

INDEX

Page numbers referring to figures or tables are italicized.

Symbols

& (ampersand), 68
= (assignment symbol), 79
* (asterisk), 173
: (colon), 78, 194
\$ (content symbol), 78–79, 87, 91
- (dash), 19–20, 52, 62, 173, 175
-- (double dash), 7
.. (double dots), 6
>> (double redirect symbol), 13
(hash mark), 84–85, 186
./ notation, 85–86, 185
| (pipe), 12. *See also* piping
> (redirect symbol), 13, 35, 89
; (semicolon), 131, 133
#! (shebang), 84, 86

A

accept method, 192
access lists, 127
access points. *See* APs
admin account. *See* root account
Advanced Packaging Tool. *See* apt
AI (artificial intelligence), 201–207
 augmentation and creation of
 cybersecurity roles, 202–203
 collaboration with, 202–203
 limitations of, 202
 major players in, 203
 social engineering attacks with, 205–206
 using in cybersecurity, 203–204
 writing bash scripts with, 206–207
aircrack-ng suite and aircrack-ng
 command, 7–10, 30, 155–157
aireplay-ng command, 157
airmon-ng command, 156

airodump-ng command, 156–157
Akira, 204
Aloha POS (Point of Sale) system, 88
ampersand (&), 68
anonymity, 137–149
 email encryption, 148–149
 proxy servers, 141–147
 adding proxies, 145
 dynamic chaining, 145
 random chaining, 146
 running traffic through, 141–142
 security concerns, 147
 setting proxies in config files,
 142–144
Tor system, 139–141
 Ahmia search engine, 141, *141*
 dark web, 140–141
 encrypted traffic data, 139–140
 installing Tor browser, 140, *140*
 security concerns, 141
 tracking methods, 138
 VPNs, 147–148
Anthropic, 203
Apache, 123–127
 creating HTTP servers with,
 124–127
 adding HTML blocks, 126
 editing the *index.html* file, 125–126
 finished product, 126–127
 default web page, 125, *125*
 downloading and installing, 124
LAMP, 125
logs
 deleting, 118
 viewing, 116
 running, 125
APs (access points), 152–158
 connecting to, 154–155
 cracking, 155–157
 viewing, 153–154

- apt (Advanced Packaging Tool), 40–43
 - adding software, 40–41
 - removing software, 41–42
 - searching for packages, 40
 - updating packages, 42
 - upgrading packages, 42–43
 - apt command, 40–42
 - GUI-based software installers, 45–46
 - installing software, 40–41
 - removing software, 41
 - searching for packages, 40
 - updating packages, 42
 - upgrading packages, 42
 - APTs (advanced persistent threats), 204
 - archiving, 100–101
 - bit-by-bit or physical copies, 100–101
 - tarring files together, 96–98
 - ARM architecture, downloading Kali
 - Linux for, xxviii
 - arrays, 188, 194
 - artificial intelligence. *See* AI
 - assignment symbol (=), 79
 - asterisk (*), 173
 - a switch
 - ls command, 7
 - modprobe command, 168
 - netstat command, 29, 29, 30
 - at command, 69, 69
 - at daemon (atd), 69
 - ATT Protocol (Low Energy Attribute Protocol), 161
 - aux switch, 12, 62–63
- B**
- bad blocks, 110
 - banner grabbing, 191–192, 196–197
 - bash shell (Bourne-again shell),
 - xx, 2, 81–93
 - changing default shell to, 72–73, 82–83
 - common built-in commands, 92
 - open port scanning script, 87–91
 - flexible version, 90–91
 - local version, 89
 - target of, 88
 - simple message script, 84–87
 - adding functionality, 86–87
 - commenting, 84–85
 - running, 85–86
 - setting execute permissions, 85
 - using AI for scripting, 206–207
 - basic service set identifier (BSSID), 152, 154–158
 - Berkeley Internet Name Domain (BIND), 34
 - bg command, 68, 92
 - binaries
 - adding to PATH variable, 79
 - defined, 2
 - directories for, 4, 4
 - finding
 - whereis command, 9
 - which command, 9–10
 - location of, 2
 - binary representation of permissions, 53, 53
 - BIND (Berkeley Internet Name Domain), 34
 - /bin directory, 4, 4
 - black hat hackers, 87–88
 - block devices, 107–108
 - defined, 107
 - listing, 107–108
 - Bluetooth, 158–162
 - confirming device reachability, 161–162
 - defined, 158
 - discoverable mode, 158
 - kernel module, 168
 - pairing, 158
 - scanning for devices, 158–161
 - BlueZ, 158–162
 - hciconfig tool, 159
 - hcidump tool, 159
 - hcitool tool, 159–160
 - l2ping command, 161–162
 - sdptool tool, 160–161
 - /boot directory, 4
 - Bourne-again shell. *See* bash shell
 - break command, 92
 - broadcast addresses
 - changing, 31–32
 - defined, 28
 - viewing, 28
 - bs option, 100

