

Index

• Symbols and Numerics •

^M character ending text files, 49
802 work group, 9
802.11 standards
 complexities of, 14
 DoS attacks and, 226–227
 802.11i (WPA2), 10–11, 275–277, 278
 encryption features, 255–257
 frame authentication lacking in, 226
 management-frame attacks exploiting, 209–211
 message integrity protection and, 256–257
 message privacy protection and, 255–256
 network-level attack vulnerabilities, 195–196
 origin of name, 9
 reference guides, 305
 RF jamming and, 229
 security vulnerabilities, 10–11
802.1X authentication, 288–290
40-bit encryption, 256, 258–259
104-bit (128-bit) encryption, 256, 258
10pht's AntiSniff, 130

• A •

access points. *See* APs
acronyms, glossary of, 341–346
active traffic injection attacks on WEP, 263–264
ACU client (Cisco), 289
Address Resolution Protocol. *See* ARP
Advanced Encryption Standard (AES), 278
AEGIS 802.1X client software (Meetinghouse Data), 289
AEGIS RADIUS server (Meetinghouse Data), 289
Aerosol wardriving software, 173
AES (Advanced Encryption Standard), 278
aircrack WEP-key cracking tool, 269–273
AirDefense IDS system, 80
AirDefense Mobile program, 219
Aireplay traffic injection tool, 263
AirJack packet injection tool, 240

Airjack suite MITM software, 209
AirMagnet
 Laptop Analyzer, 219–220
 packet analyzer, 119
 wardriving software, 173
Aironet 340 antenna (Cisco), 94
AiroPeek and AiroPeek NX sniffers
 deauthentication attack viewed in, 247–248
 described, 35, 218
 detecting network anomalies with, 130
 Expert analysis, 189–190
 finding unauthorized equipment with, 188–191
 overview, 114–115
 Peer Map creation with, 188–189
 Security Audit Template.ctf, 189
 as wardriving software, 173
 Web site, 35
AirScanner Mobile Sniffer freeware, 119
Airscanner wardriving software, 173
AirSnare WIDS program, 296
AirSnarf program, 178
AirSnort WEP-key cracking tool, 267–269
AirTraf sniffer, 114
airwaves. *See* controlling radio signals;
 determining network bounds;
 RF jamming
Amap application mapping tool, 103, 105
American Registry for Internet Numbers (ARIN), 35
Anger PPTP cracker, 295
Anritsu spectrum analyzer, 90
antennae
 buying wireless NICs and, 59
 cantennae, yagi-style, or wave guide, 60, 62, 92–93
 choosing, 304
 dipole, 93
 directional versus omnidirectional, 60–61
 DoS attacks and, 252
 further information, 62
 omnidirectional, 13, 60–61, 94
 parabolic grid, 92
 radiation patterns, 91–94
 signal strength adjustment, 94–95
 Web sites, 335
AntiSniff (10pht), 130

Anritsu RF generators, 64
 anwrap LEAP-cracking tool, 293
 AP overloading
 association and authentication attacks, 234–240
 open authentication phases and, 234–235
 packet-injection tools for, 235–237, 240
 testing for, 235–237
 unintentional, 240–241
 AP Scanner wardriving software, 173
 application mapping (Linux), 105
 APs (access points). *See also* AP overloading;
 SSIDs (service-set identifiers);
 unauthorized equipment
 common client vulnerabilities, 104–105
 default settings, 76–77
 defined, 11
 enumeration of SNMP on, 214–216
 evil twins, 286
 fake (honeypots), 74, 175–176
 rogue APs, 178
 searching the Internet for yours, 34–35, 71
 signal strength adjustment, 94–95
 WEP encryption settings, 258–259
 on Wi-Fi databases, 34–35
 APsniff wardriving software, 173
 ARIN (American Registry for Internet Numbers), 35
 ARP (Address Resolution Protocol)
 ARP-poisoning attacks, 209, 211–213
 Network Scanner for ARP lookups, 100
 arping tool, 126
 Arpmim MITM software, 209
 arpmim (LBL), 129
The Art of War (Sun Tzu), 155
 asleap LEAP-cracking tool, 291–292
 attenuators, 94
 Auditor Linux, 119
 Auditor Security Collection (Knoppix), 236, 274, 297–299
 authentication
 association and authentication attacks, 234–240
 Auditor Security Collection for testing, 297–299
 countermeasures, 293–299
 cracking LEAP, 290–293
 deauthentication attacks, 242–250
 defined, 281
 EAP (Extensible Authentication Protocol), 284–288, 297
 802.11 methods, 282–283
 802.1X implementation, 288–290

frame authentication lacking in 802.11, 226
 MAC (message authentication code), 257
 open-system, 282
 shared-key, 282–284
 states of, 281–282
 VPNs for, 295–296
 WDMZ setup, 297
 WPA for, 293–294
 WPA2 for, 294–295

• B •

bandwidth, limiting, 253
 baseline usage, establishing, 251
 Basic Service Set (BSS) configuration, 179
 Basic SSID (BSSID), 132. *See also* MAC
 (media-access control) addresses
 beacon packets of unauthorized systems, 182
 Beaver, Kevin
 Hacking For Dummies, 2, 14, 19, 33, 56, 78, 107, 111
 Hacking Wireless Networks For Dummies, 1–6
 Bluesocket IDS system, 80
 Bochs emulation software, 46
 bounds of network. *See* determining network bounds
 broadcasts
 beacon, increasing intervals, 175
 SSID, disabling, 13, 129
 BSD-Airtools wardriving software, 173
 BSS (Basic Service Set) configuration, 179
 BSSID (Basic SSID), 132. *See also* MAC (media-access control) addresses

• C •

cables, 304
 Cain & Abel password recovery tool, 120–124
 candy security, 68
 antennae, 60, 62
 Capsa packet analyzer, 119
 caret-M (^M) character ending text files, 49
 Casio MIPS PDA, 44
 CD distributions of Linux, 55–56
 CENiffer packet analyzer, 119
 CERT (Computer Emergency Response Team), 27
 certifications, 327
 Chappell, Laura (troubleshooting book author), 130
 Chase, Kate (*Norton All-in-One Desk Reference For Dummies*), 46

