

# INDEX

## Symbols and Numbers

<form> tags, 122  
220 message, 116  
250 message, 116  
389 Directory Server, 313

## A

ACK flags, 63  
ACK packets, 49  
Active Directory service, attacking,  
313–318  
address resolution protocol (ARP),  
17–20  
Advanced Encryption Standard (AES),  
75  
-aes-256-ctr flag, 75  
AES-GCM (Galois/counter mode), 104  
AF\_INET6 parameter, 55  
AF\_INET parameter, 55  
AFL (American Fuzzy Loop), 170  
Ahmed, Humaeed, 206  
air-gapped machines, 333  
Ajax spider, 276  
American Fuzzy Lop (AFL), 170  
American Registry for Internet  
Numbers (ARIN), 153  
American Standard Code for  
Information Interchange  
(ASCII), 69  
Android Package (APK), 208  
Android Runtime (ART), 210  
Android Studio, 212  
Angr, 179–182  
animation, of static images, 124–127  
anonymous binds, 315  
antivirus tools  
evading with encoders, 200–205  
evading with -i flag, 190  
APK (Android Package), 208  
apktool, 208  
*apktool.yml* file, 209  
Apple Open Directory, 313

application layer, 35  
ARIN (American Registry for Internet  
Numbers), 153  
Armitage, 237–240  
ARP (address resolution protocol),  
17–20  
ARP spoofing attacks  
detecting, 26  
inspecting ARP tables, 27  
performing, 20–25  
arp spoof tool, 23–25  
ART (Android Runtime), 210  
artificial neural networks, 125  
ASCII (American Standard Code for  
Information Interchange), 69  
associative operators, 70  
asymmetric cryptography, 76  
authenticated encryption with  
associated data, 104  
authentication, two-factor, 137  
authentication servers, 318

## B

backdoors  
dbd backdoor, 199  
detecting, 151  
exploiting in Metasploitable, 11–14  
installing, 199  
vsftp backdoor, 54, 57  
banners, reading information in, 141  
Barnhouse, Kyle, 199  
base64 encoding, 201  
Bash Bunny, 334  
BeEF. *See* Browser Exploitation  
Framework (BeEF)  
bettercap tool, 107  
Bezos, Jeff, 215  
big-endian format, 165  
binaries, creating executable, 179  
bind function, 57  
binding, 315  
Bitcoin blockchain, 326

- Bitcoin wallets, 325
- blind injection attacks, 249
- block cipher modes, 72
- block ciphers, 75
- BloodHound, 317
- Boer, Bert den, 259
- Boneh, Dan, 98
- Bosselaers, Antoon, 259
- Botnet Architectures, 60
- botnets, 58–61
- Browser Exploitation Framework (BeEF), 278–281
  - control panel, 280
  - fake Google login screen, 280
  - injecting the BeEF Hook, 278
  - login screen, 278
  - social engineering attacks with, 279
- browsers, exploiting, 281
- Brueggemann, Maik, 335
- brute-force attacks
  - Hashcat tool, 262
  - web logins, 265
- buffer overflow attacks, 160
- buffer over-read attacks, 160
- bug bounty programs, 285
- bugs, exploiting, 160, 167
- Burp Suite, 266

**C**

- Caesar cipher, 68
- CAINE (Computer Aided INvestigative Environment), 334
- CAM (content addressable memory), 29
- cameras, controlling, 138
- carriage return character (<CR>), 117
- carrier sense multiple access protocol, 36
- case studies
  - exploiting Heartbleed OpenSSL vulnerability, 160
  - exploiting older versions of Chrome browser, 281
  - re-creating Drovorub using Metasploit, 188–193
- cellular infrastructure, attacking, 333
- Center for Internet Security (CIS), 329
- certificate authorities, 93
- certificate validation process, 93
- CFAA (Computer Fraud and Abuse Act), 138
- challenge-response nonces, 309
- Chang, Oliver, 281
- chkrootkit, 330
- Chrome browser, exploiting, 281
- CIDR (classless inter-domain routing) notation, 19
- cipher text, 68
- CIS (Center for Internet Security), 329
- classless inter-domain routing (CIDR) notation, 19
- clauses, in SQL injection, 246
- Client Hello* message, 90, 161, 164
- Client Random* message, 163
- client-server model, 52
- Client TLS Version, 163
- CNC (command and control) servers, 56
- code segment (CS) register, 226
- Colab notebooks, 124–127
- collisions, when hashing passwords, 256
- command and control (CNC) servers, 56
- Common Vulnerabilities and Exposures (CVE) database, 147
- Computer Aided INvestigative Environment (CAINE), 334
- Computer Fraud and Abuse Act (CFAA), 138
- concolic execution, 176
- concrete values, 176
- content addressable memory (CAM), 29
- Cookie Quick Manager, 273
- cookies
  - in HTTP requests, 251
  - stealing users, 271
- copy-on-write (COW) procedure, 301
- corporate networks, exploring, 310
- correlation attacks, 325
- counter mode block cipher (CTR), 74
- cr0 register, 230
- crawling, 276
- credential databases, leaked, 136
- Crenshaw, Adrian, 247
- cross-device tracking, 334