BSSID (basic service set identifier),
152, 154–158
bunzip2 command, 99
Butler, Max (Max Vision), 88
bzip2 command, 98–99

C

Cactus, 204
CardersMarket, 88
case sensitivity, 2, 62
cat command
 checking kernel version, 165
 creating files, 12–14
 filtering text, 21–22
 viewing files, 18
cd command, 6, 92
CERN, 149
CERT (Computer Emergency
 Response Team), 88
channels, 152
character devices, 107
ChatGPT, 203
check command, 156
chgrp command, 51
chmod command, 52, 54–58, 85, 87,
 89, 185, 191–192
 decimal notation, 54
 group permissions, 58
 temporary permissions, 57
 UGO syntax, 54–55
chown command, 50
classes, 189–190
Claude 2, 203
cloud vulnerabilities, 203
colon (:), 78, 194
commenting, 84–85, 186–187
compress command, 98–99
compression, 95–99
 bzip2 command, 98–99
 compress command, 98–99
 defined, 96
 gzip command, 98–99
 lossy vs. lossless, 96
 tarring files together, 96–98
Computer Emergency Response Team
 (CERT), 88
connect() function, 191
content symbol (\$), 78–79, 87, 91

continue command, 92
control block, 194
control statements, 194–195
 if...else structure, 194–195
 if structure, 194
Copilot, 203
cp command, 14
CPUs
 identifying, xxviii
 process management, 62–64
 Raspberry Pi, 128
cron daemon (crond), 68–69,
 172, 174
crontab file, 172–176
 scheduling backup tasks, 174–175
 scheduling jobs to run automatically,
 172–174
 scheduling *MySQLScanner*, 175–176
 shortcuts, 176
cron table (crontab), 172, 172, 173, 175
cross-site scripting (XSS), 124
cryptocurrency-related attacks, 204
-c switch
 airodump-ng command, 157
 tar command, 97
cyber threat intelligence, 203

D

Daixin Team, 204
dash (-), 19–20, 52, 62, 173, 175
dd command, 100
delete command, 131
deleting
 environment variables, 80
 logs, 118
denial-of-service (DoS) attacks, 31
describe statement, 134
/dev directory, 4, 104–107
 block devices, 107–108
 character devices, 107
 logical labels, 105, 105–106
 major and minor numbers,
 105–106
 mount points, 108
 partitions, 105–107
 USB devices, 108
df command, 109–110
dhclient command, 32–33

