

# Index

## • *Symbols and Numerics* •

\$ (dollar sign), shares marked with.  
See hidden shares  
2600 — *The Hacker Quarterly* magazine, 32

## • *A* •

- abuse.net member, SMTP relay, 274
- access points (APs), 162
- account lockout, 110–111
- accounts, user
  - lock outs during password cracks, 92
  - weak passwords in limbo, 107
- Active Server Pages (ASP) scripts, 312–313
- Acunetix Web Vulnerability Scanner, 294
- address, IP
  - gateway, displaying, 52
  - IM, capturing, 282
  - MAC address, comparing, 177–178
  - NetWare system, scanning, 245
  - URL, converting, 314–315
- address, URL
  - code-injection and SQL injection attacks, 304–307
  - file manipulation, 295, 297
  - login return messages, 298–299
- address, URL filter bypassing
  - countermeasure, 315
  - described, 313–315
- admin utilities, NetWare, 256
- administrator reset programs, 107–108
- AdRem Software version of rconsole, 251
- Advanced Archive Password Recovery
  - password cracking tool, 103
- advice about tools, obtaining, 19
- aircrack tool, 170, 171
- AirMagnet Handheld Analyzer, 164
- AirMagnet Laptop Analyzer wireless device scan, 176–177
- AiroPeek tool
  - rogue wireless devices, 173, 174–175
  - WEP keys, 171–172
- Akin, Thomas (e-mail systems and forensics expert), 267
- ally and sponsor, cultivating, 347
- Amap application version mapping tool, 222, 228, 229
- analog war dialing, 117
- anonymity, hackers maintaining, 32
- antenna, external, 165, 184
- anticipating vulnerabilities, 13
- AP system names
  - MAC spoofing, 179
  - rogue wireless devices, 173, 174
- Apache Web server, 302
- AppDetective database server tool, 320–321
- Apple Macintosh computer
  - war dialing software, 119
  - WEP key cracking software, 170
- application service providers, 39
- applications
  - attacks, 15
  - passwords, blocking storage, 110
  - test choices, 37
- applications, Web
  - assessment tools, 19
  - case study, 295
  - default script attacks, 312–313
  - described, 293, 294, 296
  - directory traversal, 299–302
  - firewalls, 323–324
  - general security scans, 315–316
  - input filtering attacks, 303–310
  - memory attacks, 310–311
  - obscurity, minimizing risks through, 322–323
  - resources, 367–368
  - URL filter bypassing, 313–315
- approval, obtaining, 33–34
- APs (access points), 162
- ARP spoofing, 153–155
- Arpwatch ARP detection software, 157
- ASCII characters, passwords and, 98
- ASP (Active Server Pages) scripts, 312–313
- attachment, e-mail, 268
- attack tree analysis, 38
- audit system, NetWare, 261

authenticated scans  
 general OS vulnerabilities, 218–219  
 network files, rooting sensitive text from, 219–220  
 authentication, SMTP relay, 277  
 awareness tools, listed, 357

## • B •

background checks, 49  
 BackTrack WLAN security tool, 163, 223  
 badges, obtaining false, 63  
 bandwidth blocking, e-mail bombs, 268  
 banner grabbing  
 countermeasures, 143  
 Netcat, 142–143  
 telnet, 142  
 banners, e-mail, 271–272  
 baud rates, war dialing, 122  
 Beaver, Kevin (*Hacking Wireless Networks For Dummies*), 171, 174  
 believability, social engineering and, 69  
 benefits, demonstrating, 349  
 Berkeley Software Distribution.  
*See* BSD r-commands  
 BIOS passwords, 106  
 Blacklisted 411 magazine, 32  
 blacklisted e-mail client, 267  
 Blaster worm, 200  
 blind assessment, 46  
 blind ethical hacking, 35  
 blind versus knowledge assessments, 41  
 Bluetooth wireless devices  
 tools, listed, 358  
 vulnerabilities, 169  
 broadcast mode, 153  
 browser, Web, 47  
 browsers, Web, memory attacks via, 310–311  
 brute-force password attacks, 94–95  
 BSD (Berkeley Software Distribution)  
 r-commands  
 disabling, 232–233  
 files, accessing without password, 232  
 services, discerning, 225  
 buffer overflow attacks, 237  
 building infrastructure  
 attack points, 78  
 countermeasures, 78–79  
 business goals, supporting, 349  
 business phones, 68  
 business Web sites, 49

## • C •

Cain and Abel network analyzer program  
 ARP poisoning, 154–155  
 obtaining, 147  
 password cracking, 91  
 voice traffic, capturing and recording, 290–292  
 Caldwell, Matt (founder and chief security officer, GuardedNet), 163  
 caller ID, hiding number from, 68  
 candy-security adage, 62  
 antenna kits and directions, 165  
 case studies  
 e-mail attacks, 267  
 network infrastructure, 128  
 passwords, 87  
 social engineering, 63  
 WLANs, 163  
 cell phones, speaking on, 67  
 CERT Vulnerabilities and Fixes site, 227  
 certification, 358  
 CGI (Common Gateway Interface) scripts, 312–313  
 Chappell, Laura (network protocols and analysis authority), 128  
 Character Generator port, NetWare, 246  
 chkconfig, Linux program, 230–231  
 chknul password cracking software, 92  
 Cisco  
 LEAP protocol, 172  
 rogue wireless devices, 174–175  
 civil liberty, as hacker philosophy, 30  
 classifying information, 73  
 cleartext packets, 257–258  
 client notification, 36  
 Client32 software, NetWare, 244  
 CMOS chip, passwords stored in, 106  
 Cobb, Chey (*Network Security For Dummies*), 111, 336  
 code injection, 304–307  
 coding  
 e-mail, 280  
 false sense of security, 12  
 weak password, 88  
 Common Gateway Interface (CGI) scripts, 312–313  
 Common Vulnerabilities and Exposures Web site (CVE), 328  
 CommView network analysis program, 147  
 Computer Underground Digest, 32  
 computers, physical security of, 81–84