- cross-site scripting (XSS), 270–276
  - DOM XSS attacks, 270
  - example template, 270
  - malicious JavaScript, 270
  - reflected attacks, 275
  - stored attacks, 270, 273
- cryptocurrencies, 326
- cryptographic hash function, 91
- cryptography
  - lattice-based, 98
  - public-key, 76, 80
- CS (code segment) register, 226
- CVE (Common Vulnerabilities and Exposures) database, 147

## D

- databases, leaked, 136
- data link layer (IP stack)
  - application layer, 35
  - physical layer, 36
  - transport layer, 35
- dbd backdoor, 199
- DC sync attacks, 321
- DDoS (distributed denial of service)
  - attacks, 59–61
- .deb* file, 193
- debian-cis, 329
- deepfake videos, creating, 123–127
- denial of service (DoS) attacks, 170
- developer tools, 271
- .dex* file, 210
- dictionary-based attacks, 248
- Diffie-Hellman algorithm, 94–104
  - attacking, 100
  - calculating shared secret keys, 98
  - elliptic-curve, 100
  - exchanging key shares and nonces, 98
  - generating public-private key pairs, 96
  - generating shared parameters, 95
  - key derivation, 99
- dig command, 115
- digital subscriber line access
  - multiplexer (DSLAM), 20
- dirb tool, 248
- directory information trees (DITs), 313
- directory services, 313
- Dirty COW vulnerability, 300–303

- Discover tool, 152–154
- distributed denial of service (DDoS)
  - attacks, 59–61
- DMARC (domain-based message authentication, reporting, and conformance), 119
- DNS (Domain Name System), 32, 311–313
- dnsrecon tool, 153
- document object model (DOM), 272
- domain-based message authentication, reporting, and conformance (DMARC), 119
- domain controllers
  - Active Directory and LDAP services, 313–318
  - DNS service, 311–313
  - Kerberos protocol, 318
  - LSSAS process, 306–308
  - network exploration, 310
  - NT LAN Manager, 309
  - purpose of, 305
- Domain Name System (DNS), 32, 311–313
- domains, defined, 310
- DOM XSS attacks, 270
- DoS (denial of service) attacks, 170
- double and add algorithm, 102–103
- driver software, 222
- driving video, 124
- Drovorub malware, 187–193
- Druin, Jeremy, 247
- DSE (Dynamic Symbolic Execution), 176
- DSLAM (digital subscriber line access multiplexer), 20
- dsniff tool, 22
- dual-homed devices
  - adding NAT to, 303
  - pivoting from, 290–298
- dynamic host configuration protocol (DHCP), 292
- Dynamic Symbolic Execution (DSE), 176–182