- DHCP (Dynamic Host Configuration Protocol) servers
 - assigning new IP addresses from, 32–33
 - DNS settings, 35
 - dictionaries, 193–194
 - dig command, 33–34
 - directories. *See also* permissions
 - changing, 6
 - creating, 14
 - defined, 2
 - identifying current, 5
 - listing contents of, 6–7
 - removing, 15
 - viewing current in shell
 - prompt, 77
 - disabling logging, 120
 - dmesg command, 169
 - DNS (Domain Name System), 32–33, 124
 - changing servers, 34–35
 - examining, 33–34
 - mapping IP addresses, 35–36
 - dnsspoof tool, 35–36
 - DoS (denial-of-service) attacks, 31
 - double dash (--), 7
 - double dots (..), 6
 - double redirect symbol (>>), 13
 - dynamic chaining, 145
 - Dynamic Host Configuration Protocol servers. *See* DHCP servers
- E**
- echo command, 84, 86–87, 92
 - PATH variable, 78–79
 - prompting for user input, 90
 - user-defined variables, 79–80
 - 8Base, 204
 - ejecting (unmounting) devices, 109
 - email encryption, 148–149
 - env command, 74
 - environment variables, 71–80
 - adding directories to PATH variable, 78–79
 - case sensitivity, 73
 - changing default shell to bash, 72–73
 - changing shell prompt, 76–77
 - creating user-defined variables, 79–80
 - defined, 71
 - deleting, 80
 - filtering, 75
 - values
 - changing for a session, 75
 - making changes permanent, 76
 - viewing
 - all default variables, 74
 - all variables, 74–75
 - ESSID (extended service set identifier), 152
 - /etc directory, 4, 4
 - ethical hacking. *See* white hat hacking
 - Ettercap, 36
 - eval command, 92
 - exception handling, 197–199
 - exec command, 92
 - exFAT (Extended File Allocation Table), 106–107
 - exit command, 92
 - exit() function, 187
 - export command, 76–77, 92
 - extended service set identifier (ESSID), 152
- F**
- FAT (File Allocation Table), 107
 - fd0 drive label, 105
 - fdisk utility, 106–107
 - fg command, 68, 92
 - files. *See also* permissions
 - appending content to, 13
 - archiving, 96–98, 100–101
 - compressing, 95–99
 - copying, 14
 - creating, 12–14
 - finding, 8–12
 - numbering lines, 20–21
 - overwriting, 13–14
 - removing, 15
 - renaming, 14–15
 - viewing
 - first lines, 18–19
 - last lines, 19–20
 - one page and paging down, 23
 - one page and scrolling or filtering, 24–25

- filesystem, 3–4
 - /bin* directory, 4
 - /dev* directory, 104–107
 - /etc* directory, 4
 - /home* directory, 2, 4
 - /lib* directory, 4
 - /media* directory, 4, 108–109
 - /mnt* directory, 4, 108–109
- monitoring
 - checking for errors, 110–111
 - viewing information about
 - mounted disks, 109–110
- navigating
 - changing directories, 6
 - identifying current
 - directory, 5
 - listing directory contents, 6–7
 - /root* directory, 3–4, 103
- filtering
 - environment variables, 75
 - processes
 - by name, 63
 - by resource use, 64
 - text, 21, 24–25
- find command, 10–11, 58
- float() function, 187
- for loop, 195–196
- fsck command, 110–111
- f switch
 - shred command, 119
 - tar command, 97
- functions in Python, 187–188

G

- Gemini, 203
- getopts command, 92
- g flag, 22–23
- git clone command, 47
- GitHub, 47
- Google
 - email, 138
 - Gemini, 203
 - packet routing, 139
 - public DNS server, 35
- Grand Unified Bootloader (GRUB),
 - xxxv–xxxvi, *xxxvi*
- granular control, xxvi
- graphical user interfaces. *See* GUIs

- gray hat hackers, 87
- grep command
 - filtering
 - for keywords, 11–12, 21, 29–30
 - by process name, 63
 - for variables, 75
 - open port scanner, 89, 91
 - piping to, 12, 21, 29, 63, 75,
 - 89, 91, 177
- Grok, 203
- groups
 - checking permissions, 51–52
 - defined, 50
 - granting root user’s group
 - permissions, 58
 - passing ownership to, 51
- GRUB (Grand Unified Bootloader),
 - xxxv–xxxvi, *xxxvi*
- GUIs (graphical user interfaces)
 - scheduling jobs to run on startup,
 - 178–179
 - shells vs., 82
 - software installers, 45–46
- gunzip command, 99
- gzip command, 98–99