- configuration information, null session, 203–205
  - Connect scan, Nmap, 136
  - console access, NetWare, 245
  - ConsoleOne (Novell), 260
  - contingency plans, formulating, 18
  - continuous capture mode, network analyzer, 159
  - conversations in public places, 67
  - CORE IMPACT
    - share permissions, 210
    - system, penetrating, 58
    - Windows testing phases, 193, 215–217
  - costs, demonstrating, 348
  - crackers, 10
  - cracking passwords, 85
  - crashing systems, need to avoid, 16–17
  - crawlers, directory traversal, 300
  - credibility, establishing, 350
  - criminal hackers, 10
  - cross-shredding, 67
  - cross-site scripting (XSS), 309
  - CVE (Common Vulnerabilities and Exposures Web site), 328
  - cyberterrorists, 27
- D •
- daemons, UNIX
    - disabling, 229–230
    - e-mail delivery flaw, 269
    - NFS, 235
    - vulnerabilities, 223, 225, 227
  - database
    - firewall, 323
    - passwords, cracking server, 318–320
    - resources, 367–368
    - scanning, 320–321
    - seriousness of, 316–317
    - servers, finding on network, 317–318
    - tools, 317
    - Web application attacks, 296
  - Davis, Peter T. (*Hacking Wireless Networks For Dummies*), 171, 174
  - DCE (Distributed Computing Environment)
    - internal protocol, 199
  - DDoS (Distributed DoS) attacks, 158
  - Debian Linux system, updating, 242
  - defacing Web page, 29
  - default script attacks, 312–313
  - defense in-depth perspective, 338
  - delimited files, saving reports as, 205
  - deliverables, 35
  - denial of service attacks. *See* DoS attacks
  - desktop auditing utilities, 285
  - devices, choosing for tests, 37
  - dial tone, phone system vulnerability, 116
  - dialing, war
    - configuration utility, 121–122
    - information gathering, 118
    - from inside, 120
    - methods, 116–118
    - modem hardware, choosing, 119–120
    - modem safety, 115–116
    - operating modems, 125–126
    - phone numbers, protecting, 125
    - resources, 367
    - rooting through systems, 124–125
    - scanning for modems and open ports, 53
    - secure modem placement, 126
    - software tools, 119
    - telephone system vulnerabilities, 116
    - testing, 122–124
  - dictionary files, 358
  - dictionary password attacks, 93–94
  - Digital Hotspotter, 164
  - directory traversal
    - countermeasures, 302
    - crawlers, 300
    - filenames, 299–300
    - Google, 300–301
    - robots.txt file, searching for, 299
  - Distributed Computing Environment (DCE)
    - internal protocol, 199
  - Distributed DoS (DDoS) attacks, 158
  - DNS queries, running, 50
  - DNSstuff.com, 50
  - documentation
    - loaded NLMs, 256
    - obtaining, 77
  - documented approval, importance of, 353
  - dollar sign (\$), shares marked with. *See* hidden shares
  - DoS (denial of service) attacks
    - causing by testing, 16, 40–41, 44, 158
    - countermeasures, 158–159
    - described, 157–158
    - distributed, 158
    - IM, 281
    - NetWare TCP/IP parameters, 261
    - Smurf, 150
    - testing, 158
    - user account lock outs during password cracks, 92

drives, network, 282–284  
 DumpSec tool  
   null session configuration, 204–205  
   share permissions, 209–210  
   unused accounts, searching for, 110  
 dumpster diving, 67–68, 80

## ● E ●

EC-Council Certified Ethical Hacker program, 12  
 Echo port, NetWare, 246  
 eDirectory browsing, disabling, 259–260  
 eDirectory, NetWare, 254  
 Eicar malware test string, 279  
 Elcomsoft Distributed Password Recovery password cracking software, 92  
 elevators, entering building in, 77  
 e-mail  
   attachment bombs, 268–269  
   automated input attacks, 303–304  
   automatic security, 270  
   banners, 271–272  
   connection bombs, 269–270  
   content filtering applications, 270  
   described, 266  
   fake Microsoft patch, 71  
   firewalls, 270  
   hacking case study, 267  
   information, seeking through, 70–71  
   Linux sendmail vulnerabilities, 228  
   malware, 278–279  
   operating guidelines, 281  
   phishing, 62  
   servers, information retrievable from, 55  
   SMTP attacks, 272–280  
   software solutions, 280  
   test information, encrypting, 21  
 employees. *See also* rogue insiders  
   fake, 62  
   former, disabling e-mail accounts, 267  
   impersonating, 70  
   Internet acceptable usage policy, 313  
   security-aware mindset, instilling, 343–344  
 encryption  
   e-mail, 280  
   false sense of security, 12  
   weak password, 88

Essential NetTools scanner, 130  
 Ethereal network analyzer program, 147  
 EtherPeek commercial network analyzer  
   described, 105  
   monitor mode, 149  
 ethical, definition of, 9  
 ethical hacking  
   commandments, 15–17  
   dangers faced by, 13–15  
   described, 9–10  
   executing plan, 21  
   formulating plan, 17–19  
   hacker defined, 10  
   malicious attackers versus, 11–12  
   need for hacking, 12–13  
   results, evaluating, 22  
   rogue insider defined, 11  
   tools, selecting, 19–21  
 ettercap network analyzer program, 147  
 event logging system, 341  
 examples  
   e-mail attacks, 267  
   network infrastructure, 128  
   passwords, 87  
   social engineering, 63  
   WLANs, 163  
 exploit tools, 358  
 EXPN (expand) SMTP command, 273–274  
 external attackers. *See* hackers  
 external hacks, 42

## ● F ●

fake Microsoft patch e-mail, 71  
 false positives and negatives, 19  
 file permissions, Linux, 235–237  
 file sharing, IM, 282–284  
 FileLocator Pro, 220  
 filenames, directory traversal, 299–300  
 files  
   accessing without password, 232  
   passwords, cracking, 102–103  
 filters  
   MAC controls, 178  
   SMTP relays, 275  
   URL, bypassing, 313–315  
 FIN Stealth scan, Nmap, 136  
 fingerprinting, 196

## firewall

- all-in-one testing tools, 144
- countermeasures, 145–146
- database, 323
- e-mail server, 281
- false security generated by, 12, 65
- Linux system scanning, 227
- malformed traffic, blocking, 159
- NetBIOS attacks, blocking, 199, 206
- Netcat testing, 144–145
- rogue wireless devices, countermeasures against, 178
- RPC enumeration, protecting against, 200
- server, hiding behind, 337
- switches, 106
- system scanning countermeasures, 196
- Windows Vista, 211

## fishing for information

- dumpster diving, 67–68
- on Internet, 66–67
- phone systems, 68

## fixes

- automating, 335–336
- managing, 334–335
- NetWare, 245, 248, 262
- Windows issues, avoiding, 189

## flowchart, attack tree analysis, 38

## footprinting

- described, 47
- mapping network, 49–51
- open ports, what's running on, 53–55
- penetrating system, 57–58
- public information, gathering, 47–49
- scanning systems, 52–53
- vulnerabilities, assessing, 55–57

## Freecon, 251

## freeloaders, 128

## freely available information, gathering

- Web crawling, 48–49
- Web search, 47–48
- Web sites, 49

## FTP

- buffer overflow attacks, 237
- disabling, 231
- for large file transfers, 269
- Linux vulnerabilities, 227–228
- NetWare vulnerabilities, 246

