
  - SMTP attacks, 257–265
  - software solutions against, 266
- e-mail bombs. *See also* messaging-system attacks
  - automated security controls against, 254–255
  - bandwidth blocking, 253–254
  - countermeasures against connection attacks, 253–254
  - perimeter protection, 255
  - storage overload, 253
  - using attachments, 252–253
  - using connections, 253–254
  - using floods of e-mails, 253
- e-mail firewalls, 255
- e-mail header disclosures, 263–264
- e-mail security testing zone, 265
- e-mail servers, 55
- e-mail traffic, capturing, 264
- EMail Verify, 257–258
- encrypted traffic, 160–164
- encrypted traffic attacks. *See also* wireless network attacks
  - countermeasures, 164–165
  - encryption protocols, 161–162
  - overview, 161–162
  - tools, 162–164
- enumeration utility, 55, 185–186
- error-based SQL injection, 287
- errors and omission insurance, 35
- Essential NetTools, 120, 357
- ethical hackers, 10
- ethical hacking
  - assessing vulnerabilities, 55–57
  - attack tree analysis, 39
  - vs. auditing, 12
  - automating, 329–330
  - avoiding system crashes in, 17
  - blind assessment in, 47
  - certification, 12
  - compliance and regulatory concerns, 12–13
  - defined, 11
  - determining systems to hack, 37–40
  - evaluating results in, 22–23
  - executing plan in, 22
  - footprinting, 47–52
  - formulating plan, 18–19
  - gathering public information, 48–49
  - goals, 13–14, 36–37
  - insurance, 35
  - logging information in, 46
  - mistakes in, 347–350
  - network mapping, 50–52
  - outsourcing, 332–333
  - penetrating system, 57–58
  - performing, 45–47
  - policy considerations, 12
  - reasons for effectiveness of, 343–345
  - respecting privacy in, 17
  - scanning systems, 52–53
  - similarity to beta testing, 45
  - similarity to malicious attacks, 46
  - testing standards, 40–43
  - tools, 20–21, 44
  - working ethically, 16–17
- ettercap utility, 135, 357
- Event ID 4226 Patcher tool, 185
- event logging system, 331
- EventsManager, 331
- exploit tools, 352

EXPN command, 257, 259  
external attackers, 10

## • F •

Facebook, 145  
Fedora Linux, 154  
File Extension Source, The, 353  
file permission attacks, 221–223  
file sharing, 267–268  
File Transfer Protocol (FTP), 123, 209, 213  
FileLocator Pro, 309, 310, 312, 361  
filetype:file-extension hostname: query (Google), 281  
findstr, 104  
finger, 123  
Finnigan, Pete, 352  
fire detection and suppression systems, 79  
Firefox, configuring for Web proxy, 284  
Firefox Web Developer, 278, 284, 298, 364  
Firewalk, 133, 357  
firewalls  
  countermeasures against attacks, 133–134  
  e-mail, 255  
  testing, 131–134  
  Web security, 299–300  
Flash files, 48–49  
Fluke WiFi Analyzer, 154  
footprinting. *See also* ethical hacking  
  gathering public information, 47–49  
  overview, 47  
  Web crawling, 49  
  Web search, 48  
Fortify Software, 361  
Fortres program 101, 104, 361  
Foundstone, 298, 364  
fping, 52  
FreeZip, 97, 356  
freshmeat.net, 209  
FTP (File Transfer Protocol), 123, 209, 213  
FTP control, 123  
fully qualified domain names (FQDNs), 51

## • G •

Getif utility, 120, 128, 232, 357  
GFI e-mail security test, 356

GFI EventsManager, 355  
GFI LANguard. *See also* software and testing tools  
  authenticated scans with, 206  
  Linux system testing with, 208  
  NetWare vulnerability testing with, 230, 233  
  patch automation with, 326  
  share finder, 197  
  storage system testing with, 309  
  system scanning with, 186, 210–212  
  vulnerability assessment with, 121  
  Web site, 357, 359, 361, 364  
  Windows system testing with, 184  
goals in ethical hacking, 36–37  
Goog Mail Enum, 258, 260  
Google, 20, 48, 67, 281–282, 353  
Google Desktop, 361  
Google Groups, 51, 282  
Google Hacking Database (GHDB), 282, 364  
Google Hacking for Penetration Testers (Long), 282  
government domains, 353  
GrabiQNs, 310, 361  
Gramm-Leach-Bliley Act (GLBA), 13, 354  
Greenidea Visible Statement, 362  
grep, 104  
GroupWide (NetWare), 232

## • H •

hackers  
  anonymity, 34  
  behavior of, 26  
  black hat, 10  
  categories of, 28  
  criminal hackers, 28  
  cyberterrorists, 29  
  defined, 10  
  ethical, 10  
  hackers for hire, 29  
  hacktivists, 29  
  mindset of, 27  
  motivations of, 25–26, 29–31  
  online resources, 354  
  reformed, 333  
  script kiddies, 26, 28