H

- Hackers Arise, xxiii
- hacking
 - advantages of Linux for,
 - xxvi–xxvii
 - black hat, 87–88
 - ethical, xxv–xxvi
 - gray hat, 87
 - importance of, xxiii–xxiv
 - importance of Linux to, xxiv
 - white hat, xxv–xxvi, 87
- hash mark (#), 84–85, 186
- hcidump tool, 159
- hcidump tool, 159
- hcitool tool, 159–160
- hda drive label, 105
- head command, 18–19, 21
- help command, 7–8
- help() function, 187
- help resources, 7–8
- High Performance File System (HPFS),
 - 106–107

HISTSIZE variable, 75–76
/home directory, 2, 4, 4
hosts file, 35–36
-h switch, 7–8
\h value, 77, 133

I

IDEs (integrated development environments), 183
ifconfig command
 changing network information, 31–33
 network analysis, 28–29
 open port scanner, 89
 remote spying camera, 128
 wireless network analysis, 152–153
if...else structure, 194–195
if structure, 194
init daemon (initd), 176
insert command, 131
insider threats, 204
insmod suite, 167
install keyword, 40–41
integrated development environments (IDEs), 183
intelligence and espionage, xxiii–xxiv, xxvi, 141
int() function, 187
IoT device vulnerabilities, 204
IP addresses
 assigning new, 31–33
 DoS attacks, 31
 mapping, 35–36
 tracking methods, 138
ipconfig command, 89
iwconfig command, 30–31, 153, 155
iwlist command, 153–154

J

JetBrain, 183
job scheduling, 171–179
 backup tasks, 174–175
 MySQLScanner, 175–176
 to run automatically, 172–176
 to run on startup
 GUI, 178–179
 rc scripts, 176–178

jobs command, 92
journalctl utility, 114–119
 deleting logs, 118
 disabling logging, 120
 help screen, 115
 viewing all logs, 114
 kernel logs, 118
 viewing events
 in last 24 hours, 116–117
 by user, 117, 117
 viewing logfiles
 highest-priority, 116
 specific services, 116
journal daemon (journald), 114, 120

K

Kali Linux
 desktop, xxxvii, xxxvii
 installation
 through WSL, xxxvii–xxxviii
 on VMs, xxxi, xxxi–xxxii
 overview, 2
 setup, xxxii–xxxvii
kali-tweaks command, xx, 72–73, 82–83
kernel, 163–170
 checking version of, 165
 defined, 163–164
 loadable kernel modules
 confirming module
 loading, 169
 defined, 164
 inserting, 167–169
 listing installed, 167
 managing, 167–169
 removing, 167, 169
 viewing information about, 168
 tuning, 165–167
kill command, 66
-k option, 118

L

l2ping command, 161–162
LAMP (Linux, Apache, MySQL, and PHP), 125
len() function, 187
less command, 24–25
/lib directory, 4, 4