## • G •

- gateway, IP address displaying, 52
- general research tools, 359
- Georgia wireless networks, security case history, 163
- Getif scanner
  - obtaining, 130
  - SNMP systems, enumerating, 140
- GetUID file permission, Linux
  - automatic testing, 237
  - manual testing, 236
  - vulnerabilities, 235
- GFI email security testing zone, 279
- GFI LANguard Network Security Scanner
  - vulnerability assessment tool, 131
- Gnutella file-share application, 128
- goals, establishing, 34
- Google
  - directory traversal, 300–301
  - hacking Web applications, 295
  - Internet searches, 48
  - NetWare ports, finding, 255
  - Usenet Groups, 51
- Google Hacking for Penetration Testers* (Long), 301
- government hackers, 28
- government Web sites, 49

## • H •

## hackers

- anonymity, maintaining, 32
  - defined, 10
  - described, 23–25
  - former, hiring, 27
  - government, 28
  - motivation, 27–30
  - publications, 360
  - skill levels, 26–27
  - styles, 30–32
  - viewpoint, looking from, 355
- Hackers: Heroes of the Computer Revolution* (Levy), 357
- Hacking Wireless Networks For Dummies* (Davis and Beaver), 171, 174
- hacktivists, 27

- hardcore vulnerability exploitation, 210–217
- hashes, password hacking, 87, 101
- Herold, Rebecca (*Managing an Information Security and Privacy Awareness and Training Program*), 357
- hidden field manipulation, 307–308
- hidden shares
  - null session attach method, 201
  - security of, 199
- hiring outside companies
  - ethical hacking, 341–343
  - security training, 73
  - social engineering testing, 64
  - testing, supervising, 356
- holes, plugging security
  - automating, 335–336
  - case study, 337
  - hardening systems, 336–337
  - managing, 334–335
  - NetWare, 245, 248, 262
  - patches, 334–336
  - reports, turning into action, 333–334
  - security infrastructure, assessing, 337–338
  - Windows issues, avoiding, 189
- hosts
  - internal, scanning, 52
  - Linux `hosts.equiv` file, 231
  - scanning systems, 52
- HTTP (Hypertext Transfer Protocol)
  - described, 15
  - for large file transfers, 269
  - Web application vulnerabilities, 294
- HTTrack Website Copier
  - spider program, 300
  - Web applications, testing, 294
- human element, social engineering and attackers' use of, 64
  - case study, 63
  - caution, 62
  - countermeasures, 72–74
  - described, 14
  - examples, 61–62
  - exploiting relationship, 69–72
  - fishing for information, 66–68
  - implications, 65
  - outsider, benefits of hiring, 64
  - passwords, cracking, 89–90
  - trust, building, 68–69
- Hypertext Transfer Protocol. *See* HTTP
- IEEE 802.11 standard. *See* WLANs
- ignorance, hackers preying on, 31
- IIS (Internet Information Server)
  - directory traversal countermeasures, 302
  - security by obscurity, 322
- IM (Instant Messaging)
  - DoS attacks, 281
  - rogue software, 284
  - system configuration, 285
  - traffic, detecting, 285
  - user behavior, 285
  - vulnerabilities, 281–284
- individualism, hacker mindset and, 28
- `inetd.conf`, Linux file, 229–230
- inference password cracks, 90
- initialization vector (IV), RC4, 169
- input filtering attacks
  - automated input, 303–304
  - buffer overflows, 303
  - code injection and SQL injection, 304–307
  - countermeasures, 309–310
  - cross-site scripting, 309
  - hidden field manipulation, 307–308
- insiders, rogue
  - attack style, 31
  - defined, 11
  - motivations, 29
  - problem with, 24
- instability, Windows, 191
- Instant Messaging. *See* IM
- insurance, liability, 34
- Integrated Services Digital Network (ISDN), 117
- intermediate hackers, 26
- internal attacks. *See* rogue insiders
- Internet
  - acceptable usage policy, 313
  - access, assessing in NetWare, 245
  - fishing for information, 66–67
  - Linux services, 223
  - public information, gathering, 47–48
  - war dialing numbers, 118
- Internet Information Server. *See* IIS
- Internet Service Provider (ISP), 39
- Internet telephone. *See* VoIP
- intruder lockout, 110–111
- intrusion detection system, 65

- IP address
    - gateway, displaying, 52
    - IM, capturing, 282
    - MAC address, comparing, 177–178
    - NetWare system, scanning, 245
    - URL, converting, 314–315
  - ISDN (Integrated Services Digital Network), 117
  - ISP (Internet Service Provider), 39
  - IV (initialization vector), RC4, 169
- J •**
- John the Ripper password cracking software
    - weak authentication, 91
    - in Windows, 96–97
- K •**
- Kazaa file-sharing application, 128
  - Kelly, Timothy V. (*VoIP For Dummies*), 286
  - keylogger, 71
  - keys, WEP, 171–172
  - keystroke-logging tools, 103–104
  - keyword searches
    - Google, 48
    - sensitive information in non-secured files, 220
  - Kismet wireless sniffer, 174
  - knowledge
    - breadth of, 355
    - systems, before testing, 18
  - Korean National Policy Agency, 27
- L •**
- L7 Enforcer and L7 Enterprise IM tracker, 285
  - LANguard Network Security Scanner
    - firewall, testing, 144
    - in Linux, 222, 224–225
    - in NetWare, 244, 246–247
    - patches, checking for, 336
    - share permissions, displaying, 210
    - shares, 198
  - LanHound tool
    - analyzing erratic network performance, 147
    - obtaining, 131
  - laptops
    - securing, 83–84
    - systems, caution against resetting, 106
  - Leiden, Candace (*TCP/IP For Dummies*), 127
  - Levy, Stephen (*Hackers: Heroes of the Computer Revolution*), 357
  - likability, social engineering and, 69
  - Linux
    - buffer overflows, 237–238
    - daemons, scanning, 223–226
    - distribution updates, 241–242
    - file permissions, 235–237
    - general security tests, 239–241
    - multiplatform update managers, 242
    - NFS, 233–235
    - ophcrack password cracking software, 100
    - password countermeasures, 112
    - password storage files, 93
    - physical security, 238–239
    - resources, 360–361
    - .rhosts and hosts.equiv files, 231–233
    - system scanning countermeasures, 227
    - tools, available, 222–223
    - unnneeded services, 227–231
    - vulnerabilities, 221–222
    - Web server security by obscurity, 322
    - WLAN security tools, 163–164, 180
  - Linux Security Auditing Tool (LSAT), 223, 240
  - List Open Files (lsof), Linux utility, 228
  - location, testing standards, 41–42
  - log
    - e-mail server transactions, 281
    - hack, maintaining, 46
    - IM conversations, 284
    - monitoring malicious use, 340–341
    - ToneLoc war dialing, 123–124
  - log analysis resources, 361
  - login
    - input fields in Web applications, targeting, 303
    - NetWare, 245, 256–257
    - random, 94
    - return messages, 298–299
  - Long, Johnny (*Google Hacking for Penetration Testers*), 301
  - lookups, Whois
    - information, using, 52
    - mapping network, 49–51
    - war dialing information, 118
  - losses, social engineering, 65
  - LSAT (Linux Security Auditing Tool), 223, 240
  - lsof (List Open Files), Linux utility, 228