- security researchers, 28
  - stereotypical view of, 25–26
  - white hat, 10
  - Hackin9*, 33, 354
  - hacking
    - civil liberties and, 32
    - planning and performing, 32–33
    - reasons for, 29–31
    - vulnerabilities in security and, 33
  - Hacking Wireless Networks For Dummies* (Davis), 162, 166, 321
  - hacktivists, 29
  - Hacme Tools, 298, 364
  - hardening, 326–327, 361–362
  - Health Information Technology for Economic and Clinical Health (HITECH), 354
  - Health Insurance Portability and Accountability Act (HIPAA), 12–13, 354
  - hidden field manipulation, 285–286
  - high-impact vulnerabilities, 320
  - Homebrew WiFi antenna, 365
  - Honeypots: Tracking Hackers, 354
  - Hoover’s business information, 353
  - hosting providers, notifying, 41
  - hosts, scanning, 52
  - `hosts.equiv` file attacks, 218–220
  - HTTP (Hypertext Transfer Protocol), 123
  - HTTP Get requests, 292
  - HTTP POST requests, 292
  - HTTP proxy, 123
  - HTTPS (HTTP over SSL), 123
  - HTTrack Website Copier, 49, 278, 280–281, 364
  - HyperTerminal, 261
  - Hypertext Transfer Protocol (HTTP), 16, 123
- 1 •**
- ICMP (Internet Control Message Protocol), 123–124
  - Identity Finder, 309, 312–313, 361
  - Identity Finder Pro, 104
  - IKE (Internet Key Exchange), 148–149
  - IKERack, 357
  - Imperva, 362
  - `inetd.conf`, 216–217
  - inference, 90–91
  - information-gathering
    - overview, 47
    - port scanning, 53–54
    - system scans, 52–53, 209–212
    - Web crawling, 49
    - Web search, 48–49
    - Web sites, 49
  - InGuardians, Inc., 153
  - input filtering attacks. *See also* Web application attacks
    - buffer overflows, 283–284
    - code injection, 287–289
    - countermeasures, 291
    - cross-site scripting, 290
    - hidden field manipulation, 285–286
    - overview, 283
    - SQL injection, 287–289
    - URL manipulation, 285
  - (*IN*)*SECURE* Magazine, 33
  - instant messaging
    - countermeasures against vulnerabilities, 268–269
    - detecting traffic, 269
    - log files, 268
    - overview, 267
    - sharing files in, 267–268
    - system configuration, 269–270
    - user behavior, 269
    - vulnerabilities, 267–268
  - insurance, 35
  - Internet Control Message Protocol (ICMP), 123–124
  - Internet Key Exchange (IKE), 148–149
  - Internet Security Advisors Group, 62
  - Internet service providers (ISP), notifying, 41
  - Internet services, 209
  - intruder lockout, 112
  - intrusion detection, 237–238
  - intrusion prevention system, evading, 27
  - inurl* Google operator, 282
  - Invisible KeyLogger Stealth, 104, 354
  - IP address, scanning, 52
  - IP Personality, 299
  - IP spoofing, 147

## • J •

JavaScript, 290  
 John the Ripper  
   cracking Unix passwords with, 98  
   cracking Windows passwords with, 96–98  
   overview, 92  
   Web site, 359  
 Johnson, Craig, 356  
 JRB Software, 240, 356  
 Juniper Networks, 300, 313

## • K •

Karalon, 132  
 Kerberos, 91  
 KeyGhost, 104, 354  
 keypads, programmable, 81  
 keys, 81  
 keystroke logging, 103–104, 354  
 KisMAC, 161, 365  
 Kismet, 154, 166  
 KLC Consulting, 173  
 Klockwork, 300, 361  
 Knoppix Linux, 108, 154, 355  
 knowledge assessment, 42  
 Korean National Police Agency, 29

## • L •

L0phtcrack, 99  
 LACNIC, 51, 353  
 LANguard. *See also* software and testing tools  
   authenticated scans with, 206  
   Linux system testing with, 208  
   NetWare vulnerability testing with, 230, 233  
   patch automation with, 326  
   share finder, 197  
   storage system testing with, 309  
   system scanning with, 186, 210–212  
   vulnerability assessment with, 121  
   Web site, 357, 359, 361, 364  
   Windows system testing with, 184

laptops, locking, 84  
 laws and regulations, 354  
 LEAP protocol, 164  
 likability in social engineering, 69  
 link Google operator, 282  
 LinkedIn, 20  
 Linux Administrator's Security Guide., 362  
 Linux Kernel Updates, 359  
 Linux operating system  
   attacks, 15  
   distribution updates, 227  
   multiplatform update managers, 227  
   overview, 207–208  
   password protection in, 114  
   password storage location in, 94  
   patching, 227  
   reasons for popularity of, 207  
   unneeded services, 213–218  
 Linux Security Auditing Tool (LSAT), 209  
 Linux systems. *See also* Windows systems  
   buffer overflows, 223–224  
   file permission attacks, 221–223  
   general security tests, 225–226  
   hosts.equiv file attacks, 218–220  
   multiplatform update managers, 227  
   NFS attacks, 220–221  
   overview, 207  
   patching, 226  
   physical security attacks, 224–225  
   .rhosts file attacks, 218–220  
   security tools, 208–209  
   system scanning, 209–212  
   vulnerabilities, 208  
   websites, 355  
 live toolkits, 355  
 location of testing, 43  
 lockdown programs, 104  
 log analysis, 355  
 LogAnalysis.org, 355  
 Logger, 331  
 LoveBug worm, 72  
 low-impact vulnerabilities, 320  
 lsof, 215  
 Lumension Patch and Remediation, 227, 359