- Linux
 - advantages of, xxvi–xxvii
 - future, xxvii
 - granular control, xxvi
 - hacking tools, xxvi–xxvii
 - open source, xxvi–xxvii
 - transparency, xxvi
 - basic commands, 4–15
 - checking login, 5
 - finding items, 8–12
 - help resources, 7–8
 - identifying current
 - directory, 5
 - modifying files and directories, 12–15
 - navigating filesystem, 6–7
 - basic concepts, 1–2
 - distributions, xxvii
 - filesystem, 3–4
 - importance of, xxiv
 - terminal, 2–3
 - terminology, 1–2
 - virtual machines, xxviii–xxix
 - listen() function, 192
 - listing
 - block devices, 107–108
 - contents of directories, 6–7
 - installed kernel modules, 167
 - lists in Python, 188
 - LKMs (loadable kernel modules), 164–169
 - confirming module loading, 169
 - defined, 164
 - inserting modules, 167–169
 - listing installed modules, 167
 - managing, 167–169
 - removing modules, 167, 169
 - viewing information about, 168
 - Llama 2, 203
 - locate command, 9, 198
 - LockBit, 204
 - logging system, 113–121.
 - See also* journalctl utility
 - logfiles defined, 113
 - priorities, 115–116
 - shredding logs, 118–119
 - logical labels, 105, 105, 106
 - long listings, 7
 - loopback addresses, 28
 - loops, 195–196
 - for loop, 195–196
 - while loop, 195
 - lossless compression. *See* compression
 - lossy compression, 96
 - Low Energy Attribute Protocol (ATT Protocol), 161
 - lsblk command, 107–108
 - ls command
 - file creation, 14
 - listing directory contents, 6–7
 - permissions, 51, 54–55, 85
 - software installation, 47
 - lsmod command, 167–169
 - lsusb command, 108
 - l switch
 - fdisk utility, 106–107
 - ls command, 7, 14, 51
 - netstat command, 29
- ## M
- MAC (media access control) addresses
 - defined, 28
 - spoofing, 32
 - viewing, 28
 - wireless networks, 153–155
 - major and minor numbers, 105–106
 - man command, 8–9
 - man-in-the middle (MITM) attacks, 164, 166
 - manual pages, viewing, 8–9
 - MariaDB, 130–135
 - accessing remote database, 133
 - connecting to database, 133–134
 - defined, 130
 - examining data, 135
 - exploring tables, 134–135
 - interacting with SQL, 131
 - logging in, 130–131
 - open port scanning script, 88–89
 - popularity of, 130
 - setting passwords, 131–132
 - starting, 130–131
 - masks
 - network, 28, 31–32
 - securing default permissions with, 56–57

- max() function, 187
- media access control addresses.
 - See MAC addresses
- /media directory, 4, 4, 108–109
- Medusa, 204
- Meta, 203
- Metasploit, 22
- methods, 190, 190
- Microsoft
 - Copilot, 203
 - Linux vs., xxvi–xxvii
 - WAMP, 125
 - Windows Subsystem for Linux, xxxvii
- military, xxiii, xxvi
- MITM (man-in-the-middle) attacks,
 - 164, 166
- mkdir command, 14
- /mnt directory, 4, 4, 108–109
- mobile device vulnerabilities, 203
- modinfo command, 168
- modprobe command, 167–169
- modules
 - loadable kernel modules, 164–169
 - in Python, 182–183, 189
- monitor mode, 155–156
- more command, 23, 74–75
- mount command, 109
- mounting devices, 104, 108–109
 - automounting, 108
 - manually, 109
 - mount points, 108
 - unmounting, 109
- munging, 22
- mv command, 15
- MySQL, 130–135
 - accessing remote database, 133
 - connecting to database, 133–134
 - defined, 130
 - development of, 130
 - examining data, 135
 - exploring tables, 134–135
 - interacting with SQL, 131
 - logging in, 130–131
 - open port scanning script, 88–91
 - popularity of, 130
 - setting passwords, 131–132
 - starting, 130–131

N

- nameservers, 33–35
- National Security Agency (NSA), 141
- netstat command, 29–30
- network cards
 - modes, 153, 155–156
 - viewing information about, 153
- network manager, 154
- network masks
 - changing, 31–32
 - defined, 28
 - viewing, 28
- networks, 27–36
 - analyzing, 28–29
 - changing information about, 31–33
 - assigning new IP addresses, 31–33
 - changing broadcast addresses, 31–32
 - changing network masks, 31–32
 - spoofing MAC addresses, 32
 - communications in Python, 190–193
 - TCP clients, 190–192
 - TCP listeners, 192–193
 - DNS, 33–36
 - changing servers, 34–35
 - examining, 33–34
 - mapping IP addresses, 35–36
 - statistics about, 29–30
 - wireless, 151–162
 - Bluetooth, 158–162
 - checking wireless devices, 30–31
 - Wi-Fi networks, 152–157
- New Technology File System (NTFS),
 - 106–107
- nice command, 64–66
- nl command, 20–21
- nmap command, 87–89, 142
- nmcli command, 154–155
- noerror option, 100
- NSA (National Security Agency), 141
- ns option, 33
- n switch
 - nice command, 65
 - shred command, 119
- NTFS (New Technology File System),
 - 106–107
- Null-Byte, xxiii