- Cheops-ng network-mapping tool, 36
- chopchop WEP cracker, 274
- Cisco
- ACU client, 289
 - Aironet 340 antenna, 94
 - SecureACS, 288
- Clear Channel Assessment (Queensland) attack, 217, 229
- Client Manager software (ORiNOCO), 184–185
- client software for 802.1X, 289
- clients. *See* hacking wireless clients
- cloaked SSIDs, 132
- Cobb, Chey (*Network Security For Dummies*), 40, 111
- Cobit standard, 27
- Common Vulnerabilities and Exposures database, 41, 110
- CommView for WiFi sniffer
- described, 218
 - detecting network anomalies with, 130
 - discovering default settings with, 115–117
 - Packet Generator tool, 236–240
 - for testing deauthentication attacks, 245–247
- complexities of wireless networks, 14–15
- Computer Emergency Response Team (CERT), 27
- configuring
- Kismet stumbling tool, 160–161
 - MiniStumbler tool, 171–172
 - NetStumbler tool, 134–141
 - private parameters for wireless interface, 85
 - wireless interface with `iwconfig`, 82–85
- containing the airwaves. *See* controlling radio signals; determining network bounds
- controlling radio signals. *See also* determining network bounds
- antenna type and, 91–94, 252
 - checking for unauthorized users, 90–91
 - DoS attacks and, 251–253
 - physical security countermeasures, 90–95
 - RF shielding for, 252
 - signal strength adjustment, 94–95
- convenience versus security, 69
- Cool Linux CD distribution, 56
- countermeasures
- for authentication, 293–299
 - for default settings, 128–130
 - for DoS attacks, 251–254
 - for encryption attacks (home), 274–277
 - for encryption attacks (organization), 277–278
 - for human vulnerabilities, 78–80
 - for network-level attacks, 222–223
 - for null sessions (Windows), 111–112
 - for physical security, 90–95
 - for unauthorized equipment, 193–194
 - for wardriving, 174–176
 - for wireless clients, 111–112
- CoWPAtty WPA-PSK-auditing tool, 294
- cracking WEP keys
- aircrack for, 269–273
 - AirSnort for, 267–269
 - requirements for, 264–265
 - WEPcrack for, 265–267
 - WepLab for, 273–274
- CRC (Cyclic Redundancy Check), 256–257, 260
- Cyghwin emulation software, 46–52
- D •
- Damn Small Linux (DSL), 56
- data analyzers. *See* sniffers (network analyzers)
- data line monitors. *See* sniffers (network analyzers)
- databases
- of vulnerabilities, 41, 332
 - Wi-Fi, footprinting using, 34–35
- Davis, Peter
- Hacking Wireless Networks For Dummies*, 1–6
 - Wireless Networks For Dummies*, 15, 40, 57, 62, 146, 280, 305
- deauthentication attacks
- CommView for WiFi for testing, 245–247
 - FATA-jack for, 242, 249
 - havoc from, 249, 250
 - overview, 242–244
 - viewed in AiroPeek NX, 247–248
- Deceit PPTP cracker, 295
- default settings
- collecting information, 113–120
 - countermeasures, 128–130
 - cracking passwords, 120–125
 - gathering IP addresses, 125–126
 - gathering SSIDs, 126–128
 - human vulnerabilities and, 76–77
 - Internet resources for, 77
 - testing for, 77
- DeLorme mapping software, 63
- Delphi Imaging Geographic Lookup Engine (DiGLE), 151–152
- denial-of-service attacks. *See* DoS attacks

- determining network bounds
 - Linux Wireless Extensions and, 81–82
 - Linux Wireless Tools for, 81–87
 - other link monitors for, 88–90
 - Wavemon for, 87
 - Wimon for, 88
 - Wmap for, 88
 - Wscan for, 88
 - XNetworkStrength for, 88
 - Devine, Christopher (aircrack programmer), 269
 - dictionary files and word lists, 339
 - DiGLE (Delphi Imaging Geographic Lookup Engine), 151–152
 - dipole antennae, 93
 - directional versus omnidirectional antennae, 60–61
 - disabling
 - probe responses, 175
 - SSID broadcasts, 13, 129
 - disassociation attacks, 242
 - displaying
 - statistics from wireless nodes with *iwspy*, 87
 - wireless interface details with *iwlist*, 86–87
 - documentation. *See* record keeping
 - domain name, looking up, 35
 - DoS (denial-of-service) attacks. *See also specific types*
 - AP overloading, 234–241
 - attacking back, 254
 - against client systems, 241–250
 - containing radio waves and, 251–253
 - countermeasures, 251–254
 - dangers of testing for, 227
 - deauthentication attacks, 242–250
 - defined, 226
 - demanding fixes for, 254
 - difficulty of preventing, 228–229
 - disassociation attacks, 242
 - disruption created by, 227
 - ease of carrying out, 228
 - 802.11 vulnerabilities and, 226–227
 - establishing baseline usage, 251
 - IDS/IPS systems and, 253–254
 - limiting bandwidth and, 253
 - MITM (man-in-the middle) attacks, 208–211
 - motivations for, 226
 - network monitoring systems and, 253
 - physical insecurities and, 250
 - power-saving features and, 228
 - Queensland attack, 217, 229
 - RF jamming, 63–64, 229–233
 - scenario demonstrating, 225
 - types of attacks, 227–228
 - DOSEMU emulation software, 46
 - DSL (Damn Small Linux), 56
 - dsniff* tools, 124–125, 209
 - dstumbler wardriving software, 173
 - dual-boot workstations, 45–46
 - Dwepcrack WEP cracker, 274
- E •
- EAP (Extensible Authentication Protocol)
 - components, 284
 - EAP-FAST, 287
 - EAP-MD5, 285–286
 - EAP-TLS, 287
 - EAP-TTLS, 288
 - Extended EAP in WPA, 285
 - LEAP, 286–287
 - overview, 284–285
 - PEAP, 286
 - selecting the right version, 297
 - ECPA (Electronic Communications Privacy Act), 318
 - education about human vulnerabilities, 79–80
 - effective radiated power (ERP), 64
 - 802 work group, 9
 - 802.11 standards
 - complexities of, 14
 - DoS attacks and, 226–227
 - 802.11i (WPA2), 10–11, 275–278
 - encryption features, 255–257
 - frame authentication lacking in, 226
 - implementing 802.1X authentication, 288–290
 - management-frame attacks exploiting, 209–211
 - message integrity protection and, 256–257
 - message privacy protection and, 255–256
 - network-level attack vulnerabilities, 195–196
 - origin of name, 9
 - reference guides, 305
 - RF jamming and, 229
 - security vulnerabilities, 10–11
 - 802.1X authentication, 288–290
 - Electronic Communications Privacy Act (ECPA), 318
 - e-mail, social engineering tests using, 73
 - empirical method, 24
 - emulation software
 - Cygwin setup, 47–52
 - for emulating Linux on Windows, 46–55
 - for emulating Windows on Mac OS, 47