• **M** •

M+Guardian, 255  
 MAC (Media Access Control), 140, 170  
 MAC address, 156  
 MAC address spoofing. *See also* wireless network attacks  
   countermeasures, 144, 175  
   overview, 170–171  
   steps in, 170–174  
   Unix-based systems, 143  
   Windows systems, 143–144  
 MAC address vendor lookup, 357  
 MAC Changer, 173, 357  
 MafiaBoy (hacker), 145  
 magazines, 33  
 mail rooms, 81  
 Mailsnarf, 264, 356  
 malicious internal users, 10  
 malicious users  
   defined, 10  
   monitoring, 330–331  
 malware, 264–266  
 managed security services provider (MSSP), 331  
 manual assessment, 56  
 MD5 passwords, 114  
 Media Access Control (MAC), 140, 170  
 medium-impact vulnerabilities, 320  
 Message Architect, 255  
 messaging-system attacks  
   case study, 251  
   e-mail attacks, 252–267  
   instant messaging, 267–270  
   testing tools, 355–356  
   voice over IP, 270–276  
   vulnerabilities, 249–250  
   Web sites, 355–356  
 Metasploit, 58, 184, 199–205, 265, 352  
 Microsoft Access database files, 307  
 Microsoft Baseline Security Analyzer (MBSA), 183, 206, 326, 365  
 Microsoft Exchange, 256  
 Microsoft IIS server, 299  
 Microsoft PPTP VPN, 123  
 Microsoft SQL Monitor, 123  
 Microsoft SQL Server, 123  
 Microsoft SQL Server Management Studio Express, 352

Microsoft TechNet Security Center, 360  
 Microsoft Update, 326  
 military domains, 353  
 Milw0rm, 352  
 mirroring, 278  
 missing patch exploitation  
   countermeasures, 205  
   overview, 198  
   using Metasploit, 199–205  
 mistakes in ethical hacking, 350  
 Mitnick, Kevin, 27  
 monitor mode, 137  
 multiplatform update managers, 227

• **N** •

NAP (Network Access Protection), 198  
 NASanon, 310, 361  
 National Institute of Standards and Technology (NIST), 88, 326  
 National Vulnerability Database, 88, 213, 321  
 nbstat, 183, 188–189  
 Nessus, 121, 209, 357  
 net view command, 192  
 NetBIOS (Network Basic Input/Output System)  
   countermeasures, 190  
   hacks, 188  
   overview, 187  
   shares, 189–190  
   unauthenticated enumeration, 188–189  
   vulnerable ports, 188  
 NetBIOS Auditing Tool, 359  
 NetBios over TCP/IP, 123  
 Netcat, 132, 357  
 Netcraft, 54, 353  
 Netfilter/iptables, 357  
 NetResident, 134, 264, 268, 357  
 NetScanTools Pro  
   denial of service testing with, 146  
   Linux system testing with, 212  
   network analysis with, 120  
   port scanning with, 126–127  
   system scanning with, 52  
   Web site, 357  
 NetScreen, 300, 313  
 NetServerMon, 356

- netstat, 183, 215
- NetStumbler, 154, 157–158, 166–167, 365
- NetUsers, 193
- NetWare Administrator, 244
- NetWare Core Protocol, 232
- NetWare Loadable Module (NLM)
  - admin utilities, 240
  - countermeasures, 241
  - documentation, 241
  - dsrepair, 239
  - modules command, 238–239
  - overview, 234
  - setpwd password reset tool, 238
  - tcpcon, 239–240
  - unauthenticated logins, 241
- network
  - countermeasures, 84
  - Internet Key Exchange weaknesses, 148
  - physical attacks, 82–83
  - unsecured interfaces, 147–148
  - vulnerabilities, 83, 147–149
- Network Access Protection (NAP), 198
- network analyzers, 53
  - Cain & Abel, 135
  - CommView, 135
  - configuring, 137
  - countermeasures, 139–140
  - defined, 134
  - detecting, 140
  - ettercap, 135
  - functions of, 134
  - information obtained from, 134, 135–137
  - monitor mode, 137
  - OmniPeek, 135
  - port scanning with, 105–106
  - programs, 120–121
  - requirements, 135
  - Web sites, 356–358
  - Wireshark, 135
- Network Associates, 134
- network browsing, UDP ports for, 188
- Network File System (NFS), 220–221
- network infrastructure attacks
  - analyzers, 120–121
    - ARP spoofing, 140–143
    - banner grabbing, 130–131
    - case study, 118
    - defenses, 149–150
    - denial of service, 145–147
    - firewall rules, 131–134
    - MAC address spoofing, 143–144
  - network analyzers, 134–140
  - overview, 15, 117
  - port scanning, 122–128
  - scanners, 120–121
  - SNMP scanning, 128–130
  - vulnerabilities, 119
  - vulnerability assessment tools, 121
- network interface card (NIC), 132
- network mapping
  - Google Groups, 51
  - overview, 50
  - privacy policies, 51–52
  - Whois lookup, 50
- Network Security Bible* (Cole), 117
- Network Security For Dummies* (Cobb), 113, 257, 323, 326
- Network Security Toolkit, 154, 355
- Network users, 365
- NFS (Network File System), 220–221
- NFS attacks, 220–221
- NGSSquirrel, 307, 352, 364
- NIC (network interface card), 132
- Nigerian 419* e-mail fraud, 72
- nipper, 133
- NIST Guide to Enterprise Password Management, 359
- NIST National Vulnerability Database, 55
- NIST SP800-58 document, 363
- NIST Special Publication 800-48, 351
- Nmap. *See also* software and testing tools
  - command-line options, 124
  - Connect scan, 126
  - FIN Stealth scan, 126
  - Linux system testing with, 208, 214
  - Null scan, 126
  - ping sweeping with, 123–124
  - port scanning with, 53, 120
  - scanning Linux system with, 212
  - SYN Stealth scan, 126
  - system scanning with, 187
  - UDP scan, 126
  - Web site, 357
  - Xmas Tree scan, 126
- NmapWin, 55, 120, 357
- NoLMHash registry key, 113
- nontechnical attacks, 14–15