O

- octal representation of permissions,
 - 53, 53
- Offensive Security, xxvii
- Onion Router system, The. *See*
 - Tor system
- ONR (US Office of Naval Research), 139
- OOP (object-oriented programming),
 - 189–190
- OpenAI, 203
- open() function, 187
- open source
 - Linux, xxvi–xxvii
 - MySQL and MariaDB, 88, 130
- OpenSSH
 - defined, 127
 - remote spying camera, 127–129
 - starting, 127
- Oracle, 130

P

- partitions, 105–107
- passwd command, 3
- passwords
 - changing, 3
 - cracking, 22
 - with exception handling, 197–199
 - Wi-Fi AP passwords, 157
 - Kali Linux, xxxiv, xxxiv
 - munging, 22
 - MySQL and MariaDB, 131–132
- PATH variable, 9–10
 - adding directories to, 78–79
 - identifying directories stored in, 78
 - mistakes to avoid, 79
- penetration testing, xxv
- permissions, 49–59
 - changing, 52–56
 - with decimal notation, 52, 53–54
 - giving root execute permission on
 - new tools, 55–56
 - with UGO syntax, 54–55
 - checking, 51–52
 - levels of, 50
 - passing ownership
 - to groups, 51
 - to individual users, 50
 - setting execute permissions, 85

- setting secure default permissions
 - with masks, 56–57
 - special, 57–59
- Perplexity, 203
- phishing, 203
- PIDs (process IDs), 62–63, 66–68
- piping
 - cat to grep, 21
 - netstat to grep, 29
 - nmap to grep, 89, 91
 - ps to grep, 12, 63, 177
 - set to grep, 75
 - set to more, 74
- pip package manager, 182–183
- Play, 204
- print() function, 185, 187–188, 191
- privilege escalation, 58
 - /proc directory, 4
- process IDs (PIDs), 62–63, 66–68
- process management, 61–69
 - changing priority, 64–66
 - killing processes, 66–67
 - moving processes to
 - foreground, 68
 - processes defined, 61
 - running processes in background,
 - 67–68
 - scheduling processes, 68–69
 - viewing processes, 62–64
 - filtering by name, 63
 - filtering by resource use, 64
- promiscuous mode, 31
- properties, 190, 190
- ProtonMail, 148–149
- proxies
 - adding, 145
 - defined, 141
 - free, 143, 144
 - setting in config files, 142–144
- proxy chains, 141
 - dynamic chaining, 145
 - random chaining, 146
- proxychains command, 142–147
- proxy servers, 141–147
 - adding proxies, 145
 - dynamic chaining, 145
 - random chaining, 146
 - running traffic through, 141–142

- proxy servers (*continued*)
 - security concerns, 147
 - setting proxies in config files, 142–144
 - PS1 variable, 77
 - ps command
 - adding services, 177–178
 - confirming process priority, 65
 - filtering processes by name, 63
 - viewing process information, 12, 62–63
 - p switch
 - fsck command, 111
 - journalctl utility, 116
 - nmap command, 88
 - purge option, 41–42
 - pwd command, 5–6, 92
 - PyCharm, 183
 - PyPI (Python Package Index), 182
 - Python scripting, 181–200
 - comments, 186–187
 - control statements, 194–195
 - if...else structure, 194–195
 - if structure, 194
 - dictionaries, 193–194
 - exception handling and password cracking, 197–199
 - formatting, 184
 - functions, 187–188
 - improving, 196–197
 - lists, 188
 - loops
 - for loop, 195–196
 - while loop, 195
 - modules, 182–183, 189
 - network communications, 190
 - TCP clients, 190–192
 - TCP listeners, 192–193
 - object-oriented programming, 189–190
 - variables, 184–186
- Q**
- q flag, 117
- R**
- random chaining, 146
 - range() function, 187
 - RansomHub, 204
 - ransomware attacks, 203–205
 - Raspberry Pi
 - connecting to peripherals, 128
 - defined, 127
 - downloading OS, 128
 - IP address, 128
 - logging in, 128
 - remote spying camera, 127–129
 - building, 128–129
 - configuring camera, 129
 - setting up, 128
 - spying with, 129
 - rcconf tool, 178–179
 - rc scripts, 176–178
 - read command, 84, 91, 92
 - readonly command, 92
 - recv method, 191
 - redirect symbol (>), 13, 35, 89
 - relational databases, 131
 - remove command, 41
 - renice command, 65–66
 - repositories
 - adding to *sources.list* file, 43–44
 - categories of, 44
 - defined, 40, 43
 - resources, 61
 - filtering processes by usage, 64
 - killing processes, 66–67
 - prioritizing processes, 65–66
 - rm command, 15
 - rmdir command, 15
 - rmdir command, 167
 - root account
 - confirming login as, 4–5
 - defined, 2
 - permissions, 50, 55–58
 - root (/) of filesystem vs., 3
 - /root directory, 3–4, 4, 55–56, 103
 - rootkits, 164, 169
 - r permission, 50, 52
 - rpicam-still application, 129
 - r switch
 - modprobe command, 169
 - rm command, 15
- S**
- SATA (Serial ATA) drives, 105
 - /sbin directory, 4