## E

- Eagle, Chris, 334
- electronic code book (ECB) cipher mode, 72

- Electronic Frontier Foundation, 26
  - elliptic-curve cryptography (ECC), 100
  - Elliptic Curve Diffie-Hellman, 104
  - elliptic curves, 100–104
  - emails, faking, 121
  - encapsulation, 34
  - encoders
    - evading antivirus software with, 200–205
    - polymorphic, 202, 205
    - purpose of, 200
  - encoding, strings into binary format, 56
  - encrypted SIMs, 138
  - encryption
    - authenticated with associated data, 104
    - encrypting and decrypting files, 75–76
    - encrypting files with RSA, 79
    - modifying encrypted messages, 91
    - plaintext versus cipher text, 68
    - purpose of, 68
    - symmetric key cryptography, 83–85
  - entities, 133
  - entry nodes, 324
  - enumeration, 314
  - escaping, 247
  - ESMTP (extended simple mail transfer protocol), 116
  - eth0 (Ethernet interface), 23, 250
  - event-driven modules, 223
  - Evil-Droid script, 216
  - exclusion lists, 139–140
  - exclusive OR (XOR), 68
  - executable binaries, creating, 179
  - execution
    - concolic, 176
    - concrete values, 176
  - exit nodes, 324
  - Exploit DB, 146
  - exploits. *See also* Browser Exploitation Framework (BeEF)
    - backdoors, 11
    - creating, 160–167
    - older versions of Chrome browser, 281
    - vulnerable services, 54
  - extended Euclidean algorithm, 78
  - extended simple mail transfer protocol (ESMTP), 116
- ## F
- fail2ban, 330
  - faking emails, 114–121
  - faking videos, 123–127
  - faking websites, 121–123
  - Faraday cages, 333
  - FBI honey pots, 140
  - Fernet module, 84
  - Feynman, Richard, 184
  - files
    - encrypting and decrypting, 75
    - encrypting with RSA, 79
    - enumerating on web servers, 248
    - hiding, 234–236
  - file transfer protocol (FTP), 35
  - filter function (data packets), 39–42
  - FIN-ACK package exchange, 49–50
  - FIN scans, 53
  - Firestore, 264
  - Firefox Headless option, 276
  - firewalls
    - bypassing with TCP-FIN packets, 53
    - reverse shells and, 51
  - first-degree connections, 132
  - forensics, 334
  - forks, creating, 56
  - forward secrecy, 105
  - Foster, Jeff, 168
  - fragmentation, 160
  - FreeIPA virtual machine, 315
  - FTP servers, breaking into machines through, 263
  - full duplex communication, 50
  - fuzzing, 168–174
    - American Fuzzy Lop (AFL), 170
    - creating test cases, 172
    - example of, 168
    - writing your own fuzzer, 169
- ## G
- general number field sieve (GNFS), 100
  - generators, 95
  - genetic algorithms, 170–171
  - genpkey program, 95

- genrsa, 79
- getdents64 function, 236
- GET request, 251
- Ghidra, 334
- GNFS (general number field sieve), 100
- Goetz, Michael, 333
- golden ticket attacks, 321
- goofile, 153
- Google Colab, 124–127
- Google Dorking, 138
- Graham, Robert, 139
- GRU (Russian military intelligence), 187

## H

- Hacker News, 335
- Hackerone.com, 285
- hacking community, 335
- hacking servers. *See also* servers
  - auditing hardened servers, 331
  - hardening process, 329
  - installing tools, 328
  - remaining anonymous, 324
  - setting up, 324
  - SSH set up, 326–328
  - virtual private servers, 326
- Hack the Box, 335
- Hak5 field kit, 334
- half duplex communication, 50
- Hanspach, Michael, 333
- hardening, 329
- hardening process, 329
- hash-based message authentication codes (HMACs), 91
- Hashcat, 262
- hash function, 91
- Hashcat, 262
- hashing passwords, 256–261
  - building salted hash crackers, 260
  - collisions, 256
  - cracking hashes, 259
  - extracting passwords on Linux, 298–300
  - extracting with Mimikatz, 306–308
  - popular tools, 261
  - salting hashes with a nonce, 260
- haveibeenpwned, 136
- header fields, 32

- Heartbeat extension, 160
- Heartbeat packets, 165
- Heinrichs, Hanno, 304
- hiding files, 234–236
  - hooking code, 235
  - linux\_direct struct, 234
- HKDF key derivation, 99
- HMAC (hash-based message authentication codes), 91
- Holland, John, 171
- honey pots, 140
- Honig, Andrew, 334
- hooking, 222, 229–236
- hook.js file, 279
- HSTS (HTTP Strict Transport Security) bypass, 107
- HTTPS Everywhere extension, 26
- https.server utility, 122
- Hydra, 263
- hypertext transfer protocol (HTTP)
  - purpose of, 35
  - requests and responses, 250