- North American Electric Reliability Corporation (NERC), 13
- Novell ConsoleOne utility, 243, 245
- Novell NetMail, 256
- Novell Netware
  - admin account, renaming, 243
  - auditing, 246
  - bindery contexts, removing, 245–246
  - cleartext packets, 242
  - eDirectory browsing, disabling, 244–245
  - intruder detection, 237–238
  - overview, 229
  - patching, 246
  - port scanning, 231–233
  - rconsole attacks, 233–236
  - security risks, minimizing, 243–246
  - security tools, 230
  - server access methods, 231
  - server-console access, 236
  - servers, 230
  - TCP/IP parameters, 246
  - testing for rogue NLMs, 238–241
  - testing tools, 356
  - vulnerabilities, 229–230
- Novell Patches and Security, 360
- npasswd, 114
- N-Stalker Web Application Security Scanner, 278, 293
- N-Stealth Web Application Security Scanner, 364
- NTAccess, 108, 359
- null password, 101–102
- null sessions
  - configuration and user information, 192–194
  - countermeasures, 194–195
  - disabling, 114
  - mapping, 191
  - net view command, 192
  - overview, 190
- 0 •
- Objectif Sécurité, 87
- OCTAVE methodology, 360
- Oechslin, Philippe, 87
- office layout and usage, physical security, 80–82
- Official Internet Protocol Standards, 117
- omnidirectional antenna, 155
- OmniPeek
  - finding hidden APs with, 166–167
  - network analysis with, 106, 135
  - port scanning with, 53
  - viewing encrypted wireless traffic with, 164
  - vulnerability assessment with, 121
  - Web site, 357, 363, 365
  - wireless network analysis with, 154
- Online Hacker Jargon File, 354
- online resources
  - Bluetooth, 351
  - certifications, 352
  - database tools, 352
  - exploit tools, 352
  - general research tools, 353
  - hacking, 354
  - keyloggers, 354
  - laws and regulations, 354
  - Linux tools, 355
  - live toolkits, 355
  - log analysis, 355
  - messaging-system testing tools, 355–356
  - NetWare, 356
  - network testing tools, 356–358
  - password cracking tool, 358–359
  - patch management, 359–360
  - security education, 360
  - security methods and models, 360
  - source code analysis, 361
  - storage testing tools, 361
  - system hardening, 361–362
  - user awareness and training, 362
  - Voice over IP, 362–363
  - vulnerability databases, 363
  - Web applications, 363–364
  - Windows, 364–365
  - wireless networks, 365–366
- open ports, scanning, 53–55
- Open Source Security Testing Methodology Manual, 58, 360
- OpenBSD, 15
- OPENROWSET command, 305
- OpenSSH, 210
- operating system attacks, 15
- operating system attacks, Linux
  - buffer overflows, 223–224
  - file permission attacks, 221–223

- operating system attacks, Linux (*continued*)
    - general security tests, 225–226
    - hosts.equiv file attacks, 218–220
    - multiplatform update managers, 227
    - NFS attacks, 220–221
    - overview, 207
    - patching, 226
    - physical security attacks, 224–225
    - .rhosts file attacks, 218–220
    - security tools, 208–209
    - system scanning, 209–212
    - vulnerabilities, 208
  - operating system attacks, Novell Netware
    - admin account, renaming, 243
    - auditing, 246
    - bindery contexts, removing, 245–246
    - cleartext packets, 242
    - eDirectory browsing, disabling, 244–245
    - intruder detection, 237–238
    - overview, 229
    - patching, 246
    - port scanning, 231–233
    - rconsole attacks, 233–236
    - security risks, minimizing, 243–246
    - security tools, 230
    - server access methods, 231
    - server-console access, 236
    - servers, 230
    - TCP/IP parameters, 246
    - testing for rogue NLMs, 238–241
    - testing tools, 356
    - vulnerabilities, 229–230
  - operating system attacks, Windows
    - authenticated scans, 205–206
    - missing patch exploitation, 198–205
    - NetBIOS, 187–190
    - null sessions, 190–195
    - overview, 181–182
    - scanning, 185–187
    - security tools, 182–184
    - share permissions, 196–198
    - testing tools, 364–365
    - vulnerabilities, 182
  - operating systems, securing, 113–114
  - ophcrack (password-cracking software), 92, 96, 99–101, 359
  - Ophcrack Live, 81
  - organizational password vulnerabilities, 86–88
  - Orinoco card, 154–155
  - Ounce Labs, 300, 361
  - outsourcing, 332–333, 350
  - OWASP WebGoat Project, 298, 360
- p ●
- packet signing, 242
  - Pandora, 92, 359
  - Pandora NetWare, 242, 356
  - Paros Proxy, 286, 364
  - passfilt.dll, 114
  - passwd+, 114
  - password cracking
    - blank, 101–102
    - brute-force attacks, 95–96
    - case study, 87
    - checking for null/blank passwords in NetWare, 101–102
    - countermeasures, 109–112
    - database hacking, 306–307
    - dictionary attacks, 94–95
    - inference, 90–91
    - keystroke logging, 103–104
    - with network analyzer, 105–106
    - password-protected files, 102–103
    - password-reset programs, 108–109
    - rainbow attacks, 96
    - rainbow cracking, 99
    - shoulder surfing, 85, 90
    - social engineering, 89–90
    - software, 92–94
    - tools, 358–359
    - Unix passwords with John the Ripper, 98
    - weak authentication, 91
    - weak BIOS passwords, 107
    - weak password storage, 104–105
    - Web sites, 358–359
    - Windows password with ophcrack, 99–101
    - Windows passwords with pwdump3 and John the Ripper, 96–98
  - Password Management Guideline document, 96
  - Password Safe, 359
  - password-protected files, 102–103
  - password-reset programs, 108–109