Schneier, Bruce, 147

script kiddies, 181

scripts

- defined, 2
- open port scanning script, 87–91
- Python scripting, 181–200
- simple message script, 84–87
- using AI for scripting, 206–207

SCSI (Small Computer System Interface) drives, 105

sda drive label, 105

SDP (Service Discovery Protocol), 160–161

sdptool tool, 160–161

searching, 8–12

- find command, 10–11
- finding and replacing text, 21–23
- grep command, 11–12
- locate command, 9
- whereis command, 9
- which command and PATH variable, 9–10

Secure Shell. *See* SSH

sed command, 21–23

select command, 131

SELECT command, 135

semicolon (;), 131, 133

Serial ATA (SATA) drives, 105

Service Discovery Protocol (SDP), 160–161

services, 123–135. *See also* Apache; MariaDB; MySQL; OpenSSH; Raspberry Pi

- defined, 123
- starting, stopping, restarting, 124

service set identifier (SSID), 152, 154, 157

set command, 74, 92

set user ID bit. *See* SUID bit

SGID (set group ID) bit, 58

shebang (#!), 84, 86

shells. *See also* bash shell

- changing default, 72–73, 82–83
- changing prompt, 76–77
- defined, 2–3, 82
- GUIs vs., 82
- variables
 - defined, 71
 - viewing, 74

shift command, 92

shred command, 118–119

shredding logs, 118–119

SIGHUP kill signal, 67, 67

SIGINT kill signal, 67

SIGKILL kill signal, 67, 67

SIGQUIT kill signal, 67

SIGTERM kill signal, 66, 67

Small Computer System Interface (SCSI) drives, 105

social engineering, 203, 205–206

software, 39–48

- adding repositories to *sources.list* file, 43–44
- installing
 - with apt, 40–41
 - with git, 47
 - with GUI-based installers, 45–46
- removing, 41–42

software packages

- defined, 39
- purging, 41–42
- searching for, 40
- updating, 42
- upgrading, 42–43

sorted() function, 187

SourceForge, 190

sources.list file, adding repositories to, 43–44

SQL, interacting with, 131

ss command, 30, 30

SSH (Secure Shell)

- defined, 127
- remote spying camera, 127–129

SSID (service set identifier), 152, 154, 157

sticky bit, 58

stop command, 156

storage device management, 103–109

- /dev* directory, 104–107
 - block devices, 107–108
 - character devices, 107
 - logical labels, 105, 105, 106
 - major and minor numbers, 105–106