## • M •

- MAC (media access control)
  - address mappings, 153
  - filtering controls, 178
  - IP address, mapping, 177–178
  - rogue wireless devices, 173
  - worldwide LAN recognition, checking, 165–166
- MAC-daddy attack
  - ARP spoofing, 153–155
  - countermeasures, 157
  - UNIX MAC address spoofing, 156
  - Windows MAC address spoofing, 156–157
- Macintosh computer
  - war dialing software, 119
  - WEP key cracking software, 170
- magazines for hackers, 31–32
- mail, electronic
  - attachment bombs, 268–269
  - automated input attacks, 303–304
  - automatic security, 270
  - banners, 271–272
  - connection bombs, 269–270
  - content filtering applications, 270
  - described, 266
  - fake Microsoft patch, 71
  - firewalls, 270
  - hacking case study, 267
  - information, seeking through, 70–71
  - Linux sendmail vulnerabilities, 228
  - malware, 278–279
  - operating guidelines, 281
  - phishing, 62
  - servers, information retrievable from, 55
  - SMTP attacks, 272–280
  - software solutions, 280
  - test information, encrypting, 21
- Mailsnarf e-mail packet sniffer, 278
- malicious attackers, 11–12
- malware
  - e-mail systems, 278–279
  - protection software, 110
  - resources, 361
- managed security services provider (MSSP), 341
- management, upper
  - ally and sponsor, cultivating, 347
  - benefits, demonstrating, 349
  - business goals, supporting, 349
  - costs, demonstrating, 348
  - credibility, establishing, 350
  - don't blow things out of proportion, 348
  - flexibility and adaptability, 351
  - techie talk, avoiding, 350
  - understanding business, 349–350
  - value, demonstrating, 350–351
- Managing an Information Security and Privacy Awareness and Training Program* (Herold), 357
- managing security changes
  - automating ethical hacking process, 339–340
  - former hackers, hiring, 343
  - keeping up with issues, 344
  - monitoring malicious use, 340–341
  - outsourcing ethical hacking, 341–343
  - security-aware mindset, instilling, 343–344
- man-in-the-middle attacks, 168
- mapping network
  - Google groups, 51
  - privacy policies, 51
  - Whois lookup, 49–51
- MBSA (Microsoft Baseline Security Analyzer), 191, 218–219
- media access control. *See* MAC
- memory attacks, 310–311
- messaging systems. *See also* e-mail; IM
  - resources, 361–362
  - VoIP, 286–292
- Metasploit tool
  - buffer overflow attacks, 237
  - described, 58, 210
  - obtaining, 193
  - remote command prompt, finding on vulnerable server, 212–215
- Microsoft Baseline Security Analyzer (MBSA), 191, 218–219
- Microsoft Windows
  - all-in-one assessment tools, 192
  - authenticated scans, 218–220
  - availability of hacking and testing tools, 190–191
  - CORE IMPACT testing, 193, 215–217
  - essential tools, 191
  - free Microsoft tools, 191–192
  - hardcore vulnerability exploitation, 210–217
  - MAC address spoofing, 156–157
  - NetBIOS, 196–199
  - network analyzer, detecting, 153
  - null sessions, 201–208

- password countermeasures, 111–112
  - password cracking method, 87
  - password storage files, 93
  - passwords, cracking with `pwdump3` and John the Ripper, 96–97
  - prevalence of, 189–190
  - resources, 368–369
  - share permissions, 208–210
  - system scanning, 194–196
  - task-specific tools, 192–193
  - telnet port, finding, 142
  - version shown, 193
  - vulnerabilities, 190
  - WLAN security tools, 164, 180
  - Microsoft Windows 2000
    - default share permissions, 208–209
    - NetBIOS security settings, 207–208
  - Microsoft Windows 2003 Server/XP default share permissions, 209
  - Microsoft Windows Explorer, 219
  - Microsoft Windows NT
    - default share permissions, 208–209
    - NetBIOS security settings, 208
    - server security example, 337
  - Microsoft Windows Resource Kits, 191–192
  - Microsoft Windows Vista, 211
  - mirroring, Web site, 294
  - mobile devices, 169
  - modems, 53. *See also* war dialing
  - modules command, NetWare server console prompt, 254
  - monitor mode, 149
  - motivation, hackers', 27–30
  - MSSP (managed security services provider), 341
- **N** ●
- name hijacking, IM, 281
  - names, AP system
    - MAC spoofing, 179
    - rogue wireless devices, 173, 174
  - National Vulnerability Database, 88
  - NCP (NetWare Core Protocol), 246, 248
  - NCP Query vulnerability assessment tool, NetWare
    - described, 244
    - server and directory tree information, gathering, 247
  - Nessus vulnerability assessment tool
    - in Linux, 223, 224
    - obtaining, 131
  - `net view` command, 203
  - NetBIOS
    - described, 196
    - firewall, 199, 206
    - network shares, 198–199
    - passwords, 199
    - ports, 197
    - shares, 198
    - traffic limiting, 199
    - unauthenticated enumeration, 197–198
  - Netcat scanner
    - banner grabbing, 142–143
    - firewall rules, testing, 144–145
    - obtaining, 131
  - Netcraft Web server version utility, 54–55
  - NetScanTools Pro scanner
    - network information, gathering general, 137–138
    - obtaining, 130
  - `netstat` Linux scan, 228
  - NetStumbler airwave monitoring tool
    - local airwaves, 167
    - rogue wireless devices, 173–176
  - NetWare Core Protocol (NCP), 246, 248
  - NetWare (Novell)
    - affected versions, 244–245
    - audit system, 261
    - cleartext packets, 257–258
    - disable eDirectory browsing, 259–260
    - enumeration countermeasures, 248
    - intruder detection, 252–253
    - NCPQuery, 247
    - password cracking software, 92
    - patches, 245, 248, 262
    - port scanning, 245–247
    - Remote Console program (`rconsole`), 249–251
    - remove bindery contexts, 260–261
    - rename admin account, importance of, 258–259
    - resources, 362
    - rogue NLMs, 253–257
    - server access methods, 245
    - server-console access, 251–252
    - TCP/IP parameters, 261
    - testing authentication, 248
    - tools, 244
    - vulnerabilities, 243–244

