

Index

Page numbers followed by *f* indicates a figure and *t* indicates a table.

A

- Access control systems, 276–277
- Administrative honeypots, 133
- Administrative intrusion detection systems, 129
- Advertisement on search engines, 68–69
- Alarm sensors, 112–113
- Alarm system evasion, 111–113
 - creating false positives, 111–112
- Analog phone lines, 116–117, 273–274
- Anomaly-based intrusion detection systems, 128
- Anonymous relays, 84–86
- Antimalware tools, 219
- Antisurveillance devices, 260–265
- Appearance, impersonating people, 78
- Application log files, 298–300
- Application-based intrusion detection systems, 127
- Attack IP address, 287*f*, 288*f*
- Attack location obfuscation
 - filtered protocol tunneling, local subnet, 291–292
 - IDS avoidance
 - IP address decoys, 289
 - thresholds, 290
 - protocol tunneling, 292–294
 - ICMP, 293–294
 - TCP/IP suite, 294
 - protocol-specific anonymizers, SOCKS tunnel, 286–289
- Attack timing, 179–180
 - attacking between shifts, 180
 - attacking during maintenance, 180
- Attack vector, 300

B

- Backdoors, 269
- Badges and uniforms
 - fabricated, 82
 - stolen, 81–82
- Baiting, 151–157
- Battlefield, 19–20
- Berkley packet filter (BPF), 194
- Biometric identifiers, 111
- Biometric systems, 110–111, 276

- Black Hat hackers, 27–28
- Blade weapon, 17
- Blended anonymized networks, 86
- Blinding cameras, 262–263
 - ways for blinding
 - blocking/dismantling, 263
 - infrared light, 262–263
 - lasers, 262
- Bluetooth, 208–209
- Botnets, 282
- Brute force attacks, 49–50, 290, 300
- Bug sweeping, 258
- Building rapport, 231
- Bump keys, 104–106
- Bushido, 2, 3–8

C

- Cameras
 - blinding, 262–263
 - temporarily, 111–112
 - hidden video, detecting, 259
- Cell phones, 255–256
- Cellular network, 209–210
- Chain weapon, 17
- Clandestine communications tools, 242
- Clandestine human intelligence, 237–244
 - clandestine reporting, 239–241
 - penetrating organizations, 238–239
 - resources, 242–244
- Clandestinely placed sensors, 220–224
 - audio eavesdropping, 220–221
 - audio bugs, 221
 - computer microphones, 221
 - VoIP, 220
 - video eavesdropping, 221–223
 - existing camera systems, 222–223
 - video bugs, 221–222
- Clickjacking, 272
- Clothing accessories, 17
- Code of Ethics, ISC, 32
- Communications Act of 1934, 260
- Communications infrastructure, 273–274
- Company events, 170
 - meetings/conferences, 170
 - outside events, 170
 - utility interruptions, 172
- Complex physical intrusion detection systems, 126

Computer hardware upgrades, 123–124

Concealment, 200–204

- data, methods of, 202–203
- device for iPod touch, 202*f*, 203*f*
- hiding locations, example, 201–202
- limitations, 200–201

Confidence trick (cons), 154–157

Converted spies, 53–54

Counterfeit hardware, 274–276

- components, 275–276

Covert channels, 241

Credential hijacking, 123

Credit reports, 250

Cydia, 186, 187

- advantage of, 187

D

Data concealment, methods of, 202–203

Data manipulation, 270–272

Data smuggling, 198–204

- data
 - in motion, 199–200
 - at rest, 199
- encryption, 198–200

Datagram Transport Layer Security (DTLS)

- protocol, 85

Debriefing, 230–231

Deception, interrogation technique, 232

Demarcation point, 273, 274*f*

Denial-of-service attacks

- against administrative IDS, 129
- against logical IDS, 129
- on physical IDS, 126–127

Deprivation, 233

Detecting surveillance, 258–260

Disguise, 122

- business, 92–93
- of employees, 79–81
- labor, 94–95
- public figures, 94
- religious, 93–94
- rural, 93
- scholastic, 91–92
- uniformed, 95