- passwords. *See also* password cracking
  - divulging, 71
  - malicious users, 27
  - null, 101–102
  - overview, 85
  - policy considerations, 110–111
  - possible combinations, 99
  - storage locations by operating systems, 93–94
  - storing, 110
  - strong, 110–111
  - vulnerabilities, organizational, 86
  - vulnerabilities, technical, 88
  - weak storage, 104–105
- patches, security
  - automating, 325–326
  - for Linux systems, 224–225
  - managing, 325
  - for password hacking, 112
  - tools, 325–326
  - Web sites, 359–360
- Patent and Trademark Office, 353
- Payment Card Industry Data Security Standard (PCI DSS), 13, 132, 354
- pcAnywhere, 123
- PDF documents, 48–49
- PGP Whole Disk Encryption, 108, 362
- Philippines, hacking ring in, 29
- phishing. *See also* social engineering
  - dumpster diving, 67
  - overview, 66
  - phone systems, 68
  - in social engineering, 62
  - using the Internet, 67
- phone systems, 68
- PHRACK, 33, 354
- physical security
  - case study, 77
  - exploiting weakness in, 27
  - factors in, 76
  - overview, 75
  - tailgating, 77
  - technical security and, 77
  - vulnerabilities, 75
- physical security attacks
  - buildings, 78–79
  - Linux operating system, 224–225
  - network components and computers, 81–84
  - Novell Netware, 236
    - office layout and usage, 80–82
    - utilities, 79–80
    - wireless networks, 176–177
  - Ping of Death, 145
  - ping sweep, 123–124, 127–128
  - Point-to-Point Tunneling Protocol (PPTP), 164
  - POP3 (Post Office Protocol version 3), 123
  - Port 80 Software, 299, 364
  - port number listing, 357
  - port number lookup, 357
  - port scanners
    - in ethical hacking, 20
    - how it works, 124
    - NetScanTools Pro, 126–127
    - Nmap, 126
    - programs, 53
    - SuperScan, 125
  - port scanning
    - commonly hacked ports, 123
    - countermeasures, 127–128
    - information obtained from, 53–55, 124–125
    - Linux systems, 209–212
    - in network infrastructure attacks, 122
    - Novell Netware systems, 231–233
    - ping sweep, 123–124
    - tools, 53, 124–127
    - Windows systems, 185–186
  - ports, commonly hacked, 123
  - PortSentry, 213, 357
  - power failure, 79
  - power-protection equipment, 79
  - PPTP (Point-to-Point Tunneling Protocol), 164
  - pre-shared keys (PSKs), 162
  - Pretty Good Privacy (PGP), 22
  - Prism Test Utility, 175
  - privacy, respecting, 17
  - privacy policies, 51–52
  - Privacy Rights Clearinghouse, 338, 363
  - Proactive Password Auditor, 92, 95, 359
  - Proactive System Password Recovery, 92, 359
  - professional liability insurance, 35
  - Project RainbowCrack, 96
  - PromiscDetect, 106, 140, 357

promiscuous mode, 106, 134  
 pwdump3, 92, 96–98, 359  
 Pyn Logic, 362

## • Q •

QualysGuard. *See also* software and testing tools  
 database testing with, 304  
 denial of service testing with, 146  
 Linux system testing with, 209  
 storage system testing with, 309  
 vulnerability assessment with, 56–57, 121  
 Web site, 352, 357, 365  
 Windows system testing with, 184, 199  
 QualysGuard Suite, 56–57  
 Queensland DoS attack, 175–176  
 Quest Policy Authority, 269

## • R •

rainbow cracking, 87, 96, 99  
 Rainbow tables, 359  
 RainbowCrack, 92, 359  
 RC4 encryption algorithm, 161  
 Rcon program, 356  
 Real-time Transport Protocol (RTP), 272  
 reCAPTCHA, 297  
 recycling bins, 81  
 Red Hat Enterprise Linux, 220, 227  
 Red Hat Linux Security Advisories, 360  
 Red Hat Package Manager, 227  
 red team, 37, 77  
 reformed hackers, 333  
 regedit, 143  
*related* Google operator, 282  
 remote procedure calls, 123, 181  
 Remote tool, 230, 356  
 remote-administration software, 83  
 reports  
 action items, 321–322  
 methods, 320–322  
 organizing information, 317–319  
 prioritizing vulnerabilities in, 319–320  
 securing, 320  
 residential phone, 68  
 reverse social engineering, 70

.rhosts file attacks, 218–220  
 rich Internet applications (RIAs), 298  
 RIPE Network Coordination Centre, 51, 353  
 risks, 18  
 rogue network, 27  
 rogue wireless devices  
 AP characteristics of, 165–166  
 countermeasures, 170  
 detecting with WLAN analyzers, 165–168  
 overview, 165  
 root directory, 218  
 RPC/DCE for Microsoft networks, 123  
 RPM Package Manager, 227  
 .rtf file, 311  
 RTP (Real-time Transport Protocol), 272