- network analyzers
    - countermeasures, 151–152
    - described, 146–147
    - detecting, 153
    - passwords, 105–106
    - physical security, 152
    - programs, 147–151
  - Network File System (NFS), 233–235
  - network infrastructure
    - assessing, 131
    - attacks, 14
    - banner grabbing, 142–143
    - case study, 128
    - countermeasures, 83–84
    - described, 127
    - DoS attacks, 157–159
    - files, rooting sensitive text from, 219–220
    - firewall rules, 143–146
    - general defenses, 159–160
    - jacks, 73
    - MAC-daddy attack, 153–157
    - network analyzers, 146–153
    - physical security, 81–84
    - port scanner, 132–139
    - resources, 362–363
    - scanners and analyzers, 130–131
    - SNMP scanning, 139–141
    - steps, 131
    - switches versus hubs, 106
    - vulnerabilities, 129–130
    - weaknesses, 81–83
  - Network Security For Dummies* (Cobb), 111, 336
  - Network Users tool, 193, 205–206
  - NFS (Network File System), 233–235
  - NGSSQuirreL database server tool, 318–319, 321
  - Nigerian 419 e-mail fraud scheme, 71–72
  - Nmap scanner
    - Linux uses, 226, 228, 229
    - obtaining, 130–131, 191
    - open ports, finding, 136–137
    - ping sweep, 134
    - uses, 222
    - Windows testing, 194–195
  - NmapWin scanner, 130–131
  - nontechnical attacks, 14
  - notebook computers
    - securing, 83–84
    - systems, caution against resetting, 106
  - Novell ConsoleOne, 260
  - Novell NetWare
    - affected versions, 244–245
    - audit system, 261
    - cleartext packets, 257–258
    - disable eDirectory browsing, 259–260
    - enumeration countermeasures, 248
    - intruder detection, 252–253
    - NCPQuery, 247
    - password cracking software, 92
    - patches, 245, 248, 262
    - port scanning, 245–247
    - Remote Console program (rconsole), 249–251
    - remove bindery contexts, 260–261
    - rename admin account, importance of, 258–259
    - resources, 362
    - rogue NLMs, 253–257
    - server access methods, 245
    - server-console access, 251–252
    - TCP/IP parameters, 261
    - testing authentication, 248
    - tools, 244
    - vulnerabilities, 243–244
  - N-Stealth Security Scanner, 294
  - NTAccess password reset tool, 107
  - null passwords, checking in NetWare, 102
  - Null scan, Nmap, 136
  - null sessions, 201–208
  - number range, war dialing, 122, 124
- 0 •
- obscurity, security by, 88, 322
  - Oechslin, Philippe (researcher and independent information security consultant), 87
  - office design and usage
    - attack points, 80–81
    - countermeasures, 81
  - Official Internet Protocol Standards page, Request for Comments list, 127
  - OmniPeek wired and wireless analyzer, 292
  - on/off switches, covering, 79–80
  - Open Source Security Testing Methodology Manual, 58
  - operating system attacks, 14–15
  - ophcrack tool, 98–100
  - Oracle database servers, finding, 317
  - Orinoco 802.11b PC Card, 164
  - OS fingerprint scan, Linux, 226
  - outcomes, specific, 35
  - Outlook Web Access (OWA), 281
  - outsourcing
    - ethical hacking, 341–343
    - security training, 73
    - social engineering testing, 64
    - testing, supervising, 356
  - OWA (Outlook Web Access), 281

## ● p ●

- P2P software, barring, 285
- packet sniffing. *See* network analyzers
- packets, WEP key, 170
- padded binary form, IP address, 314
- Pandora NetWare hacking suite, 257
- Pandora password cracking software, 92
- Paros Web application testing tool, 294
- Password Safe software, 108
- passwords
  - account lockout, 110–111
  - administrator reset programs, 107–108
  - BIOS, 106
  - brute-force attacks, 94–95
  - case study, 87
  - cracking, ease of, 88–89
  - cracking tools, 19, 364
  - cross-site scripting, 309
  - database cracking tool, 319
  - dictionary attacks, 93–94
  - ease of access to, 85
  - files, cracking, 102–103
  - inference cracks, 90
  - John the Ripper, 96–97
  - keystroke logging, 103–104
  - in limbo, 107
  - memory attacks, 310–311
  - network analyzer, 105–106
  - null session, gathering during, 202
  - organizational vulnerabilities, 86, 88
  - policies, 109
  - pwdump3, 96–97
  - rainbow attacks, 95–96
  - rainbow tables with ophcrack tool, 98–100
  - RainbowCrack Online, cracking Windows passwords with, 101
  - random number, 98
  - shoulder surfing cracks, 90
  - social engineering cracks, 71, 89–90
  - software cracking, 91–93
  - storage, 104–105, 108–109
  - technical vulnerabilities, 88
  - unsecured login mechanisms, 296–298
  - weak authentication cracks, 90–91
  - Windows countermeasures, 111–112
- passwords, NetWare
  - null, checking, 102
  - rconsole, 249–251
  - server reset tools, 254
  - testing, 248
  - vulnerability, 257
- passwords, UNIX
  - countermeasures, 112
  - John the Ripper, creating, 97–98
  - storage files, 93
- passwords, Windows
  - countermeasures, 111–112
  - cracking method, 87
  - John the Ripper cracking, 96–97
  - pwdump3 cracking, 96–97
  - storage files, 93
- patches
  - automating, 335–336
  - managing, 334–335
  - NetWare, 245, 248, 262
  - Windows issues, avoiding, 189
- PDAs (personal digital assistants), 83
- penetration test, 40
- perimeter protection, e-mail, 270
- permission
  - goals, establishing, 34
  - obtaining, 11–12
- permissions, share
  - testing, 209–210
  - Windows defaults, 208–209
  - Windows security flaws, 208–210
- personal digital assistants (PDAs), 83
- personal information, 49
- PGP (Pretty Good Privacy)
  - e-mail, 280
  - files, protecting, 103
  - passwords, storing, 108
- Philippines hacker ring, 27
- phishing e-mail, 62
- phone, Internet. *See* VoIP
- phone numbers
  - checking for war dialing, 124–125
  - protecting from war dialing, 125
- phone system
  - fishing for information, 68
  - war dialing vulnerabilities, 116
- PhoneSweep war dialing software, 119
- PHRACK magazine, 32
- physical security
  - assessing, 76–78
  - attacks, 14
  - building infrastructure, 78–79
  - Linux, 238–239
  - network analyzers, 152
  - network components and computers, 81–84
  - office design and usage, 80–81
  - utilities, 79–80
  - vulnerabilities, 75–76
  - wireless network, walking perimeter, 176