Disruption of physical traffic patterns, 136

Distractors, 177–178

- feature of, 177
- misdirection, 177–178

Doomed spies, 54

Drugs, interrogation under, 233–234

Dumpster diving, 145

E

Earth element, 158

EDGAR. *See* Electronic Data Gathering, Analysis, and Retrieval System

802.11 wireless networks, 209–210

Electromagnetic radiation, eavesdropping, 223–224

- blinky lights, 224
- keyboard emissions, 224
- van Eck phreaking, 224

Electronic Data Gathering, Analysis, and Retrieval System (EDGAR), 252–254, 253*f*

Electronic lock safe, 108

E-mail attacks, 64–67

Employee/contractor home networks, 113–114

Environmental events, 170–172

- fires, 171–172
- storms, 171

Equipment and resources, 243–244

Ethics, modern-day Ninja

- appropriateness, 35–36
- community, 33–36
 - Crime Stopper program, 34
 - Japanese organizational structure, 33
- family
 - advantage of, 33
 - application of, 32
 - definition of, 32
 - example of, 33
- guideline for White and Black Hat hackers, 32
- homeland, cyber attacks, 35
- ISC Code of Ethics, 32

Excluded Parties List System (EPLS), 252, 253*f*

EXIF data, 256

External networks, lower levels of security on, 114–115

F

Fabricated badges and uniforms, 82

Fan site, 69

Federal court filings, 251

Fiber optic cables, 273

Filtered protocol tunneling, local subnet, 291–292

Financial manipulation, 271

Financial resources, 243

Fingerprints method, 110

Fire element, 158

Firefox SOCKS, configuring, 288*f*

Firefox Web browser, 287

Fish nets, 17
 Five constant factors, *The art of war*, 41–44
 Five elements, 157–158, 158*t*
 Five weaknesses, 158–161, 158*t*
 Flashy attacks, 177
 Fraudulent certificates, 98–99

G

Gates, 140–142, 148
 logical, 141–142
 physical, 140–141
 Global System for Mobile Communications (GSM), 209
 Gnu C compiler, 192, 192*f*
 GNU Privacy Guard (GnuPG), 199
 Good cop/bad cop strategy, 232
 Google hacking, 147–148, 149
 GPS mechanism, 248
 GPS tracking devices, 254–255
 cameras and EXIF data, 256
 cell phones, 255–256
 Google and others, 256–257
 tracking systems for, 255
 vehicle-based, 254–255
 volunteered location information, 257
 Gray Hat hacker, definition, 29
 GSM. *See* Global System for Mobile Communications
 Guards, 143–144
 Guns, 142–143, 148

H

Hagakure, 6–8
 Hardware
 compromised, 294–296
 infected, 270
 Hardware key loggers, 210–211
 placing, 211–212
 PS2, 211, 212
 retrieving data from, 213
 USB, 211
 Hensōjutsu, 76–78
 Hidden video cameras, detecting, 259
 Hijacking accounts, 174–175
 Hira shuriken, 17
 Historical ninja, 8–18
 origins, 10–13
 Holidays events, 168
 government, 168
 religious, 168
 Honey_pot, 132–133

Host-based intrusion detection systems (HIDS), 128, 220
 Human intelligence (HUMINT), 227–231
 clandestine, 237–244
 relationship analysis, 228–230
 sources for, 228

I

IDS. *See* Intrusion detection systems
 Impersonation of people, 76–78
 Information diving
 logical, 146–148
 physical, 144–146
 Information Security community (ISC), 32
 Insurance, loss of, 66
 Intelligence gathering, 248–254
 Internationalized domain name (IDN), 147
 Internet Control Message Protocol (ICMP), 293–294
 Interrogation techniques, 231–237
 deception, 232
 drugs, 233–234
 good cop/bad cop strategy, 232
 suggestion, 233
 torture, 234–237
 Intrusion detection systems (IDS), 42, 220
 administrative, 129
 avoidance, 125–133
 logical, 127–129
 physical, 126–127
 rule, snippet of, 290
 Inward spies, 53
 IP address decoys, 289
 IP camera, 222, 223, 223*f*
 iPod touch, 184, 186
 application of, 190
 concealment device for, 202*f*, 203
 disadvantage of, 192
 Netcat backdoor on, 196*f*
 Nmap application installation on, 187*f*
 Nmap running on, 188*f*
 scapy installed on, 192*f*
 SSH server information on, 196*f*
 tools installed on, 197*t*
 Iron war fan, 18
 ISC. *See* Information Security community
 IT support for employee, 80