- for emulating Windows or DOS on Linux, 46
 - overview, 46–47
 - VMware setup, 52–55
 - Web sites, 46, 333
 - enabling MAC address controls, 198
 - encryption. *See also specific types*
 - attacking WEP, 263–264
 - countermeasures against attacks (home), 274–277
 - countermeasures against attacks (organization), 277–278
 - cracking WEP keys, 264–274
 - cryptographic protection lacking with WEP, 260
 - 802.11 features, 255–257
 - key size and security, 256
 - message integrity protection and, 256–257
 - message privacy protection and, 255–256
 - not a panacea, 255
 - using, 257–259
 - VPN protocols, 279–280
 - WEP vulnerabilities, 78, 256, 259–261
 - WPA vulnerabilities, 11, 277
 - WPA2 vulnerabilities, 11
 - enumeration
 - defined, 37
 - performing, 37–38
 - of SNMP on APs, 214–216
 - for Windows systems, 103, 108–109
 - ERP (effective radiated power), 64
 - ESS (Extended Service Set) configuration, 179, 180
 - essid_jack SSID reporting tool, 127, 188
 - Ethereal sniffer, 113–114, 157, 219
 - ethical hacking. *See also hacking wireless clients*
 - breaking the law, avoiding, 316–319
 - certifications, 327
 - defined, 1, 10
 - ethical defined, 22
 - following up, 316, 321–324
 - getting written permission for, 21–22, 312–313
 - involving others in, 308
 - local wireless groups, 329–331
 - other terms for, 1, 10
 - over-penetrating live networks, 314
 - penetration testing versus, 1, 10
 - planning for, 15–16, 307–308
 - repeated testing needed for, 11
 - reporting all findings, 25, 314–316
 - rules for, 319
 - standards, 26–30
 - Ten Commandments, 19–25
 - tools for, 16–17, 303–305, 313–314
 - using a methodology, 308–309
 - using data improperly, 314
 - vulnerability testing versus, 1, 10
 - Ettercap tools, 209, 212–213, 295
 - evil twins, 286
 - Extended Service Set (ESS) configuration, 179–180
 - Extensible Authentication Protocol. *See* EAP
 - extranet VPNs, 279
- F ●**
- Fake AP software, 176
 - fake APs (honeypots), 74, 175–176
 - FATA-jack program, 242, 249
 - file2air packet injection tool, 240
 - filters
 - for MAC addresses, 13
 - in NetStumbler, 146–147
 - firmware vulnerabilities, testing, 129
 - following up
 - documenting lessons learned, 323
 - failing, 316
 - keeping up with security issues, 324
 - monitoring your airwaves, 324
 - obtaining sign-off, 322–323
 - organizing and prioritizing results, 321–322
 - plugging holes you find, 323
 - practicing with your tools, 324
 - preparing a professional report, 322
 - repeating tests, 323
 - retesting if needed, 322
 - footprinting
 - defined, 32
 - searching Wi-Fi databases, 34–35
 - searching with Google, 33–34
 - 40-bit encryption, 256, 258–259
 - Foundstone
 - query tool for Google, 34, 72
 - SiteDigger tool, 72
 - SuperScan port scanner, 37–38, 100–101
 - fping network-mapping tool, 36
 - freeRADIUS server, 289
 - Funk Software
 - Odyssey 802.1X client software, 289
 - Steel Belted RADIUS, 289

• G •

- gathering public information. *See* footprinting
- Getif utility, 215, 216
- GFI LANguard Network Security Scanner tool, 40, 103, 108–109, 214
- Global Gadget signal generator, 232
- global positioning system. *See* GPS
- glossary of acronyms, 341–346
- GNU/Debian Linux CD distribution, 56
- goal setting, 20–21, 24
- Google
 - as essential hacking tool, 305
 - footprinting using, 33–34
 - Foundstone query tool for, 34, 72
 - further information for ethical hacking with, 72
 - passive tests for social engineering, 71–72
 - security issue information from, 41
- GPS (global positioning system)
 - Kismet GPSD installation and options, 159–160
 - NetStumbler options, 138–139
 - overview, 62–63
 - receiver, 304
- GpsDrive GPS mapping software, 157
- Gulpit sniffer, 117–119
- gWireless wardriving software, 173

• H •

- hackers (unethical), 12–14
- Hacking For Dummies* (Beaver)
 - downloading passwords chapter, 78, 107
 - Ethical Hacking Commandments in, 19
 - ethical hacking methodology in, 56
 - information-security assessment in, 33
 - for insight into hackers, 14
 - as inspiration for this book, 2
 - operating system security information in, 111
- hacking wireless clients
 - application mapping (Linux), 105
 - for common application weaknesses, 104–105
 - countermeasures, 111–112
 - discovering WEP keys, 109–110
 - information available from clients, 98
 - looking for general vulnerabilities, 103–109
 - overview, 97–98
 - port scanning, 99–102
 - security dangers of clients, 98–99

- steps for, 99
- tools for, 100, 102–103
- VPNMonitor for, 102–103
- for Windows null sessions, 106–109
- Hacking Wireless Networks For Dummies* (Beaver and Davis)
 - assumptions about the reader, 3
 - icons in margins, 5
 - organization, 3–5
 - overview, 1–2
 - using, 2–3, 6
- hardware. *See also* unauthorized equipment; *specific kinds*
 - antennae, 13, 59–62, 91–95, 252, 304, 335
 - attenuators, 94
 - GPS, 62–64, 138–139, 159–160, 304
 - PDA's, 44
 - portables or laptops, 44–45, 75–76, 155–156, 178, 303
 - signal generators, 232–233
 - transceivers (wireless NICs), 57–59, 109–110, 199–200, 304, 309–312
- harm, doing no, 23–24
- Hermes chipset, 57–58
- Hewlett-Packard PDA's, 44
- Honeyd-WIN32 honeypot software, 176
- honeypots (fake APs), 74, 175–176
- HP RF generators, 64
- human vulnerabilities. *See also specific kinds*
 - candy security and, 68
 - countermeasures for, 78–80
 - dangers of ignoring, 68
 - default settings, 76–77
 - ground-level security and, 69, 80
 - overlooking, mindset and, 69–70
 - overview, 67–68
 - security versus convenience and usability, 69
 - social engineering, 17, 67, 70–74
 - training and education for preventing, 79–80
 - unauthorized equipment, 69, 74–76
 - weak passwords, 77–78
 - wireless security policy and, 78–79

• I •

- IAS (Internet Authentication Service) of Microsoft, 288
- IBSS (Independent Basic Service Set) configuration, 180–181
- icons in margins of this book, 5
- ICV (integrity check value), 257