- storage device management (*continued*)
 - /dev* directory (*continued*)
 - mount points, 108
 - partitions, 105–107
 - USB devices, 108
- mounting devices, 104, 108–109
 - manually, 109
 - mount points, 108
 - unmounting, 109
- viewing information about
 - mounted disks, 109–110
- strip() function, 199
- sT switch, 88
- sudo command, xix, 9, 31
- SUID (set user ID) bit
 - defined, 57
 - granting temporary root
 - permissions with, 57
 - privilege escalation, 58–59
- superuser account. *See* root account
- supply chain attacks, 204
- Synaptic, 45–46
- sysctl command, 165–167
- /sys* directory, 4
- syslog daemon (syslogd), 114, 120
- systemd suite, xix–xx, 114
- SysV utilities, xix–xx

T

- tail command, 19–20
- tar command, 96–98
- tar files (tape archive files; tarballs)
 - creating, 96–97
 - extracting files from, 97–98
 - viewing files from, 97
- TCP clients, 190–192
- TCP connect scanning, 88
- TCP listeners, 192–193
- telnet, 127
- terminal, 2–3
- test command, 92
- text, 17–25
 - filtering, 21
 - finding and replacing, 21–23
 - numbering lines, 20–21
 - viewing
 - first lines, 18–19
 - last lines, 19–20

- one page and paging down, 23
 - one page and scrolling or filtering, 24–25
- text editors, 84
- times command, 92
- top command, 64, 66–67
- Tor (The Onion Router) system, 139–141
 - Ahmia search engine, 141, 141
 - dark web, 140–141
 - encrypted traffic data, 139–140
 - installing Tor browser, 140, 140
 - security concerns, 141
- Torrent, xxviii
- Torvalds, Linus, xxvii
- touch command, 14
- traceroute command, 138–139
- traffic correlation, 141
- transparency, xxvi
- trap command, 92
- try/except structure, 197–199
- t switch
 - netstat command, 29
 - tar command, 97
- type command, 92
- type() function, 187

U

- UGO syntax, changing permissions
 - with, 54–55
- umask command, 56–57, 92
- umount command, 109
- union command, 131
- unmounting (ejecting)
 - devices, 109
- unset command, 80, 92
- update command, 42, 131
- updatedb command, 9
- upgrade keyword, 42
- USB devices, checking for, 108
- user land, 163
- US Office of Naval Research (ONR), 139
- /usr* directory, 4
- u switch
 - journalctl utility, 116
 - netstat command, 116
- \u value, 77

V

- variables
 - adding functionality to scripts
 - with, 86
 - adding to scripts, 90–91
 - defined, 86
 - environment, 71–80
 - naming, 90
 - Python, 184–186
- VirtualBox
 - installing, xxix, xxxii
 - setting up, xxix–xxx, xxx
- Vision, Max (Max Butler), 88
- VMs (virtual machines), xxviii–xxxii
- VPNs (virtual private networks), 147–148
- v switch, 97–98
- vulnerability assessments, xxv

W

- wait command, 92
- WAMP (Windows, Apache, MySQL, and PHP), 125
- WEP (Wired Equivalent Privacy), 152
- whereis command, 9
- which command, 9–10
- while loop, 195
- white hat hacking, xxv–xxvi
 - defined, 87
 - military and espionage, xxvi
 - penetration testing, xxv
- whoami command, 5
- Wi-Fi networks, 152–157
 - basic commands, 152–155
 - connecting to APs, 154–155

- cracking APs, 155–157
- frequency of, 158
- modes, 158
- power of, 158
- range of, 158
- security protocols, 158
- terminology, 158
- viewing APs, 153–154
- viewing interfaces and statistics, 153
- Wi-Fi Protected Access (WPA), 152
- wildcards, 11
- Windows, Apache, MySQL, and PHP (WAMP), 125
- Windows Subsystem for Linux (WSL), xxxvii–xxxviii
- Wired Equivalent Privacy (WEP), 152
- wireless networks, 151–162
- WPA (Wi-Fi Protected Access), 152
- WPA2-PSK, 152
- WPA3, 152
- w permission, 50, 52
- WSL (Windows Subsystem for Linux), xxxvii–xxxviii
- \w value, 77

X

- X (formerly Twitter), 203
- x permission, 50, 52
- XSS (cross-site scripting), 124
- x switch, tar command, 97

Z

- zombie processes, 66
- Z shell (zsh), xx, 73, 82