## • S •

SANS, 113  
 scanners, 120–121  
 screens, locking, 84  
 script kiddies, 26, 28  
 ScriptLogic Patch Authority Ultimate, 326  
 search engines, 48, 67  
 SearchSecurity.com, 20  
 SeattleWireless Hardware Comparison page, 365  
 SEC filings, 67  
 SecureCRT, 261  
 SecureIIS, 300, 362  
 SecureWorks, 331  
 Securities and Exchange Commission, 353  
 SecurITree, 360  
 Security Accounts Manager (SAM)  
 database, 93, 97  
 security assessment tools, 44  
 security auditing, 12  
 security awareness, 333–334  
 security by obscurity, 299  
 security infrastructure, assessing, 327–328  
 Security Innovation, 300  
 security measures  
 account enumeration attacks, 257–260  
 ARP poisoning, 144  
 ARP spoofing, 144  
 assessing security infrastructure, 327–328  
 banner attacks, 257  
 banner grabbing, 131

- buffer overflows, 223–224
- database attacks, 308–309
- default configuration settings exploits, 177–178
- default script attacks, 294
- denial of service attacks, 146–147, 176
- directory reversal attacks, 282–283
- e-mail attachment attacks, 253
- e-mail attacks, 266–267
- e-mail bombs, 253–254
- e-mail connection attacks, 253
- e-mail header disclosures, 263
- encrypted traffic attacks, 164–165
- file permission attacks, 222–223
- firewalls, 133–134
- hosts.equiv file attacks, 219–220
- implementing, 323–324
- input filtering attacks, 291
- instant messaging vulnerabilities, 268–269
- MAC address spoofing, 144, 175
- missing patch exploitation, 205
- NetBIOS, 190
- Netware intruders, 238
- NetWare Loadable Module, 241
- network analyzers, 139–140
- network infrastructure attacks, 135
- NFS attacks, 221
- null sessions, 194–195
- packet capture, 242
- password cracking, 109–114
- patching, 324–326
- physical security attacks, 224–225
- physical security problems, 176–177
- port scanning, 127–128
  - .rhost file attacks, 219–220
- rogue NLM attack, 241
- rogue wireless devices, 170
- security awareness and training, 333–334
- SMTP relay attacks, 263
- SNMP scanning, 130
- social engineering, 72–74
- storage system attacks, 313
- system hardening, 326–327
- system scans, 212
- unnneeded services, 216–217
- unsecured login mechanisms, 297
- Voice over IP, 276
- vulnerable wireless workstations, 177–178
- wireless network attacks, 158–159
- Security On Wheels, 360
- security portals, 20
- Security Tools Distribution, 154, 355
- SecurityFocus.com, 20
- semidirectional antenna, 155
- sendmail server, 214
- Server Message Block (SMB), 188
- ServerDefender, 300, 362
- ServerMask, 299, 364
- service set identifier (SSID), 157–158
- Session Initiation Protocol (SIP), 272
- SetGID, 221–222
- setpwd password reset tool (NetWare Loadable Module), 238
- SetUID, 221–222
- share permissions
  - defaults, 196
  - overview, 196–198
  - testing, 197
  - Windows 2000/NT, 196
  - Windows XP, 196
- ShareEnum, 184
- Shavlik Technologoes NetChk, 325
- shoulder surfing, 85, 90
- shredders, 67
- Sima, Caleb (SPI Dynamics), 279
- Simple Mail Transfer Protocol (SMTP), 16, 123, 257
- Simple Network Management Protocol (SNMP), 123, 128–130
- SIP (Session Initiation Protocol), 272
- sipsak, 363
- SiteDigger, 364
- site:hostname keywords*: query (Google), 281
- SiVus, 272–274, 363
- Slackware, 154, 227
- Slackware Package Tool, 227
- SMAC, 143–144, 173, 357
- SMB (Server Message Block), 188
- SMTP (Simple Mail Transfer Protocol), 123, 257
- SMTP attacks
  - account enumeration, 257–260
  - e-mail header disclosures, 263–264
  - e-mail traffic capture, 264
  - malware, 264–266
  - relay, 260–263

- smtpscan, 256, 356
- Smurf, 160, 351
- SNARE, 357
- Sniffdet, 140, 358
- sniffers, 134
- SNMP (Simple Network Management Protocol), 123, 128–130
- SNMP scanning, 128–130
- SNMPUTIL, 128, 358
- social engineering
  - behaviors associated with, 69–70
  - believability in, 69
  - building trust in, 68–69
  - case study, 63
  - consequences of, 65
  - countermeasures, 72–74
  - deceptive practices in, 69–72
  - defined, 15
  - examples of, 61–62
  - false employees, 62
  - false support personnel, 62
  - false vendors, 62
  - likability in, 69
  - outsourcing, 64
  - overview, 61
  - password cracking, 89–90
  - phishing, 62, 66–68
  - policies, 72
  - reasons for using, 64–65
  - reverse, 70
  - user awareness and training, 73–74
- software and testing tools
  - Linux systems, 208–209
  - network analyzers, 120–121, 135
  - Novell Netware, 230
  - password cracking, 92–94
  - scanners, 120–121
  - selecting, 20–21, 44
  - storage systems, 309–310
  - vulnerability assessment, 121
  - Web applications, 278
  - Windows systems, 181–185
  - WLAN security tools, 154–155
- Software as a Service (SaaS), 331
- Software Engineering Institute, 360
- SonicWall, 300, 313
- source code analysis, 300–301, 361
- SourceForge.net, 209
- Southeast Cybercrime Institute, 251
- Special Ops Security, 306
- Spector Pro (keystroke-logging software), 104
- SpectorSoft, 104, 354
- spidering, 278, 280–281
- Spitzner, Lance, 34
- sponsorship, 18
- SQL injection, 27, 287–289
- SQL Injector, 288–289
- SQLPing3 (password-cracking software), 93, 304, 352, 359
- SSH (Secure Shell), 123
- SSID (service set identifier), 157–158
- storage system attacks. *See also* database attacks
  - best practices for minimizing risks, 313
  - misconceptions, 309
  - overview, 309
  - scanning for vulnerabilities, 310
  - testing tools, 309–310, 361
  - text file search, 310–313
  - Web sites, 361
- StorScan, 310, 361
- strong passwords, 110–111
- SUN RPC (remote procedure calls), 123
- Super Antenna, 365
- SuperScan
  - Linux system testing with, 208, 209–212
  - Netware testing with, 230
  - pinging multiple addresses with, 52
  - port scanning with, 53, 120
  - scanning Novell Netware systems with, 232
  - storage system testing with, 309
  - Web site, 358, 361
  - Windows system testing with, 184
- SUSE Linux, 227
- SUSE Linux Security Alerts, 360
- .swf files, 48–49
- SWFScan, 298, 364
- Switchboard.com, 353
- SYN floods, 145
- Sysinternals, 183, 365
- SYSKEY utility, 113
- System Center Configuration Manager, 269
- system hardening, 326–327, 361–362
- system scans. *See also* port scanning