- IDS/IPS (intrusion-detection/prevention system), 80, 253–254, 336–337
- IEEE (Institute of Electrical and Electronics Engineers) standards. *See also* 802.11 standards
 - 802 work group for, 9
 - 802.11i (WPA2), 10–11
 - Organizationally Unique Identifiers (OUI), 144
 - Web site, 328–329
- `ifconfig` utility (Linux), 199
- implementing a testing methodology
 - determining what services are running, 39
 - formal procedures overview, 31
 - gathering public information, 32–35
 - logging what you do, 32
 - mapping your network, 35–37
 - not using a methodology, avoiding, 308–309
 - scanning your systems, 37–38
 - system-penetration phase, 41–42
 - vulnerability assessment, 39–41
- Independent Basic Service Set (IBSS)
 - configuration, 180–181
- Information Systems Security Assessment Framework (ISSAF) standard, 27–28
- installing
 - AirSnort WEP-key cracking tool, 268–269
 - Cygin emulation software, 47–51
 - Kismet GPSD, 159–160
 - Kismet stumbling tool, 157–159
 - MiniStumbler tool, 170–171
 - NetStumbler tool, 133
 - VMware emulation software, 52–53
- Institute for Security and Open Methodologies (ISECOM), 28–29
- Institute of Electrical and Electronics Engineers. *See* IEEE
- integrity check value (ICV), 257
- integrity of messages
 - CRC check for, 256–257, 260
 - cryptographic protection lacking with WEP, 260
 - 802.11 standard and, 256–257, 260
 - protecting, 256–257
- interference. *See* RF jamming
- International Organization for Standardization (ISO), 26
- Internet Authentication Service (IAS) of Microsoft, 288
- Internet resources
 - AiroPeek sniffer, 115
 - AirSnare WIDS program, 296
 - AirSnarf program, 178
 - AirTraf sniffer, 114
 - antennae, 335
 - `arping` tool, 126
 - attenuators, 94
 - Auditor Linux, 119
 - Auditor Security Collection (Knoppix), 297
 - Cain & Abel password recovery tool, 124
 - cantennae (yagi-style antennae), 60
 - certification organizations, 327
 - client vulnerability testing tools, 103
 - Cobit standard, 27
 - CommView for WiFi sniffer, 115
 - CoWPAtty WPA-PSK-auditing tool, 294
 - deauthentication attack tools, 242
 - for default settings, 77
 - default SSID information, 128
 - dictionary files and word lists, 339
 - DiGLE, 151–152
 - `dsniff` penetration-testing tools, 125
 - emulation software, 46–47, 52, 333
 - `essid_jack` SSID reporting tool, 127
 - Ethereal sniffer, 114
 - Foundstone query tool for Google, 34, 72
 - general resources, 328
 - general wireless tools, 331–332
 - Google, 33–34, 71–72
 - Gulpit sniffer, 119
 - hacker sites, 328
 - Hacking For Dummies* passwords chapter, 78, 107
 - Hermes chipset information, 58
 - honeypot software, 176
 - IDS systems, 80
 - IDS/IPS vendors, 336–337
 - IEEE site, 328–329
 - IP address-gathering tools, 339
 - IPSec testing tools, 295–296
 - ISO/IEC 17799 standard, 26
 - ISSAF standard, 28
 - Kismet driver information, 157
 - LEAP-cracking tools, 292–293, 340
 - link-monitoring tools (Linux), 87–89
 - Linux distributions (freeware), 332
 - Linux distributions on CD, 56
 - Linux Wireless Extensions, 82
 - local wireless groups, 329–331
 - MAC address vendor IDs, 198
 - MiniStumbler wardriving tool, 170
 - Mognet sniffer, 119
 - NetStumbler tool, 133
 - network scanners, 340

Internet resources (*continued*)

- network-management programs using SNMP, 214
- network-mapping tools, 35–36, 340
- OCTAVE standard, 27
- open EAP issues, 290
- operating system security information, 111
- OSSTMM standard, 28, 30
- packet-injection tools, 236, 240
- partitioning software, 46
- passive tests for social engineering, 71–72
- password cracking tools, 338–339
- pong vulnerability-assessment tool, 129
- port scanners, 100
- PPTP crackers, 295
- RADIUS servers, 288–289
- RF jamming devices, 64
- RF monitoring software, 333–334
- RF prediction software, 333
- security awareness and training, 331
- security awareness products, 80
- signal generators, 232–233
- SMAC MAC address changer, 203
- Snagit screen capture software, 32
- sniffers (network analyzers), 119–120, 337–338
- SNMP enumeration utilities, 215
- SNMP vulnerabilities, 216
- spectrum analyzers, 90
- SSE-CMM standard, 27
- SSID-gathering tools, 127–128, 339
- SSIDsniff tool, 128
- StumbVerter software, 150
- unauthorized equipment searches, 193
- U.S. Patent and Trademark Office site, 33
- Void11 packet-injection tool, 236
- vulnerability databases, 41, 332
- wardriving tools, 335–336
- WarLinux wardriving tool, 169
- Wellenreiter wardriving tool, 168
- WEP key-cracking tools, 265, 267, 269, 273, 274
- WEP vulnerability information, 110
- WEP/WPA cracking tools, 338
- Wi-Fi Alliance, 10
- Wi-Fi databases, 34–35
- WiLDing information, 169
- wireless NIC comparisons, 59
- wireless organizations, 328–329
- WPA Cracker tool, 294
- intranet VPNs, 279

- intrusion-detection/prevention system (IDS/IPS), 80, 253–254, 336–337
- IP addresses
 - gathering from wireless networks, 125–126, 339
 - looking up yours, 35
 - social engineering to obtain, 73
- iPAQ PDA (Hewlett-Packard), 44
- IPSec encryption, 280, 295–296
- ISECOM (Institute for Security and Open Methodologies), 28–29
- ISO (International Organization for Standardization), 26
- ISO/IEC 17799 standard, 26–27
- ISSAF (Information Systems Security Assessment Framework) standard, 27–28
- iStumbler wardriving software, 174
- iwconfig Wireless Tool (Linux), 82–85
- iwlist Wireless Tool (Linux), 82, 86–87
- iwpriv Wireless Tool (Linux), 82, 85
- iwspy Wireless Tool (Linux), 82, 87

• J •

- jamming signals. *See* RF jamming
- jc-wepcracker WEP cracker, 274
- Jornada PDA (Hewlett-Packard), 44

• K •

- KisMAC packet analyzer, 119, 174
- Kismet stumbling tool
 - capabilities of, 156
 - commands, 165–166
 - configuring, 160–161
 - driver information online, 156
 - flags (options), 162
 - GPS units and, 62
 - gpsd command-line options, 160
 - Info frame, 164–165
 - installing Kismet, 157–159
 - installing the GPSD, 159–160
 - log files, 166–167
 - need for, 56
 - Network List frame, 163–164
 - obtaining, 157
 - as passive network scanner, 155
 - preparing to install, 157
 - Prism2 chipset and, 57
 - programs useful with, 157

shutting down, 167
 starting, 161–162
 Status frame, 165
 StumbVerter and MapPoint with, 167
 switches (options), 158
 user interface, 163–165
 wardriving countermeasures using, 174
 Web site, 119
Knoppix
 Auditor Security Collection, 236, 274,
 297–299
 Linux distribution, 55–56
Knoppix For Dummies (Sery), 56