## I

- ICA (intermediate certificate authority), 93
- ICMP (internet control message protocol), 36
- identity element property, 70
- i flag, 190
- images
  - animating static, 124
  - encrypted with ECB, 73
- impacket collection, 321
- IMSI (international mobile subscriber identity), 333
- InCommon, 94
- industrial systems, hacking, 335
- Infectious Media Generator, 207
- injection attacks, 246–247
- inodes, 235
- input, sanitizing, 247
- installers, modifying to carry trojans, 193
- intermediate certificate authority (ICA), 93
- international mobile subscriber identity (IMSI), 333

- internet control message protocol (ICMP), 36
- Internet of Things (IoT) devices, 59
- internet protocol version 6 (IPv6), 144
- internet service provider (ISP), 20
  - inurl filter, 138
- IoT (Internet of Things) devices, 59
- IP (internet protocol)
  - address prefixes, 20
  - communication between systems
    - using, 31–33
  - five-layer stack, 33–36
  - internal IP addresses, 145
  - IP addresses, 18–20, 311
- IP forwarding, 22, 303
- iptables, 330
- IPv4 address, 19
- IPv4 TCP socket, 56
- IPv6 (internet protocol version 6), 144
- IPv6 address, 145

## J

- jarsigner utility, 211
- Java Development Kit (JDK), 211
- Java Keystore, 211
- John the Ripper, 261
- Jshielder, 329

## K

- Kali Linux, 10
- Kali Linux browser, 13
- Kennedy, David, 328
- Kerberoasting attacks, 322
- Kerberos protocol, 318–322
- kernel mode, 226
- kernel module, 188
- kernel space, 226
- key derivation, 72
- keyloggers, 218, 240
- key point extraction algorithm, 124
- keys
  - calculating shared secret keys, 98
  - computing shared keys, 94–100
  - encryption using, 68
  - private keys, 76
  - public-key cryptography, 76, 80
  - sharing public keys in TLS, 90

- key space, 68
- Keystore (Java), 211
- keytool utility, 211
- King Phisher, 127
- Kryptos statue, 86

## L

- LAN (local area network), 20
- LAN Turtle, 334
- lattice-based cryptography, 98
- Lazarus group, 208
- leaked credential databases, 136
- LHOST (listening host), 189
- Lightweight Directory Access Protocol (LDAP), 313–318
- linear congruential generator (LCG), 71
- line feed (<LF>) character, 117
- link analysis, 132–133
- linker, 224
- Link-Local Multicast Name Resolution (LLMNR), 311
- Linux
  - extracting password hashes on, 298–300
  - installing headers, 224
  - linux\_direct struct, 234
  - writing kernel modules, 222–226
- live cameras, locating, 138
- LLMNR poisoning attacks, 311
- lo (loopback) interface, 37
- local area network (LAN), 20
- Local Security Authority Subsystem Service (LSSAS), 306
- loopback interface (lo), 37
- ls command, 58
- lsmod command, 225, 243
- Lynis, 331

## M

- MAC addresses, 18
- MAC flooding, 29
- machines, accessing, 52
- macros, 208
- Magnet links, 136
- mail exchanger (MX), 115
- mail servers, 114
- Maltego, 133–136

- malware
  - analyzing, 334
  - avoiding detection, 236
  - evading detection, 200–205
  - hiding implants in legitimate files, 193–199
  - Stuxnet malware, 335
  - Triton malware, 335
- man-in-the-middle attacks, 334
- masks, 263
- Masscan, 139–144
- Matthes, Eric, xxii
- maximum transmission unit (MTU), 160
- md5sums file, 195
- MDXfind, 263
- media access control (MAC) protocol, 36
- message authentication, 91–92
- Metasploitable, 8–9
- Metasploit Framework, 153, 188–193, 294–297
- Meterpreter, 188, 191
- Miller, Barton, 168
- Mimikatz, 306–308
- Mirai botnet, 59
- modules
  - event-driven, 223
  - Fernet module, 84
  - self-hiding, 243
- MongoDB, 264
- motion detection, 124
- Mousepad editor, 55
- msfconsole, 189
- msfvenom, 187, 190
- MTU (maximum transmission unit), 160
- multiclient bot server, 61
- Mutillidae, 247
- MX (mail exchanger), 115