J

Jammers, 260–261, 261*f*, 264
 Job postings, 248–249

K

Key logging, 210–214. *See-also* Hardware key loggers. *See-also* Software key loggers
 Kismet, 137
 Kunoichi, in social engineering, 162–164, 165
 Kusarifundo, 17
 Kyoketsu shoge, 17

L

Laser-listening devices
 defeating, 261–262
 detecting, 258–259
 Laying Plans, 40–46
 Laziness, 159
 Legacy networks, 116–117
 Local spies, 52–53
 Location tracking, 254–257
 Lock picking, 103–111
 avoiding lock, 103–104
 locks without leaving evidence, 104–107
 reproducing keys, 106–107
 Log file
 after local login, 297*f*
 manipulated, 297*f*
 modification of, 298*f*
 Log manipulation
 application log files, 298–300
 user log files, 296
 Log record, on Linux system, 296*f*
 Logging, 299*f*
 Logical access controls, 277
 Logical distractors, 177
 Logical gates, 141–142
 Logical guards, 144
 Logical guns, 143
 Logical honeypots, 132
 Logical information diving, 146–148
 Logical intrusion detection system, 127–129
 Logical sabotage
 data manipulation, 270–272
 malware, 268–270
 Logical traffic patterns, 136–140
 disrupting, 139–140
 wireless security surveys, 137–138
 Logins, failed, 299*f*
 Loss of job, e-mail attack, 67

M

Malicious software installation, 71
 Malware, 176, 268–270, 294
 cell phones, 295
 hard drives, 295
 in network devices, 295–296

Meeting places for clandestine meetings, 242–243
 Melon Drop, 156
 Memory sticks, 294–295
 Metasploit, installation screen for, 190*f*
 Metsubishi, 111–112
 Military offensive strategic goals, 59
 MiniSD chip, 203, 204*f*
 Mobile devices, 184–198
 advantages and disadvantages of, 184
 detection methods, 184–185
 frequency analysis, 185
 heat detection, 184–185
 radio transmissions, 185
 trend, 186–198
 Modern disguises, 79–84
 Modern kunoichi, 162–163
 Multiple fronts, attacking on, 178–179
 local and remote attacks, 178–179
 physical and logical attacks, 178
 Multipronged attacks, 176–180

N

Netcat, 188
 Netstumbler, 137
 Network
 blended anonymized network, 86
 hardware, 274, 275*f*
 infrastructure, 273–274
 peer-to-peer, 85–86
 sniffing, 138–139
 and system traffic patterns, 122–123
 Tor, 84–85
 Network-based intrusion detection systems
 (NIDS), 127–128
 NIDS. *See* Network-based intrusion detection systems
 Nikto Web server scanner, 193*f*
 Ninja, 2, 10
 ethics, 18–19
 hierarchy, 12–13
 modern vision of, 23
 modern-day
 ethics of, 31–33
 examples of, 24
 teachings in Bujinkan organizations, 24
 orthodox and unorthodox methods, 24
 penetration testing, 24
 roles and responsibilities of, 285
 versus samurai, 18–21
 stories of, character
 Ishikawa, Goemon, 14–15, 14*f*
 Kurando, Yakushimaru, 13

- Momochi, Sandayu, 13
 - Sawamura, Yasusuke, 13
- sword, 16
- tactics of, 23
- weapons, 16–18
- White Hats *versus* Black Hats, 26–31
- Ninja hackers
 - advantages and disadvantages, 30
 - Gray Hat hacker, 29
 - methods using unconventional attacks, 30
 - negative side-effect of, 30
 - unconventional penetration test tactics, 29
 - use of unconventional tactics, 31
- Ninjutsu. *See* Ninja
- Nmap, 188, 188*f*
 - applications of, 188, 189
 - decoy scan, 289, 290*f*
 - installation screen for, 187*f*
- Nonstandard internal networks, 115–116

O

- On-site vendors, 83
- OpenSSH, 190
- OpenVPN application, 200, 200*f*
- Operating system upgrades, 124
- Origins of ninja, 10–13
- Out-of-band attacks, 130–132, 130*f*
 - against administrative controls, 131–132
 - against logical controls, 131
 - against physical controls, 130