- countermeasures, 212
- hosts, 52
- information obtained from, 52–53
- Linux systems, 209–212
- scanning, 53–55
- Windows systems, 185–187

systems

- knowledge of, 19
- selecting, 18

## • T •

tailgating, 77

TCP ports, 188

TCP scans, 122

TCP Wrappers, 217, 358

tcpcon (NetWare Loadable Module), 239–240

*TCP/IP For Dummies* (Leiden), 117

TCPCView, 184

telecom wires, 80

Telnet, 123, 130–131, 209, 213

Temporal Key Integrity Protocol (TKIP) encryption, 162

tests

- assumptions in, 43–44
- blind vs. knowledge assessments, 42
- denial of service, 146
- Linux systems, 225–226
- location, 43
- MAC address protocols, 171–174
- mistakes in, 347–350
- Novell Netware intruders, 237–238
- Novell Netware intruders, 237–238
- overview, 40
- password security, 97–100
- performing, 45–47
- reacting to vulnerabilities, 43
- rogue NLM programs, 238–241
- share permissions, 197
- specific tests, 41–42
- standards, 40
- timing, 40–41
- VoIP hosts, 273
- Windows systems, 185–187

- text files, searching for, 310–313
- TFTP (Trivial File Transfer Protocol), 123
- THC-Amap, 208
- TheHarvester, 258
- TheTrainingCo, 77
- Tiger, 208
- tiger team, 37
- time-memory tradeoffs, 87
- Traffic IQ Pro, 132–133, 358
- Tripwire, 223
- Trivial File Transfer Protocol (TFTP), 123
- TrueCrypt, 108, 224, 362
- trustworthiness, 16
- TSGrinder, 359
- Twitter, 145
- .txt file, 311

## • U •

UAC (User Account Control), 198

UDP ports, 188

UDP scans, 122

UDPFlood, 146, 358

unauthorized software, 27

Universal Naming Convention (UNC), 306

Unix systems

- password protection in, 114
- wireless hacking tools for, 154

unlimited attack, 19

unnneeded services

- access control, 217
- chkconfig, 217
- countermeasures, 216–217
- disabling, 216–217
- inetd.conf, 216–217
- security tools, 214–216
- vulnerabilities, 213–214

unsecured login mechanisms, 294–297

up2date, 227

URL manipulation, 285

U.S. Patent and Trademark Office, 353

US Search.com, 353

US-CERT Vulnerability Notes Database, 55, 363

User Account Control (UAC), 198  
 user awareness and training, 362  
 user ID, 27, 86, 112  
 UserDump, 356  
 USSearch, 49  
 utilities, physical security, 79–80

## • U •

VBScript, 290  
 vendor passwords, default, 358  
 virtual local area network (VLAN), 271  
 virtual machine software, 52  
 virtual private network (VPN), 164  
 VirtualBox, 52, 148  
 VMWare Workstation, 52  
 VNC, 83  
 Voice over IP (VoIP). *See also* messaging-system attacks  
   attacks, 16  
   capturing and recording voice traffic, 274–276  
   countermeasures against  
     vulnerabilities, 276  
   overview, 16, 270  
   scanning for vulnerabilities, 272–274  
   testing tools, 362–363  
   vulnerabilities, 270–272  
   Web sites, 362–363  
*VoIP For Dummies* (Kelly), 270  
 VoIP Hopper, 271, 363  
 VoIP servers, 68  
 vomit, 363  
 VRFY command, 257, 259  
 vulnerabilities. *See also* vulnerability testing  
   addressing, 323  
   assessing, 55–57  
   database attacks, 307–308  
   high-impact, 320  
   instant messaging, 267–268  
   Linux systems, 208  
   low-impact, 320  
   medium-impact, 320  
   messaging-system, 249–250  
   network infrastructure, 119–120

Novell Netware, 229–230  
 passwords, 86–88  
 physical security, 76  
 ranking, 320  
 reporting, 319–320  
 storage systems, 310  
 unneeded services, 213–214  
 Voice over IP, 270–272  
 Web applications, 280, 297  
 Windows systems, 182  
 wireless local area networks, 152  
 vulnerability assessment tools, 121  
 vulnerability databases, 363  
 vulnerability scanners, 17, 146  
 vulnerability testing  
   automated assessment, 56  
   manual assessment, 56  
   tools, 56–57  
   Web sites, 55