- ping
    - host names or IP addresses, 52
    - port sweeping, 134
  - Ping of Death, 158
  - plan
    - approval, obtaining, 33–34
    - attack tree analysis, 38
    - ethical hacking, 17–19
    - executing, 21
    - goals, establishing, 34–36
    - systems, choosing, 36–38
    - testing standards, 39–43
  - plugging security holes
    - case study, 337
    - hardening systems, 336–337
    - patches, 334–336
    - reports, turning into action, 333–334
    - security infrastructure, assessing, 337–338
  - point-to-point software, barring, 285
  - Point-to-Point Tunneling Protocol (PPTP), 172
  - port scanner
    - commonly hacked ports, listed, 133–134
    - described, 132
    - network information, gathering, 137–138
    - Nmap, 136–137
    - ping sweeping, 134
    - SuperScan, 135–136
    - traffic denial, 139
    - traffic restriction, 138–139
  - port scanning
    - inability to check passwords, 19
    - NetWare, 248, 255
    - Windows testing, 194–195
  - portable computers
    - securing, 83–84
    - systems, caution against resetting, 106
  - ports
    - footprinting, 53–55
    - NetBIOS, 197
    - open, scanning for, 53
    - Web application running, 323
  - positives, false, 19
  - PPTP (Point-to-Point Tunneling Protocol), 172
  - pre-shared keys (PSKs), 171
  - Pretty Good Privacy. *See* GPG
  - privacy policies, 51
  - privacy, respecting, 16
  - Proactive Password Auditor password cracking software, 91
  - Proactive System Password Recovery password cracking software, 92
  - production systems, 356
  - promiscuous mode, placing network card in, 147
  - prosecution, criminal, 29
  - PSKs (pre-shared keys), 171
  - Public Browse right, NetWare eDirectory, 259, 261
  - public information, gathering
    - Web crawling, 48–49
    - Web search, 47–48
    - Web sites, 49
  - pwdump3 password cracking software, 91, 96–97
- *Q* •
- QualysGuard vulnerability assessment tool
    - cost, 57
    - described, 131, 192
    - exploitable items, finding, 211–212
    - in Linux, 223, 226
    - in NetWare, 244, 246
    - reports by, 56–57
  - Queensland University of Technology's Information Security Research Centre, 183
- *R* •
- radio signals, weak, 173
  - rainbow table password attacks
    - described, 95–96
    - ophcrack tool, 98–100
  - RainbowCrack Online, cracking Windows passwords with, 101
  - RainbowCrack password cracking software, 92
  - random logins, 94
  - random number passwords, 98
  - RAS (remote access servers), 115–116
  - r-commands, BSD
    - disabling, 232–233
    - files, accessing without password, 232
    - services, discerning, 225
  - Rconj version of rconsole, 251
  - rconsole (Remote Console) program
    - alternatives, 251
    - NetWare password cracking, 244
    - passwords, cracking, 249–250
    - securing, 251
  - Real-time Transport Protocol (RTP), 288
  - Red Hat Linux systems, updating, 241
  - red team, 36

- Registry, Windows
    - null session hacks, avoiding, 206–207, 208
    - passwords, finding, 111
    - RPC server, caution against disabling, 201
  - remote access servers (RAS), 115–116
  - remote command prompt, finding on vulnerable server, 212–215
  - Remote Console program (rconsole)
    - alternatives, 251
    - NetWare password cracking, 244
    - passwords, cracking, 249–250
    - securing, 251
  - remote procedure call. *See* RPC
  - remote-mounting capability, Linux, 235
  - reports
    - goals, 19
    - highlighting important areas in documentation, 327–329
    - methods, 330–332
    - prioritizing vulnerabilities, 329–330
    - QualysGuard vulnerability assessment tool, 56–57
    - turning into action, 333–334
  - residential phones, 68
  - resources
    - databases, 367–368
    - management, 364–365
    - messaging, 361–362
    - network, 362–363
    - password cracking, 364
    - risk analysis, 366
    - security education, 366
    - security standards, 365
    - source code analysis, 365
    - storage, 366
    - threat modeling, 366
    - VoIP, 366–367
    - war dialing, 367
    - Web applications, 367–368
    - Windows, 368–369
    - wireless network, 369–370
  - results, evaluating, 22
  - reusing passwords, 88
  - reverse social engineering, 70
  - review, need for, 22
  - RFprotect Mobile wireless device scan, 176–177
  - Rhoades, David (information security expert), 117
  - .rhosts file, Linux, 232
  - risk analysis resources, 366
  - risks, contingency plans and, 18
  - robots.txt file, searching for, 299
  - rogue insiders
    - attack style, 31
    - defined, 11
    - motivations, 29
    - problem with, 24
  - root, applications running as, 237
  - routers, blocking malformed traffic, 159
  - RPC (remote procedure call)
    - buffer overflow attacks, 237
    - described, 199–200
    - enumeration, 200–201
    - Linux, disabling, 227
  - Rpcdump tool, 193, 200
  - r-services, Linux, 225, 228
  - RTP (Real-time Transport Protocol), 288
- S ●
- SAM database, 112
  - Sam Spade for Windows scanner
    - obtaining, 130
    - SMTP Relay check, 274
  - sample cases
    - e-mail attacks, 267
    - network infrastructure, 128
    - passwords, 87
    - social engineering, 63
    - WLANs, 163
  - scanning systems
    - hosts, 52
    - modems and open ports, 53
  - screen captures, 46
  - screens, locking, 83
  - script kiddies, 26, 30
  - search-engine information, social engineering and, 66–67
  - Secure Shell (SSH), 172
  - Securities and Exchange Commission (SEC) filings, 66
  - security by obscurity, 88, 322
  - security desk, 63
  - security education resources, 366
  - security, physical
    - assessing, 76–78
    - attacks, 14
    - building infrastructure, 78–79
    - Linux, 238–239
    - network analyzers, 152
    - network components and computers, 81–84
    - office design and usage, 80–81
    - utilities, 79–80
    - vulnerabilities, 75–76
    - wireless network, walking perimeter, 176