P

- PACER. *See* Public Access to Court Electronic Documents
- Padlock shims, 106, 106*f*
- Patch process, exploiting, 71–72
- Patch Windows exploiting, 69–71
- Pcap file, encrypting, 199*f*
- PDA devices. *See* Personal data assistant devices
- Peer-to-peer network, 85–86
- Penetrating organizations
 - recruitment, 238–239
 - sleepers, 239
- People's fears and curiosity, 63–69
- Personal data assistant (PDA)
 - devices, 184, 185, 195
- Personal information, sources of, 250–251
- Phishing, 146–147, 149
 - attacks, 95–99
 - e-mail, 97–98

- sender, 96–97
 - Web site, 98
- Physical access controls, 140, 141
- Physical distractors, 177
- Physical guards, 143–144
- Physical guns, 142–143
- Physical honeypots, 132
- Physical information diving, 144–146
- Physical intrusion detection systems, 126–127
- Physical sabotage, 272–277
 - counterfeit hardware, 274–276
 - network and communications infrastructure, 273–274
- Physical security design flaws, 104
- Physical surveillance, detecting, 260
- Physical tailgating, 119–122
- Physical torture, 236
- Physical traffic patterns, 136
- Pin tumbler lock, 105*f*
- Pirni, 194
 - default regular expressions, 195*f*
 - sniffer screen for, 194*f*
- Pivot an attack, 189*f*
- PKI. *See* Public key infrastructure
- Pretexting, 90–95
- Project management processes, 44
- Protective software, poor/missing, 114
- Proximity card systems, 109–110
 - card cloning, 109
 - stealing cards, 109–110
- Psychological methods of torture, 236–237
- Psychological Warfare (PSYWAR), 55–59
- Psychology
 - impersonating people, 78
 - of tailgating, 120
- PSYWAR. *See* Psychological Warfare
- Public Access to Court Electronic Documents (PACER), 251, 252*f*
- Public key infrastructure (PKI), 98, 99
- Public records, 250–254

R

- Radio frequency (RF)
 - devices, 258
 - jammers, 260–261, 261*f*
 - scanners, 207–210
- Remote log servers, 300
- Remote vendor, 83–84
- Research and development networks, 115
- Resumes, 248–249
- Rootkits, 269–270

S

- Sabotage, 267
 - access controls to, 276–277
 - external sources
 - criminal enterprises, 282
 - criminals, 282
 - foreign governments and terrorists, 281
 - hacktivists, 281
 - script kiddies and hackers, 281–282
 - software pirates, 282–283
 - internal sources, 278–280
 - automated processes, 280
 - curious employees, 279
 - disgruntled employees, 278–279
 - human error, 279–280
 - locks, 276–277
 - logical, 268–272
 - physical, 272–277
- Safe cracking, 103–111
 - combination safe, 107–108
 - electronic lock safe, 108
 - elegant methods, 108–109
- Samurai, 2
 - historical, 3–8
 - versus* ninja, 18–21
 - weapons, 8
- Satellite maps, 136
- Scam baiting, 156
- Screening codes, 228, 228*f*
- Search engines, 67–69
 - advertisement on, 68–69
 - fan site, 69
- Security employees, 80–81
- Sengoku period, 267
- Sensors
 - alarm, 112–113
 - thermal motion, 112
 - ultrasonic motion, 113
- Sequential attacks, 179–180
- Shill Web sites, 172–176
 - company troubles, 173–174
 - false layoff rumors, 173
 - spurious company data, 172–174
- Shinobigatana, 16
- Shuriken, 17
- Signature-based intrusion detection systems, 128
- Site-to-site VPN connections, 115
- Social engineering, 251
 - elements, 157–158
 - kunoichi in, 162–164, 165
 - needs, 161
 - weaknesses, 158–161
- Social networking, 174–176, 229–230
 - advertising negative information, 174–175
 - blogs and, 249
 - false personal information, 174
 - false search engine results, 176
 - hijacking accounts, 174–175
 - using restraint, 174–175
- SOCKS proxy, 286, 287
 - set up on local machine, 287*f*
- Software key loggers, 210
 - placing, 212, 214
 - retrieving data from, 212–213, 214
- Software pirates, 282–283
- Sourcefire Vulnerability Research Team (VRT)
 - site, 290
- Spanish Prisoner, 155–156
- Spies, uses of, 51–55
- Sporting events, 168–170
 - country-specific sports, 169
 - event-based violence, 169–170
- Spyware, 214–220
 - installing, 216–218
 - operating systems and browsers, 216
 - Windows user account control, 216–218
 - and managing system resources, 218
 - modifying configurations, 215–216
 - stealing credentials, 215
 - stealing personal information, 215
 - using, 218–220
- SSH, 196
 - application of, 199, 200
 - server information on ipod touch, 196*f*
- Staffs and canes, 18
- Steganography, 239–241, 240*f*
- Sting operation, 157
- Storage channels, 241
- Strategies and tactics, Ninja
 - Laying Plans
 - deception, 44–46
 - method and discipline, 44
 - project manager, 43, 44*f*
 - team champion, 42, 43*f*
 - typical organizational structure, penetration test, 42, 43*f*
 - maneuvering
 - brute-force attacks, 49–50
 - penetration test, traditional methods, 48
 - practice dissimulation, 49
 - studying moods, 50–51
 - preconceived notions
 - control systems, 58
 - design of enemy, 57