● **L** ●

LANfielder packet analyzer, 120
 LANguard Network Security Scanner tool
 (GFI), 40, 103, 108–109, 214
 LanSpy enumeration tool, 103, 108
 laptops. *See* portables or laptops
 Layer 2 Tunneling Protocol (L2TP), 280
 LBL's arpwatch, 129
LEAP (Lightweight Extensible Authentication
 Protocol)
 cracking tools, 292–293, 340
 cracking with *anwrap*, 293
 cracking with *asleap*, 291–292
 cracking with *THC-LEAPcracker*, 292–293
 overview, 286–287
 security vulnerabilities, 290–291
 legal issues, 316–319
 Legion enumeration tool, 108
 libpcap freeware, 157
 libradiate packet injection tool, 240
 Lightweight Extensible Authentication
 Protocol. *See* LEAP
 LinkFerret packet analyzer, 120
link-monitoring tools (Linux)
 iwconfig, 82–85
 iwlist, 82, 86–87
 iwpriv, 82, 85
 iwspy, 82, 87
 other tools, 88–90
 Wavemon, 87
 Wimon, 88
 Wireless Extensions, 81–82
 Wmap, 88
 Wscan, 88
 XNetworkStrength, 88

link-monitoring tools (Windows). *See*
 NetStumbler (Network Stumbler) tool
Linux
 application mapping, 105
 Auditor Linux, 119
 distributions on CD, 55–56
 emulating on Windows, 46–55
 emulating Windows on, 46
 freeware distributions, 332
 link-monitoring tools, 82–88
 Mac OS and, 47
 MAC-address spoofing, 198–199
 security resources online, 111
 Wireless Extensions, 81, 82
 Wireless Tools, 81–87
Long, Johnny (ethical-hacking
 webmaster), 72
 L2TP (Layer 2 Tunneling Protocol), 280

● **M** ●

^M character at end of text files, 49
MAC Changer software, 199
MAC (media-access control) addresses. *See*
 also MAC-address spoofing
 BSSID as, 132
 checking for unauthorized users, 90
 detecting with Network Scanner, 100
 determining ad-hoc device connection to
 your system, 191–192
 enabling MAC address controls, 198,
 204–207
 filtering, ease of circumventing, 13
 in NetStumbler, 144–145
 Organizationally Unique Identifiers
 (OUI), 144
 overview, 197
 searching Wi-Fi databases for, 34
 Signal-to-Noise Ratio in NetStumbler,
 147–148
 SMAC MAC address changer, 90–91
 sniffing for security vulnerabilities, 221
 social engineering to obtain, 73
 of unauthorized systems, 183
 vendor IDs online, 198
MAC (message authentication code), 257
 Mac OS, emulating Windows on, 47
MAC-address spoofing
 editing the Windows Registry, 200–203
 enabling MAC address controls and, 198,
 204–207

- MAC-address spoofing (*continued*)
 - in Linux, 198–199
 - MAC address vendor IDs online, 198
 - SMAC MAC address changer for, 203–204
 - spoofing defined, 197
 - testing MAC address controls, 204–207
 - in Windows, 199–203
 - MacStumbler wardriving software, 174
 - management-frame attacks, 209–211
 - man-in-the-middle attacks. *See* MITM attacks
 - mapping null sessions (Windows), 106–107
 - mapping your network, 35–37, 340
 - MapPoint software (Microsoft), 62–63, 149–150, 167
 - media-access control addresses. *See* MAC addresses
 - Meetinghouse Data
 - AEGIS 802.1X client software, 289
 - AEGIS RADIUS server, 289
 - message authentication code (MAC), 257
 - methodology implementation. *See*
 - implementing a testing methodology
 - Microsoft. *See also* Windows
 - IAS, 288
 - MapPoint software, 62, 63, 149–150, 167
 - PPTP protocol, 279–280
 - Streets & Trips, 63, 150
 - Virtual PC, 47
 - MIDI (Musical Instrument Digital Interface), 140, 170
 - Milner, Marius (wardriver), 169
 - MiniStumbler wardriving tool, 170–173
 - MIPS PDA (Casio), 44
 - mistakes to avoid
 - breaking the law, 316–319
 - failing to equip yourself, 313–314
 - failing to get written permission, 312–313
 - failing to report results or follow up, 314–316
 - forgetting to unbind the NIC when wardriving, 309–312
 - not involving others in testing, 308
 - not using a methodology, 308–309
 - over-penetrating live networks, 314
 - skipping planning, 307–308
 - using data improperly, 314
 - MITM (man-in-the-middle) attacks
 - ARP poisoning, 209
 - dangers of, 208–209
 - defined, 208
 - management-frame attacks, 209–211
 - methods for, 209
 - port stealing, 209
 - tools for, 209
 - Magnet sniffer, 119, 174
 - monitoring laws, 317–318
 - monkey-in-the-middle attacks. *See* MITM (man-in-the-middle) attacks
 - monkey_jack MITM attack utility, 208, 210–211
 - multi-boot workstations, 45–46
 - Musical Instrument Digital Interface (MIDI), 140, 170
- N ●
- National Marine Electronics Association (NMEA) GPS protocol, 62
 - Nessus vulnerability assessment tool, 40, 103–104
 - NetChaser wardriving software, 174
 - NetStumbler (Network Stumbler) tool. *See also* wardriving
 - active scanning method of, 132
 - DiGLE with, 151–152
 - Display options, 138
 - downloading, 133
 - enumeration with, 37
 - example window from session, 133–135
 - exporting plotted data from, 148
 - filters, 146–147
 - finding unauthorized equipment with, 186–188
 - flags, 144
 - General options, 137
 - GPS options, 138–139
 - GPS units and, 62–63
 - Hermes chipset and, 57
 - information recorded by, 132
 - installing, 133
 - interpreting results, 141–148
 - MAC addresses in, 144, 145
 - mapping data from, 149–152
 - menus and commands, 135–136
 - merging files, 147
 - Microsoft Streets & Trips with, 150
 - MIDI options, 140
 - need for, 56
 - network mapping with, 35–36
 - RF jamming displayed in, 230–232
 - right-pane columns described, 142–143
 - running, 133
 - scan speed settings, 137