**N**

- Naik, Mayur, 175
- Nance, Kara, 334
- NAT (network address translation), 145–146, 303
- National Institute of Standards and Technology (NIST), 101, 147
- National Telecommunications and Information Administration (NTIA), 132
- National Vulnerability Database (NVD), 54, 147
- Nessus, 148
- Netbios Name Service (NBT-NS), 312
- Netcat (nc), 13
- netdiscover tool, 12, 22
- network address translation (NAT), 145–146, 303
- network interface card (NIC)
  - capturing and viewing packets from, 37
  - intercepting and parsing packets from, 26
  - network connections through, 23
  - purpose of, 18
  - web requests and, 20
- network layer, 36
- networks, exploring corporate, 310
- networks, hierarchy of, 19
- Nexpose, 148, 294
- NIC. *See* network interface card (NIC)
- NIST (National Institute of Standards and Technology), 101, 147
- nixarmor, 329
- nmap tool
  - enumerating files and folders, 152
  - identifying operating systems, 152
  - listing installed scripts, 152
  - scanning all common ports, 152
  - scanning for open ports, 52–53
  - scanning for vulnerabilities, 152
- nonces, 74, 98
- NoScript, 325
- NoSQL injection, 264
- NoSQLMap, 265
- NPCAP library, 37
- NTIA (National Telecommunications and Information Administration), 132
- NT LAN Manager (NTLM) protocol, 309
- NVD (National Vulnerability Database), 54, 147

## O

- OAEP (optimal asymmetric encryption padding), 78, 81–82
- Oester, Phil, 300
- one-time pad algorithm, 68–71
- one-way functions, 256
- OpenCV library, 217
- open source intelligence (OSINT), 131
- openssl library, 79
- optimal asymmetric encryption padding (OAEP), 78, 81–82
- organizational units (OUs), 310
- OWASP (Open Web Application Security Project), 249
- OWASP Zed Attack Proxy (ZAP), 276

## P

- P-256 elliptic curve, 101
- packet, 18
- Packet Length, 163
- packets
  - bypassing firewalls with, 53
  - filtering, 39–42
  - fragmented, 160
  - purpose of, 18
- padding algorithm, 82
- pass-the-hash attacks, 303, 309
- pass-the-ticket attacks, 320
- Password-Based Key Derivation Function 2 (PBKDF2), 72
- password binds, 315
- passwords
  - building salted hash crackers, 260
  - collisions when hashing, 256
  - cracking hashes, 259
  - editing read-only files, 301–303
  - extracting hashes on Linux, 298–300
  - extracting hashes with Mimikatz, 306–308
  - hash cracking tools, 261
  - stealing from websites, 247–250
- path constraints, 174
- PAYLOAD flag, 189
- peers, 136
- peer-to-peer (P2P) model, 52
- PenTesters Framework (PTF), 328
- periods, in pseudorandom number generation, 72

- PF\_RING* ZC driver, 139
- pfSense, 3–8, 43–45
- phishing attacks, 113, 127
- physical hacking tools, 334
- physical layer, 36
- pipng, 60
- pivoting
  - from dual-homed devices, 290, 294
  - with Metasploit, 294–297
- pkeyparam program, 96
- pkey utility, 97
- PKI (public key infrastructure), 93
- plaintext, 68
- PLC-Blaster, 335
- PLCs (programmable logic controllers), 335
- polymorphic encoders, 202, 205
- port numbers, 32
- PostgreSQL, 189
- postint* file, 195
- POST requests, 251
- powershell\_base64 encoder, 201
- private keys, 76
- privilege escalation attacks, 303
- privileged state, 223
- privilege escalation attacks, 300
- privilege levels, 226
- processes, defined, 33
- programmable logic controllers (PLCs), 335
- Project Zero, 168
- protocols
  - defined, 31
  - sequence diagram, 32
- Protonmail, 133
- proxies, 294, 297
- ps command, 192
- pseudorandom generators (PRGs), 71–72
- PTF (PenTesters Framework), 328
- public key, 80
- public-key cryptography, 76–78
- public key infrastructure (PKI), 93
- pwd command, 58
- pyca/cryptography library, 86
- pymongo library, 264
- python-af1 program, 171
- Python Cryptography Authority, 83
- python-mss library, 218