- security standards, 365
- security training, 73
- security-aware mindset, instilling, 343–344
- sendmail vulnerabilities, 228
- Server Message Block (SMB), 197
- servers. *See also* Web server
  - AppDetective database server tool, 320–321
  - database, finding on network, 317–318
  - e-mail, 281
  - information, gathering, 247
  - NetWare, 245, 251–252
  - Oracle, 317
  - RPC, caution against disabling, 201
  - version, 54–55
  - Web, 231, 302
  - Windows NT security example, 337
- service set identifier (SSID), 167
- Session Initiation Protocol (SIP), 288, 290
- SetGID file permission, Linux
  - automatic testing, 237
  - manual testing, 236
  - vulnerabilities, 235
- share permissions
  - testing, 209–210
  - Windows defaults, 208–209
  - Windows security flaws, 208–210
- shares, hidden
  - null session attach method, 201
  - security of, 199
- shoulder surfing password cracks, 85, 90
- shredding, 67
- signing in
  - input fields in Web applications, targeting, 303
  - NetWare, 245, 256–257
  - random, 94
  - return messages, 298–299
- Sima, Caleb (application security expert), 295
- Simple Mail Transport Protocol. *See* SMTP
- single number, war dialing, 122
- SIP (Session Initiation Protocol), 288, 290
- SiteDigger Web application tool, 301
- SiVuS VoIP network scanning tool, 288–290
- Slackware Linux system, updating, 242
- small services, TCP and UDP ports, 223
- SMB (Server Message Block), 197
- S/MIME e-mail encryption, 280
- SMTP (Simple Mail Transport Protocol)
  - attacks, 272–280
  - banner, displayed, 271
  - described, 15
  - relay, checking with telnet, 275–277
  - Sam Spade for Windows Relay check, 274
  - Smurf DoS attack, 150, 158
  - sniffer. *See* network analyzers
  - Sniffer Network Analyzer, 128
  - snmp daemon, disabling, 231
  - SNMP scanning
    - countermeasures, 141
    - described, 139
    - vulnerabilities, 140–141
  - social engineering
    - attackers' use of, 64
    - case study, 63
    - caution, 62
    - countermeasures, 72–74
    - described, 14
    - examples, 61–62
    - exploiting relationship, 69–72
    - fishing for information, 66–68
    - implications, 65
    - outsider, benefits of hiring, 64
    - passwords, cracking, 89–90
    - trust, building, 68–69
  - software
    - attacks, 15
    - IM, rogue, 284
    - password cracking, 91–93
    - passwords, blocking storage, 110
    - P2P, barring, 285
    - random, protecting against keystroke-logging tools, 104
    - test choices, 37
    - version, 54–55
  - source code analysis resources, 365
  - specialized attacks, 15
  - SPI Proxy tool, 308
  - spidering, Web site, 294, 300
  - Spies Among Us: How to Stop the Spies, Terrorists, Hackers, and Criminals You Don't Even Know You Encounter Every Day* (Winkler), 63
  - SQL injection, 304–307
  - SQLPing2 database server tool, 318
  - SSH (Secure Shell), 172
  - SSID (service set identifier)
    - local wireless airwaves, 167
    - man-in-the-middle attacks, 168
    - rogue wireless devices, 173, 174
    - wireless NIC configuration, 182
  - SSL/TLS (Secure Sockets Layer/Transport Layer Security), 172
  - staff. *See also* rogue insiders
    - fake, 62
    - former, disabling e-mail accounts, 267
    - impersonating, 70
    - Internet acceptable usage policy, 313
    - security-aware mindset, instilling, 343–344

- standards, testing
  - assumptions, 42–43
  - blind versus knowledge assessments, 41
  - location, 41–42
  - specific tests, 40–41
  - timing, 39–40
  - vulnerabilities, reacting to, 42
- storage media, 68, 234
- storage resources, 268, 366
- Sunbelt Network Security Inspector
  - vulnerability assessment tool, 131
- SuperScan tool
  - described, 192
  - Linux, using, 222, 224
  - NetWare, using, 244, 246
  - obtaining, 130
  - TCP port scans, 135–136, 194
- support personal, false, 61
- SUSE Linux system, updating, 242
- switches
  - firewalls, 106
  - Google, 48
- SYN floods, 158
- SYN Stealth scan, Nmap, 136
- SYSKEY utility, 112
- system
  - choosing, 36–38
  - IM software configuration, 285
  - specific, limiting test to, 18
- system scanning, Windows
  - countermeasures, 196
  - fingerprinting, blocking, 196
  - information, protecting, 196
  - testing, 194–196

• T •

- tailgating employees, 77
- tarpitting e-mail messages, 270
- TCP ports
  - blocking, 206
  - compromised, 197
  - NetWare, 255
  - open, finding in Windows, 194
  - scans, 135
  - small services, 223
  - Windows limitation, 193
- TCP Wrappers, 231
- tcpcon, NetWare, 255
- TCP/IP
  - ARP spoofing problem, 153
  - Novell NetWare parameters, 261
  - scanning, poking, and prodding systems, 131

- TCP/IP For Dummies* (Leiden and Wilensky), 127
- techie talk, avoiding, 350
- technology, social engineering deceit, 70–72
- telephone numbers
  - checking for war dialing, 124–125
  - protecting from war dialing, 125
- telephone system
  - fishing for information, 68
  - war dialing vulnerabilities, 116
- telnet
  - banner grabbing, 142
  - disabling, 231
  - Linux vulnerabilities, 228
  - SMTP relay, checking, 275–277
- Temporal Key Integrity Protocol (TKIP)
  - encryption system, 172
- testing
  - application service providers, notifying
    - about, 39
  - applications, 37
  - client notification, 36
  - correct systems, 355
  - DoS attacks caused by, 16, 40–41, 44, 158
  - need to perform multiple times, 354
  - outsourced, supervising, 356
  - realistic attitude toward, 354
  - share permissions, 209–210
  - timeline, 18
  - ToneLoc war dialing software, 122–123
  - unsecured login mechanisms, 296–298
- testing standards
  - assumptions, 42–43
  - blind versus knowledge assessments, 41
  - location, 41–42
  - specific tests, 40–41
  - timing, 39–40
  - vulnerabilities, reacting to, 42
- text messaging
  - DoS attacks, 281
  - rogue software, 284
  - system configuration, 285
  - traffic, detecting, 285
  - user behavior, 285
  - vulnerabilities, 281–284
- TFN (Trinoo and Tribe Flood Network)
  - attacks, 158
- THC-Scan war dialing software
  - modem problems, 119–120
  - obtaining, 119
- TheTrainingCo., 77
- threat modeling resources, 366

- Tiger local system security setting tool, 223, 240
- tiger team, 36
- timeline
  - notifying, 39–40
  - testing, 18
- time-memory trade-offs, 87
- TKIP (Temporal Key Integrity Protocol)
  - encryption system, 172
- ToneLoc war dialing software
  - configuring, 121–122
  - modem problems, 119–120
  - obtaining, 119
  - testing, 122–123
- tools
  - capabilities and limitations, 44
  - correct, using, 355
  - multiple tests, controlling, 17
  - suggested, 43
  - Windows instability and, 191
- traffic
  - IM, detecting, 285
  - port scanner restriction, 138–139
- Traffic IQ Pro tool, testing firewalls with, 145
- training tools, listed, 357
- traversal, directory
  - countermeasures, 302
  - crawlers, 300
  - filenames, 299–300
  - Google, 300–301
  - robots.txt file, searching for, 299
- Trinoo and Tribe Flood Network (TFN)
  - attacks, 158
- Trojan horses
  - keylogger, 71
  - password-cracking, 110
- trust, building, 68–69
- trustworthiness, 16

## • u •

- UDP ports
  - compromised, 197
  - NetWare, 255
  - Nmap scan, 136
  - small services, 223
- unauthenticated enumeration, 197–198