## • W •

walls, 79–80  
 wardriving, 155  
 warwalking, 168  
 weak authentication, 91  
 Web 2.0 hacking, 297  
 Web application attacks  
   best practices for minimizing risks, 298–301  
   case study, 279  
   default script attacks, 292–293  
   directory reversal, 280–283  
   input filtering attacks, 283–291  
   scanning for vulnerabilities, 297  
   testing tools, 20, 278  
   tools, 363–364  
   unsecured login mechanisms, 294–297  
   vulnerabilities, 280  
   Web sites, 363–364  
 Web browsers, configuring for Web proxy, 284  
 Web crawling, 49  
 Web page defacement, 31  
 Web Proxy, 284, 286

- Web search, 48
- Web security
  - firewalls, 299–300
  - obscurity, 299
  - source code analysis, 300–301
- Web sites
  - background checks, 49
  - Bing, 48
  - Bluetooth, 351
  - certifications, 352
  - database tools, 352
  - defaced Web pages, 31
  - exploit tools, 352
  - general research tools, 353
  - Google, 48
  - government and business, 49
  - hacking, 354
  - keyloggers, 354
  - laws and regulations, 354
  - Linux tools, 355
  - live toolkits, 355
  - log analysis, 355
  - messaging-system testing tools, 355–356
  - NetWare, 356
  - network analyzers, 121–122
  - network testing tools, 356–358
  - password cracking tools, 358–359
  - patch management, 359–360
  - scanners, 121–122
  - security education, 360
  - security methods and models, 360
  - security portals, 20
  - security tools, 20
  - source code analysis, 361
  - Spitzner, Lance, 34
  - storage testing tools, 361
  - system hardening, 361–362
  - user awareness and training, 362
  - VirtualBox, 52
  - Voice over IP, 362–363
  - vulnerability assessment tools, 122
  - vulnerability databases, 363
  - vulnerability testing, 55
  - Web applications, 363–364
  - Whois lookup, 50–51
  - Windows, 364–365
  - wireless networks, 365–366
- WebGoat, 364
- WebInspect, 146, 278, 288, 290, 364
- Wellenreiter, 154, 366
- WEP (Wired Equivalent Privacy), 160–161
- WEPCrack, 161, 366
- WhatIsMyIp.com, 52, 353, 358
- white hat hackers, 10
- Whois.net, 50, 353
- Whole Disk Encryption, 84, 108
- Wi-Fi. *See* wireless local area networks (WLANs)
- Wi-Fi Protected Access (WPA), 160, 162
- WifiMaps, 366
- WiGLE database, 156–157, 366
- WildPackets OmniPeek, 121, 154
- Wiles, Jack (TheTrainingCo.), 77
- WinAirsnot, 366
- windows, 79–80
- Windows 7 operating system, 198
- Windows BitLocker, 84, 108
- Windows Defender, 198
- Windows Firewall, 198
- Windows operating system
  - attacks, 15
  - password storage location in, 93–94
  - securing, 113–114
- Windows password. *See also* password cracking
  - cracking, 87
  - cracking with ophcrack, 99–101
  - cracking with pwdump and John the Ripper, 96–98
  - protection of, 113–114
- Windows Registry, 113, 143–144
- Windows Server Update Services, 326, 360
- Windows systems. *See also* Linux systems
  - authenticated scans, 205–206
  - missing patch exploitation, 198–205
  - NetBIOS, 187–190
  - null sessions, 190–195
  - overview, 181–182
  - scanning, 185–187
  - security tools, 182–184
  - share permissions, 196–198
  - testing tools, 364–365
  - vulnerabilities, 182
- Windows Terminal Server, 123

- Winfo, 184, 192–193, 365
  - WinHex, 111, 292, 359
  - Winkler, Ira (Internet Security Advisors Group), 63
  - WinNuke, 145
  - WinRAR, 95
  - WinZip, 97, 356
  - Wired Equivalent Privacy (WEP), 160–161
  - wireless antennas, 155
  - Wireless Hardware Comparison, 155
  - wireless local area networks (WLANs)
    - access points, 152
    - case study, 153
    - checking for AP's MAC address, 156–157
    - default configuration settings, 178
    - hacking tools, 154–155
    - overview, 151
    - scanning SSIDs, 157–158
    - vulnerabilities, 152
  - WiGLE database, 156–157
  - wireless network attacks
    - Bluetooth, 160
    - encrypted traffic, 160–165
    - MAC address spoofing, 170–175
    - overview, 158–159
    - physical security problems, 176–177
    - Queensland DoS attack, 175–176
    - rogue wireless devices, 165–170
    - tools, 365–366
    - vulnerable wireless workstations, 177–178
    - Web sites, 365–366
  - Wireless Vulnerabilities and Exploits, 152, 363
  - wireless workstations, vulnerability of, 177–178
  - Wireshark, 53, 106, 135, 268, 358
  - word lists (password cracking), 358
  - Wotsit's Fromat, 353
  - WPA (Wi-Fi Protected Access), 160, 162
  - WPA2, 162–163
  - Wright, Joshua (InGuardians Inc.), 153
  - WSDigger, 298, 364
  - WSFuzzer, 298, 364
- X •
- .xls file, 311
  - .xlsx file, 311
  - xp\_dirtree extended stored procedure, 306
  - XSS (cross-site scripting), 290
- Y •
- Yahoo! Finance, 353
  - YaST2 Package Manager, 227
- Z •
- ZabaSearch, 49, 353
  - zombie computers, 71