## Q

QR codes, 215  
quantum algorithm, 80  
quantum computation, 335  
quantum-safe encryption algorithms,  
98  
query string parameters, 251

## R

race conditions, 301  
random fuzzing, 169  
randomness, 71  
ransomware  
    adding encryption to server, 108  
    description of, 67  
    extending the client, 86  
    implementing servers, 85  
    writing, 82–85  
RCE (remote code execution), 160  
Recon-ng tool, 153  
Redhawk, 333  
reflected XSS attacks, 275  
remote code execution (RCE), 160  
Reptile, 243  
Responder tool, 312  
reverse engineering, 334  
reverse shell clients, writing, 54–56  
reverse shell programs, 47  
reverse shells, 51, 326  
RFC 5246, 162  
Rivest–Shamir–Adleman (RSA) theory,  
77  
rkhunter, 330  
rmmmod command, 226  
*robots.txt* file, 138  
rootkits, 192, 221, 237–240, 282–285,  
330  
root privileges, 301  
routers, 18  
routers, hierarchy of, 19  
rsaut1 utility, 80  
rtorrent utility, 137  
Russian military intelligence (GRU),  
187

## S

salt, 260  
same origin policy, 271

Sanborn, Jim, 87  
sandboxing, 281  
sanitizing input, 247  
SASL (Simple Authentication and  
Security Layer) binds, 315  
scanning the internet  
    Masscan, 139–141  
    reading banner information,  
141–144  
    Shodan, 143  
    using an exclusion list, 139  
Scapy, 26–27  
Schwartke, Hendrik, 335  
screenshots, 218  
SDRs (software-defined radios), 332  
SecLists, 260  
second-degree connections, 132  
secp256k1 curve, 101  
Sectigo, 94  
secure block ciphers modes, 74–75  
secure sockets layer (SSL) library,  
104–106  
SELECT queries, 246  
self-hiding modules, 243  
self-inversive operators, 70  
SELinux, 331  
sequence number, 48  
*Server Done* message, 161  
*Server Hello* message, 90  
servers. *See also* hacking servers  
    adding encryption to, 108  
    auditing after hardening, 331  
    breaching into machines through,  
263  
    enumerating files on, 248  
    hardening for protection, 329  
    implementing ransomware servers,  
85  
Service Name and Transport Protocol  
Port Number Registry, 52  
services, exploiting vulnerable, 54  
Session ID, 163  
SET (Social Engineering Toolkit), 207  
Shark Jack, 334  
Sharpshound, 317  
shells, 12  
Shikata Ga Nai (SGN) Encoder, 204  
Shodan, 143–144  
Shor, Peter, 80

- Shor's quantum algorithm, 335
- Shoshitaishvili, Yan, 179
- Shoup, Victor, 98
- showkey command, 241
- Siarohin, Aliaksandr, 123
- signature algorithms, 92
- signature detection, 200
- signed hashes, 91
- signing, in public-key cryptography, 77
- Sikorski, Michael, 334
- SIM jacking, 137–138
- Simple Authentication and Security Layer (SASL) binds, 315
- simple mail transfer protocol (SMTP), 115
- smali* folder, 209
- smtp lib library, 119
- SMTPS (SMTP secure), 115, 119, 128
- social engineering
  - Android trojans, 208–215
  - attacks using BeEF, 279
  - fake emails, 114–121
  - fake videos, 123–127
  - fake websites, 121–123
  - link analysis, 132–138
  - trojans, 193–199
  - Windows trojans, 206–208
- Social Engineering Toolkit (SET), 207
- SOCK\_DGRAM parameter, 55
- sockets
  - defined, 48
  - process communication and, 48–52
- SOCK\_STREAM parameter, 55
- software-defined radios (SDRs), 332
- source URL, 272
- Spenneberg, Ralf, 335
- SPF (Symbolic PathFinder), 176
- spidering, 276
- spike fuzzer, 183–184
- spike tool, 183
- spoofing
  - ARP spoofing attacks, 20–25
  - emails, 114–121
- Springer, Jake, 182
- SQL injection, 245–256
- SQLMap, 254–256
- squatting, 123
- SSL (secure sockets layer) library, 104–106
- SSL stripping, 107
- state actors, 94
- state-level actors, 325
- Stingray, 333
- stored XSS attacks, 270
- Stuxnet malware, 335
- subdomains, 107
- subprocesses, 56
- swaks tool, 128
- symbolic execution, 174–176
- Symbolic PathFinder (SPF), 176
- symbolic registers, 182
- SYN-ACK packets, 49
- SYN scans, 53, 62–63
- System Bus Radio, 334
- system calls (syscalls), modifying, 226–230