Scripting options, 139–140
 searching the Internet for your files, 71
 setting up, 134–141
 Signal-to-Noise Ratio in, 147–148
 SSIDs in, 145–146
 status messages, 134–135
 StumbVerter and MapPoint with, 149–150
 toolbar, 140–141
 Web site, 35

network analyzers or monitors. *See* sniffers

network bounds. *See* determining network bounds

network interface cards (NICs). *See* wireless NICs (transceivers)

Network Protocol Analyzer (SoftPerfect), 120

Network Scanner (SoftPerfect), 100

network scanners, 340

Network Security For Dummies (Cobb), 40, 111

Network Stumbler. *See* NetStumbler tool

Network Stumbler Options dialog box, 136–140

network-level attacks

- ARP-poisoning attacks, 209, 211–213
- Clear Channel Assessment attack, 217
- countermeasures, 222–223
- dangers of attacks, 196–197
- dangers of testing for, 197
- 802.11 vulnerabilities, 195–196
- MAC-address spoofing, 197–207
- management-frame attacks, 209–211
- man-in-the middle (MITM) attacks, 208–213
- overview, 18, 196–197
- port stealing, 209
- Queensland attack, 217, 229
- sniffing for vulnerabilities, 218–222
- SNMP vulnerabilities, 213–216

ngrep packet analyzer, 120

NICs (network interface cards). *See* wireless NICs (transceivers)

NIST ICAT Metabase, 41, 110

nmap network-mapping tool, 36–37

NMEA (National Marine Electronics Association) GPS protocol, 62

non-technical attacks, 17

Norton All-in-One Desk Reference For Dummies (Chase), 46

null sessions (Windows)

- countermeasures, 111–112
- defined, 106
- finding shares, 107–109
- getting information from, 107
- mapping, 106–107

• 0 •

Observer packet analyzer, 120

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) standard, 27

Odyssey 802.1X client software (Funk Software), 289

omnidirectional antennae, 13, 60–61, 94

104-bit (128-bit) encryption, 256, 258

Open Information System Security Group, 27

Open Source Security Testing Methodology Manual (OSSTMM) standard, 28–30

open-system authentication, 282

operating systems. *See* emulation software; *specific operating systems*

Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) standard, 27

Organizationally Unique Identifiers (OUI), 144

ORINOCO

- Client Manager software, 184–185
- wireless NICs, 59, 109–110

Osborne, Mark “Fat Bloke” (programmer), 249

OSSTMM (Open Source Security Testing Methodology Manual) standard, 28–30

OUI (Organizationally Unique Identifiers), 144

• p •

packet analyzers. *See* sniffers (network analyzers)

packet-injection tools, 235–237, 240. *See also* AP overloading

Packetyzer packet analyzer, 120

parabolic grid antennae, 92

partitioning software, 45–46

PartitionMagic (Symantec), 46

passive attack decryption for WEP, 264

passwords

- cracking tools, 338–339
- dangers of weak, 77–78
- dictionary files and word lists, 339
- downloading *Hacking For Dummies* chapter on, 78, 107
- searching the Internet for, 71
- social engineering to obtain, 71, 73
- SSIDs versus, 126

Patent and Trademark Office Web site, 33

PDAAs (personal digital assistants), 44–45

- PEAP (Protected Extensible Authentication Protocol), 286
- penetration testing. *See also* ethical hacking; vulnerability assessment or testing
- defined, 20
 - dsniff tools for, 124–125
 - ethical hacking versus, 1, 10
 - performing, 41–42
- Pepper, Hugh (cantennae vendor), 60
- permission for ethical hacking, written, 21–22, 312–313
- personal digital assistants (PDAs), 44–45
- physical security. *See also* human vulnerabilities
- countermeasures, 90–95
 - DoS attacks and, 250
- ping sweep, 36, 100, 126. *See also* port scanning
- planning for ethical hacking
- goal setting, 20–21
 - importance of, 307–308
 - overview, 15–16, 21
- Plex86 emulation software, 46
- Pocket Warrior wardriving software, 174
- pocketWinc wardriving software, 174
- Point-to-Point Tunneling Protocol (PPTP) of Microsoft, 279–280, 295
- pong vulnerability-assessment tool, 129
- port scanning
- commonly hacked ports (table), 38, 101–102
 - enumeration using, 37–38
 - information discovered by, 99–100
 - ping sweep for, 100
 - tools for, 100, 305
- port stealing, 209
- portables or laptops
- advantages for ethical hacking, 44–45
 - choosing, 303
 - components for, 45
 - PDAs versus, 44–45
 - portability of, 155–156
 - testing for unauthorized equipment using, 75–76
 - unauthorized clients, 178
- ports commonly hacked, 38, 101–102. *See also* port scanning
- power signal generators (PSGs), 64
- power-saving features, DoS attacks and, 228
- PPTP (Point-to-Point Tunneling Protocol) of Microsoft, 279–280, 295
- Prism Test Utility, 217
- Prism2 chipset, 57–58, 217
- privacy of messages, 23, 255–256
- probe responses, disabling, 175
- Protected Extensible Authentication Protocol (PEAP), 286
- protocol analyzers. *See* sniffers (network analyzers)
- protocols. *See also specific protocols*
- sniffing for security vulnerabilities, 220
 - unauthorized systems and, 183
 - for VPNs, 279–280
- PSGs (power signal generators), 64
- public information, gathering. *See* footprinting

• Q •

- QualysGuard network-mapping tool
- automatic vulnerability assessment with, 40
 - described, 103
 - finding client vulnerabilities with, 104–105
 - network mapping with, 36
 - SNMP vulnerabilities found by, 214–215
- Queensland attack, 217, 229

• R •

- radiation patterns of antennae, 91–94
- radio signals. *See* controlling radio signals; determining network bounds; RF jamming
- RADIUS servers, 288–289
- RC4 algorithm (WEP), 258, 260–261, 283–284
- record keeping
- documenting lessons learned, 323
 - logging what you do, 32
 - overview, 22–23
 - reporting all findings, 25, 314–316
- Registry (Windows), editing for MAC-address spoofing, 200–203
- Remember icon, 5
- remote access VPNs, 279
- repeating tests, 11, 24, 323
- reporting all findings, 25, 314–316. *See also* following up
- resources. *See* Internet resources
- RF generators, 64
- RF jamming
- common signal interrupters, 230
 - dangers of, 230
 - devices for, 64
 - 802.11 standards and, 229

history of, 64
 NetStumbler display of, 230–232
 Queensland attack, 217, 229
 by signal generators, 232–233
 sources of, 63–64, 229–230
 unintentional, 229–230
 wireless network susceptibility to, 229
 RF monitoring software, 333–334
 RF prediction software, 333
 risks, 11–12. *See also* vulnerabilities
 Rohde & Schwarz spectrum analyzer, 90