- force dispositions, 59–60
- friendly forces, allocation of, 60
- morale and combat, 58
- PSYWAR, 55–59
- women ninja, 55
- spies, uses
 - converted, 53–54
 - doomed, 54
 - five classes of, 51–54
 - inward, 53
 - local, 52–53
 - rewards for spying, 54–55
 - surviving, 54
- Waging War
 - prolonged attacks, 46–47
 - rousing anger, 47–48
 - victory, 48
- Surplus hardware, 145–146
- Surviving spies, 54
- Sympathy, 160
- Synchronization of attacks, 179

T

- Tailgating, 104, 119–125
 - on authentication credentials, 122
 - exploiting weak entrances, 121–122
 - network and system, 122–125
 - physical, 119–122
 - psychology of, 120
 - regular patching cycles, 124–125
 - traffic patterns, 120–121
- Takamatsu, 15
- Technical Surveillance Countermeasures (TSCM), 258
- TEMPEST, 263–265
 - equipment, shielded, 263
 - facilities, shielded, 264
 - fonts, 264–265
- Tessen, 18
- The art of war*, 38–40
 - five constant factors, 41–44
- The Book of Five Rings*, 4–6
- The Open Organisation of Lockpickers (TOOOL), 104, 105
- Thermal motion sensors, 112
- Timing channels, 241
- Toami jutsu, 17
- TOOOL. *See* The Open Organisation of Lockpickers
- Tor network, 84–85, 286
- Torture, 234–237
 - legality and ethics of, 235

- physical, 236
- psychological methods of, 236–237
- utility of, 235
- Traffic patterns, 135–140
 - logical traffic, 136–140
 - physical, 136
- Trojan horse, 295
 - in hardware, 153–154
 - in software, 152
- Trusted networks, 113–117
- Truth drugs, interrogation under, 234
- TSCM. *See* Technical Surveillance Countermeasures
- 2D barcode, 203, 204*f*

U

- Ultrasonic motion sensor, 113
- Unfiltered security networks, 116
- USB
 - storage device, stealthy, 270*f*
 - Trojan devices, 153, 153*f*, 154
- User interface manipulation, 271–272
- User log files, 296

V

- Vandalism, 272
- Vanity, 160, 161
- Vendor/partner networks, 114–115
- Vendors, 82–84
- Virtual disguises, 84–86
- Void element, 158
- VoIP, eavesdropping on, 220
- VPN connections
 - site-to-site, 115
 - split tunneling on, 113–114
- Vulnerability
 - exploitation, 190–192
 - identification, 189–190

W

- Waging War
 - prolonged attacks, 46–47
 - rousing anger, 47–48
 - victory, 48
- Warfare, deception, 44–46
- Water element, 158
- Wavebubble, 261, 261*f*
- Weapons, 20–21
 - ninja, 16–18
 - samurai, 8
- Web hacking, 192–194

Web sites, shell, 172–176
Weighted chain, 17
White Hat hackers, 28–29. *See also* Black Hat hackers
Wind element, 158
Windows, user account control (UAC), 216–218
Windows Resource Monitor, 219*f*
Wireless attacks, 194–195
Wireless mesh network, 86

Wireless security surveys, 137–138
Wireshark Protocol hierarchy, 139*f*
Wiretapping, 258

X

X.509 standard, 99

Y

Yagi rifles, 208, 208*f*