## T

- Tacotron 2, 127
- Tails, 325
- TCP (transmission control protocol)
  - clients and servers, 51
  - conversation filtering, 41
  - full duplex communication, 50
  - handshakes, 48
  - reverse shell, 50
  - TCP streams, 41–42
  - three-way handshake diagram, 49
  - three-way handshakes, 49
- tcpdump tool, 42
- template engines, 270
- theHarvester, 153
- theorem provers, 174–175
- thread library, 108
- ticket-granting services, 318
- timestamp, 43
- TLS (Transport Layer Security)
  - handshake packets, 162
  - message exchange, 90–93
  - TLS 1.2, 100, 161
  - writing TLS sockets, 104
- tools, installing, 328
- Tor Browser Bundle, 325
- Tor Directory Authorities, 324
- torrent files, 136
- traceroute, 154
- traceroute tool, 36
- Transform Hub, 135

- transforms, 133
- transmission control protocol. *See* TCP (transmission control protocol)
- transmission medium, 36
- transport layer, 35–36
- Transport Layer Security. *See* TLS (Transport Layer Security)
- transposition, 86
- trapdoors, 77
- Triton malware, 335
- trojans
  - building with Metasploit, 188–193
  - creating Android trojans, 208–215
  - creating Windows trojans, 206–208
  - defined, 187
  - evading virus detection, 200–205
  - hiding implants in legitimate files, 193–199
  - practice exercises, 215–219
- try finally keywords, 84
- tuples, 55
- two-factor authentication, 137

## U

- Ubuntu, 10–11
- Uncomplicated Firewall, 330
- unsolved codes, 86
- URLCrazy, 119, 153
- urLsnarf, 24
- USB Rubber Ducky, 334
- user datagram protocol (UDP), 36

## V

- vftpd vulnerability, 239
- victim machines, accessing, 52
- videos, creating deepfake, 123–127
- Vigenère cipher, 86
- Vigna, Giovanni, 179
- VirtualBox, 3
- virtual memory, 301
- virtual private servers (VPSs), 324, 326
- Virus Total, 200
- voice cloning, 127
- vsftpd backdoor, 11, 54, 57
- vulnerabilities
  - Dirty COW, 300
  - exploiting services, 54
  - finding with Zed Attack Proxy, 276

- scanning for, 152
- vulnerability databases, 146
- vulnerability scanners, 148–151
- vulners script, 152

## W

- webcams, controlling, 217–218
- Webshells, 260
- websites
  - faking, 121–123
  - installing rootkits, 282–285
  - stealing passwords from, 247–250
- weights, 125
- whatweb, 154, 277
- whois database, 132, 153
- Wi-Fi Pineapple, 334
- Windows
  - attacking Active Directory and LDAP services, 313–318
  - attacking DNS service, 311–313
  - creating virtual labs, 306
  - exploring corporate Windows networks, 310
  - extracting password hashes, 306–308
  - Kerberos protocol, 318
  - pass-the-hash attacks, 309
- Wireshark, 36–42
- with keyword, 84
- wlan (wireless LAN), 23
- write-protect (WP) flag, 230
- writing a SQL injection tool, 250–254

## X

- XMas scans, 53–54
- XOR (exclusive OR), 68
- XSS. *See* cross-site scripting (XSS)
- xxd command, 200

## Z

- Z3 theorem prover, 174
- Zalewski, Michal, 170
- ZED Attack Proxy (ZAP), 276
- zero-click vulnerabilities, 215
- zero-day vulnerabilities, 54
- Zerodium, 54
- zipbombs, 260
- Zsolnai-Fehér, Károly, 124