● S ●

scanning
 port scanning, 37–38, 99–102, 305
 for unauthorized equipment, 75–76, 80
 your systems, 37–38
 scientific process, 24
 screen capture software, 32
 scripts (NetStumbler), 139–140
 Secure Shell (SSH2) tunneling, 280
 SecureACS (Secure Access Control Software)
 of Cisco, 288
 security awareness products, 80
 SEI (Software Engineering Institute), 27
 services, determining which are running, 39
 service-set identifiers. *See* SSIDs
 Sery, Paul (*Knoppix For Dummies*), 56
 shared-key authentication
 overview, 282–283
 problems with, 259, 262, 283–284
 shares (Windows), finding, 107–109
 signal generators, 232–233. *See also* RF
 jamming
 signal jamming. *See* RF jamming
 signal strength
 adjusting, 94–95
 NetStumbler graphing of, 132
 unauthorized equipment and, 185–186
 Simple Network Management Protocol. *See*
 SNMP
 SiteDigger tool (Foundstone), 72
 SLAX Linux CD distribution, 56
 SMAC MAC address changer, 90–91, 203–204
 Snagit screen capture software, 32
 Sniff-em wardriving software, 174
 Sniffer Netasyst packet analyzer, 120
 Sniffer Wireless packet analyzer, 120, 174
 sniffers (network analyzers). *See also specific*
 programs
 anti-sniffing programs, 130
 detecting, 129–130

finding network-level attack vulnerabilities
 with, 218–222
 finding unauthorized equipment with,
 188–192
 origin of name, 57
 overview, 56–57, 305
 programs, 113–120, 218–219, 337–338
 tips for using, 219
 trends to look for, 220–222
 for VPNs, 102–103
 SNMP (Simple Network Management
 Protocol)
 checking if running, 214
 network-level attack vulnerabilities, 214–216
 network-management programs using, 214
 overview, 213–214
 SNMPUTIL utility, 215
 social engineering
 active tests, 73–74
 dangers of, 70
 defined, 17, 67, 70
 hiring third parties for testing, 70
 overview, 70–71
 passive tests, 71–72
 SoftPerfect
 Network Protocol Analyzer, 120
 Network Scanner, 100
 software attacks, 18
 Software Engineering Institute (SEI), 27
 spectrum analyzers, 90
 spoofing MAC addresses. *See* MAC-address
 spoofing
 SSE-CMM (Systems Security Engineering
 capability maturity model) standard, 27
 SSH2 (Secure Shell) tunneling, 280
 SSIDs (service-set identifiers). *See also* APs
 (access points)
 changing defaults, 128
 cloaked, 132
 default settings information, 128
 disabling broadcasts, 13, 129
 gathering from wireless networks,
 126–128, 339
 in NetStumbler, 145–146
 passwords versus, 126
 reporting with `essid_jack`, 127, 188
 searching the Internet for yours, 34, 71
 social engineering to obtain, 73
 systems identified by names of, 13
 of unauthorized systems, 182–183
 on Wi-Fi databases, 34
 SSIDsniff tool, 128

standards for ethical hacking

- Cobit, 27
- ISO/IEC 17799, 26–27
- ISSAF, 27–28
- OCTAVE, 27
- OSSTMM, 28–30
- overview, 26
- SSE-CMM, 27

standards for wireless networks, 9–11. *See also specific standards*

- Steel Belted RADIUS (Funk Software), 289
- Street Atlas USA (DeLorme), 63
- Streets & Trips (Microsoft), 63, 150
- stumbling tools, 56, 186–188, 304. *See also specific tools*
- StumbVerter software, 62, 149–150, 167
- Sun Tzu (*The Art of War*), 155
- SuperScan port scanner (Foundstone), 37–38, 100–101
- Symantec's PartitionMagic, 46
- Systems Security Engineering capability maturity model (SSE-CMM) standard, 27

• T •

- table-based attacks on WEP, 264
- Tcpdump packet sniffer, 119
- Technical Stuff icon, 5
- Tektronix power signal generators, 64
- telephone, social engineering tests using, 73
- Temporal Key Integrity Protocol (TKIP), 294
- Ten Commandments of Ethical Hacking
 - ISSAF standard and, 28
 - overview, 19–20
 - Thou shalt do no harm, 23–24
 - Thou shalt keep records, 22–23
 - Thou shalt not covet thy neighbor's tools, 24–25
 - Thou shalt obtain permission, 21–22
 - Thou shalt plan thy work, 21
 - Thou shalt report all thy findings, 25
 - Thou shalt respect the privacy of others, 23
 - Thou shalt set thy goals, 20–21
 - Thou shalt use a scientific process, 24
 - Thou shalt work ethically, 22
- 10pht's AntiSniff, 130
- Terabeam Wireless signal generator, 232
- testing methodology implementation. *See implementing a testing methodology*
- Tethereal packet sniffer, 118
- text files, ^M character at end, 49

- THC-LEAPcracker tool, 292–293
- THC-Scan wardriving software, 174
- THC-Wardrive wardriving software, 174
- threats, 11. *See also vulnerabilities*
- time frame for tests, 24
- Tip icon, 5
- TKIP (Temporal Key Integrity Protocol), 294
- TopoUSA mapping software (DeLorme), 63
- training about human vulnerabilities, 79–80
- transceivers. *See wireless NICs*

• U •

- UCD-SNMP utility, 215
- unauthorized equipment. *See also APs (access points)*
 - APs, 178
 - characteristics indicating, 181–184
 - countermeasures, 193–194
 - dangers of, 75
 - determining if connected to your system, 191–192
 - excuses for setting up, 69, 74
 - finding with stumbling software, 186–188
 - main types of, 178
 - in online databases, 193
 - other software for finding, 193
 - rogue APs or clients, 178
 - scanning for, 75–76, 80
 - signal strength and, 185–186
 - system configurations and, 179–181
 - typical scenario for setting up, 74–75
 - wireless clients, 178
- unauthorized users, checking for, 90–91
- U.S. Patent and Trademark Office Web site, 33
- usability versus security, 69
- US-CERT Vulnerability Notes Database, 41, 110

• V •

- Virtual PC (Microsoft), 47
- VMware emulation software, 46, 52–55
- Void11 packet-injection tool, 235–236, 242
- VPNMonitor sniffer, 102–103
- VPNs (Virtual Private Networks)
 - authentication using, 295–296
 - defined, 278
 - as encryption attack countermeasure, 278–280
 - IPSec for, 280, 295–296