- UNIX
  - e-mail delivery vulnerability, 269
  - MAC address spoofing, 156, 178
  - network analyzer, detecting, 153
  - password countermeasures, 112
  - password storage files, 93
  - passwords, creating with John the Ripper, 97–98
  - telnet port, finding, 142
  - WLAN security tools, 162–164
- unlimited attacks, planning, 41
- unsecured login mechanisms
  - countermeasures, 298–299
  - testing, 296–298
- Web Brute account-hacking tool, 298
- unsolicited e-mails and attachments, 280
- updated programs, testing, 40
- upper management
  - ally and sponsor, cultivating, 347
  - benefits, demonstrating, 349
  - business goals, supporting, 349
  - costs, demonstrating, 348
  - credibility, establishing, 350
  - don't blow things out of proportion, 348
  - flexibility and adaptability, 351
  - techie talk, avoiding, 350
  - understanding business, 349–350
  - value, demonstrating, 350–351
- URL
  - code-injection and SQL injection attacks, 304–307
  - file manipulation, 295, 297
  - login return messages, 298–299
- URL filter bypassing
  - countermeasure, 315
  - described, 313–315
- Usenet Groups, Google, 51
- user accounts
  - lockouts during password cracks, 92
  - weak passwords, 107
- user IDs
  - cracking, 110
  - cross-site scripting, 309
  - memory attacks, 310–311
- username, 296
- users
  - e-mail storage space, limiting, 269
  - IM, 285
  - Internet acceptable usage policy, 313

- organizational password vulnerabilities, 86, 88
- P2P software, barring, 285
- storing passwords, 108–109
- utilities
  - attacks, 79
  - countermeasures, 80
  - physical security, 79–80

## • U •

- vendors, false, 61
- vigilance, false sense of, 41
- virtual local area network (VLAN), 287
- Virtual Network Computing (VNC), 82
- virtual private networks (VPNs), 12
- Vision security tool, 191
- VLAD the Scanner security settings tool, 223, 240–241
- VLAN (virtual local area network), 287
- VNC (Virtual Network Computing), 82
- voice mail, phone system vulnerability, 116
- Voice over IP. *See* VoIP
- voice traffic, capturing and recording, 290–292
- VoIP (Voice over IP)
  - countermeasures, 292
  - resources, 366–367
  - specialized attacks, 15
  - voice traffic, capturing and recording, 290–292
  - vulnerabilities, 286–290
- VoIP For Dummies* (Kelly), 286
- VPNs (virtual private networks), 12
- VRFY command, SMTP, 274

## • W •

- Walksam null session configuration tool, 205
- WANRemote tool, 150
- war dialing
  - configuration utility, 121–122
  - information gathering, 118
  - from inside, 120
  - legal issues, 117
  - methods, 116–118
  - modem hardware, choosing, 119–120
  - modem safety, 115–116

- operating modems, 125–126
- phone numbers, protecting, 125
- resources, 367
- rooting through systems, 124–125
- scanning for modems and open ports, 53
- secure modem placement, 126
- software tools, 119
- telephone system vulnerabilities, 116
- testing, 122–124
- weak authentication password cracks, 90–91
- Web
  - acceptable usage policy, 313
  - access, assessing in NetWare, 245
  - fishing for information, 66–67
  - Linux services, 223
  - public information, gathering, 47–48
  - war dialing numbers, 118
- Web applications
  - assessment tools, 19
  - case study, 295
  - default script attacks, 312–313
  - described, 293, 294, 296
  - directory traversal, 299–302
  - firewalls, 323–324
  - general security scans, 315–316
  - input filtering attacks, 303–310
  - memory attacks, 310–311
  - obscurity, minimizing risks through, 322–323
  - resources, 367–368
  - URL filter bypassing, 313–315
- Web crawling, 48–49
- Web page, defacing, 29
- Web server
  - directory traversal countermeasures, 302
  - disabling, 231
- WebInspect
  - Web application testing tool, 294
  - Web Brute Web application tool, 298
- WEP (Wired Equivalent Privacy) encryption protocol, 168–172, 186
- Whois lookups
  - information, using, 52
  - mapping network, 49–51
  - war dialing information, 118
- Wi-Fi Protected Access (WPA), 172–173
- WIGLE database, viewing MAC address on, 166

- WildPackets EtherPeek network analysis program, 147
- WildPackets EtherPeek scanner, 131
- Wilensky, Marshall (*TCP/IP For Dummies*), 127
- Windows (Microsoft)
  - all-in-one assessment tools, 192
  - authenticated scans, 218–220
  - availability of hacking and testing tools, 190–191
  - CORE IMPACT testing, 193, 215–217
  - essential tools, 191
  - free Microsoft tools, 191–192
  - hardcore vulnerability exploitation, 210–217
  - MAC address spoofing, 156–157
  - NetBIOS, 196–199
  - network analyzer, detecting, 153
  - null sessions, 201–208
  - password countermeasures, 111–112
  - password cracking method, 87
  - password storage files, 93
  - passwords, cracking with `pwdump3` and John the Ripper, 96–97
  - prevalence of, 189–190
  - resources, 368–369
  - share permissions, 208–210
  - system scanning, 194–196
  - task-specific tools, 192–193
  - telnet port, finding, 142
  - version shown, 193
  - vulnerabilities, 190
  - WLAN security tools, 164, 180
- Windows 2000 (Microsoft)
  - default share permissions, 208–209
  - NetBIOS security settings, 207–208
- Windows 2003 Server/XP (Microsoft) default share permissions, 209
- Windows Explorer (Microsoft), 219
- Windows NT (Microsoft)
  - default share permissions, 208–209
  - NetBIOS security settings, 208
  - server security example, 337
- Windows Resource Kits (Microsoft), 191–192
- Windows Vista (Microsoft), 211
- Winfo command-line tool, 203–204
- WinHex tool
  - active memory, searching, 310
  - described, 110
- Winker, Ira (*Spies Among Us: How to Stop the Spies, Terrorists, Hackers, and Criminals You Don't Even Know You Encounter Every Day*), 63
- WinNuke, 158
- Wired Equivalent Privacy (WEP) encryption protocol, 168–172, 186
- wireless cards, 164
- Wireless Local Area Networks. *See* WLANs
- wireless NIC configuration, 182
- Wireless Vulnerabilities and Exploits site, 162
- WLANs (Wireless Local Area Networks)
  - attacks, 168
  - case study, 163
  - described, 161–162
  - encrypted traffic attacks, 168
  - infrastructure, 73
  - Linux security tools, 163–164, 180
  - local airwaves, scanning, 167
  - resources, 369–370
  - tools, 162–165
  - walking perimeter, 176
  - worldwide recognition, checking, 165–166
- word lists, 358
- workers. *See also* rogue insiders
  - fake, 62
  - former, disabling e-mail accounts, 267
  - impersonating, 70
  - Internet acceptable usage policy, 313
  - security-aware mindset, instilling, 343–344
- working ethically, 16
- workstation bandwidth usage, 150–151
- WPA Cracker tool, 171
- WPA (Wi-Fi Protected Access), 172–173



- `xinetd.conf`, Linux file, 230
- Xmas Tree scan, Nmap, 136
- XSS (cross-site scripting), 309