- Layer 2 Tunneling Protocol (L2TP) for, 280
 - Point-to-Point Tunneling Protocol (PPTP)
 - for, 279–280, 295
 - Secure Shell (SSH2) for, 280
 - sniffing, 102–103
 - types of, 279
 - vulnerabilities. *See also* human vulnerabilities
 - for all networks, 12–13
 - AP weaknesses, 104–105
 - defined, 11
 - for network-level attacks, 18
 - for non-technical attacks, 17
 - reporting all findings, 25, 314–316
 - for smaller networks, 12
 - for software attacks, 18
 - threats versus, 11
 - vulnerability assessment or testing. *See also*
 - ethical hacking; penetration testing
 - automatic, 40–41
 - for client vulnerabilities, 99–110
 - for default settings, 77
 - defined, 39
 - ethical hacking versus, 1, 10
 - for firmware vulnerabilities, 129
 - further information, 41
 - manual, 40
 - overview, 39–40
 - for social engineering, 71–74
 - for unauthorized equipment, 75–76
 - vulnerability databases, 41, 332
- *W* •
- warchalking, 169
 - warcycling, 169
 - wardriving. *See also specific software*
 - countermeasures, 174–176
 - defined, 22, 131
 - first conviction for, 22
 - Kismet for, 156–167
 - legal and ethical issues, 317
 - MiniStumbler for, 170–173
 - NetStumbler for, 132–152
 - origin of name, 169
 - other software for, 173–174
 - other war memes, 169
 - overview, 131–132
 - tools for, 335–336
 - unbinding the NIC for, 309–312
 - WarLinux for, 168–169
 - Wellenreiter for, 167–168
 - warflying, 169
 - warkayaking, 169
 - WarLinux CD distribution, 56
 - WarLinux wardriving tool, 168–169
 - Warning! icon, 5
 - warspying, 169
 - warsurfing, 169
 - warwalking, 169
 - Waterfall Spectrum Analyzer, 90
 - wave guide antennae, 60, 62
 - Wavemon link-monitoring tool, 87
 - WDMZ (wireless demilitarized zone), 297
 - Web sites. *See* Internet resources
 - Wellenreiter wardriving tool, 167–168
 - WEP (Wired Equivalent Privacy)
 - active traffic injection attacks, 263–264
 - AP encryption settings, 258–259
 - attacking, 263–264
 - changing keys, 259
 - cracking keys, 264–274
 - cracking tools, 338
 - Cyclic Redundancy Check (CRC),
 - 256–257, 260
 - encryption flaws, 78, 256, 259–263
 - extensions for longer key lengths, 256
 - hacking wireless clients for keys,
 - 109–110
 - key vulnerabilities other than encryption,
 - 261–263
 - multiple uses for keys in, 261
 - overview, 256
 - passcode generation, 262
 - passive attack decryption, 264
 - RC4 algorithm, 258, 260–261, 283–284
 - risks for larger networks, 13
 - rotating keys, 275
 - shared-key problems, 259, 262, 283–284
 - social engineering to obtain key(s), 73
 - summary of weaknesses, 262
 - table-based attacks, 264
 - types of attacks, 259
 - vulnerability information online, 110
 - WepAttack WEP cracker, 274
 - WEPcrack key-cracking tool, 265–267
 - WepLab WEP-key cracking tool, 273–274
 - WEPWedgie traffic injection tool, 263
 - white-hat hacking. *See* ethical hacking
 - WIDS (wireless intrusion-detection system),
 - 253–254, 296
 - Wi-Fi Alliance, 10, 329
 - Wi-Fi databases, footprinting using, 34–35

- Wi-Fi networks
 - advantages of, 9, 10
 - commonly hacked ports (table), 38, 101–102
 - complexities of, 14–15
 - risks increased by popularity of, 9–10
 - security policy for, 78–79
 - smaller network vulnerabilities, 12
 - standards, 9, 10–11
 - system configurations, 179–181
 - types of risks for, 11–12
 - vulnerabilities for all networks, 12–13
 - Wi-Fi Protected Access. *See* WPA standard
 - WiGLE database, 34
 - WiLDing (Wireless LAN Discovery). *See* wardriving
 - Wimon connection-monitoring tool, 88
 - Windows (Microsoft). *See also* Microsoft 802.1X client software for XP, 289
 - emulating Linux on, 46–55
 - emulating on Linux, 46
 - emulating on Mac OS, 47
 - finding shares, 107–109
 - MAC-address spoofing, 199–203
 - security resources online, 111
 - testing for null sessions, 106–109
 - testing for unauthorized equipment using, 75–76
 - WINE emulation software, 46
 - Win4Lin emulation software, 46
 - Wired Equivalent Privacy. *See* WEP
 - wireless client software, 184–186
 - wireless demilitarized zone (WDMZ), 297
 - Wireless Extensions (Linux), 81–82
 - wireless intrusion-detection system (WIDS), 253–254, 296
 - Wireless LAN Discovery (WiLDing). *See* wardriving
 - wireless local-area networks (WLANs). *See* Wi-Fi networks
 - Wireless Networks For Dummies* (Davis)
 - antennae information in, 62
 - manual assessment information in, 40
 - NetStumbler filters described in, 146
 - as reference guide, 305
 - VPN information in, 280
 - wireless NIC information in, 57
 - wireless-network fundamentals in, 15
 - wireless NICs (transceivers)
 - buying, 59, 304
 - determining your chipset, 57–58
 - external antenna connector, 59
 - NetStumbler versus Kismet and, 57
 - resetting network properties for
 - MAC-address spoofing, 199–200
 - unbinding when wardriving, 309–312
 - WEP key vulnerabilities, 109–110
 - Wireless Security Auditor software, 174
 - wireless security policy, 78–79
 - Wireless Tools (Linux)
 - iwconfig, 82–85
 - iwlist, 82, 86–87
 - iwpriv, 82, 85
 - iwspy, 82, 87
 - overview, 81–82
 - WiStumbler wardriving software, 174
 - Wlandump wardriving software, 174
 - WLAN-jack, 242, 249
 - WLANs (wireless local-area networks). *See* Wi-Fi networks
 - Wmap link-monitoring tool, 88
 - word lists and dictionary files, 339
 - WPA Cracker tool, 294
 - WPA (Wi-Fi Protected Access) standard
 - authentication using, 293–294
 - cracking tools, 338
 - Extended EAP authentication, 285
 - overview, 10
 - security vulnerabilities, 11, 277
 - using, 275–277
 - WPA2 (IEEE 802.11i) standard
 - authentication using, 294–295
 - overview, 10, 278
 - security vulnerabilities, 11
 - social engineering and, 73
 - using, 278
 - WPA versus, 275–277
 - Wright, Joshua (programmer), 294
 - Wscan link-monitoring tool, 88
-
- X •
 - XMap mapping software (DeLorme), 63
 - XNetworkStrength tool, 88

 - Y •
 - yagi-style antennae, 60, 62, 92–93
 - YDI power signal generators, 64
 - YDI Wireless signal generator, 232