

INDEX

Symbols & Numbers

"" (comment) characters, 190
(comment) character, 83
#! (shebang) characters, 82
--help command, 8–9
-? (help) command, 9
-h (help) command, 8–9
.
(execute) command, 84, 90
..
(move up level) command option, 7
/
(forward) command, 25
32-bit/64-bit CPU types, xxv
:
(return true) command, 84, 90
[
(conditional test) command, 91

A

access. *See also* permissions
 network, 31, 32
 remote databases, 132–133
 restricted internet, 148–149
access lists. *See also* wordlists, 125
access points (AP), 31, 154, 155–156, 157
Advanced Packaging Tool (apt),
 40–44
aircracking suite, 9, 157–159
aireplay-ng command, 159
airmon-ng command, 157–158
airodump-ng command, 158–159
anonymity
 IP address tracking, 140–141
 with proxy servers, 143–148
 with Tor network, 141–143
 with VPNs, 148–149
Apache Web Server service, 122–125
apt (Advanced Packaging Tool),
 40–44
apt-cache command, 40
apt-get command, 40–43
archiving, 94–96, 115
ARM architecture, xxvi
arrays, 191
at daemon, 69
automount, 106

B

background processes, 68–69
backup scheduling task, 176–177
bad blocks table, 108
banner-grabbing, 194–195, 199–201
banners, 194
bash (Bourne-again shell)
 common commands, 90–91
 overview, 2, 4, 72, 82
Bcast (broadcast address), 30
bg (background) command, 90
/bin directories, 5, 76
binaries
 defined, 2
 in Linux filesystem, 5
 search commands, 10
BIND (Berkeley Internet Name
 Domain), 34
black hat hackers, 86
block devices, 105–106
Bluetooth, 159–164
 overview, 159–160
 scanning, 160–164
Bluetooth SIG site, 162
BlueZ protocol stack, 160–161
bootloader, xxxiv
break command, 90
broadcast address
 changing, 32
 information, 30
broadcast command option, 32
BSSID (basic service set identifier),
 154, 158–159
bunzip2 command, 97
Butler, Max “Max Vision”, 86–87
bzip2 command, 97

C

case sensitivity, 2
cat (concatenation) command, 13–14,
 22, 167
cd (change directory) command, 7

- channels (CH), Wi-Fi, 154, 158, 158–159
- character devices, 105
- chgrp (change group) command, 51
- chmod (change mode) command, 52–55, 56, 58
- chown (change owner) command, 50
- classes and subclasses, 193–194
- command directories, 76–77
- command line interface (CLI), 2
- comment characters, 83, 190
- compress command, 97
- compression, 93–94, 96–97
- concatenation, 13–14, 22, 67
- configuration files, 5
- connect method, 194–195
- continue command, 90
- control statements, 197–199
- copy commands
 - bit by bit, 98–99
 - file, 15
- cp (copy file) command, 15
- CPU types, xxv
- createuser command, 137
- cron daemon, 174
- cron* table, 174–178
- crond command, 69, 174
- crontab command, 175–176

D

- daemons, 32, 69
- dark web, 142
- databases. *See also* MySQL databases
 - hacking, 87, 130
- db_status command, 137
- dd command, 98–99
- Debian distribution, xxv
- deleted file copy, 98–99
- denial-of-service (DoS) attacks, 31
- describe command, 134
- /dev* directory, 102–106
- device drivers, as hacking target, 171
- df (disk free) command, 107–108
- dhclient command, 33
- dhcp daemon, 32
- DHCPDISCOVER request, 33
- DHCPOFFER request, 33
- DHSCP servers, 32–33, 35
- dict statement, 197
- dictionaries, 197
- dig command, 33–34

- directories. *See also* filesystems
 - changing, 7
 - creating, 15
 - Linux filesystem, 5
 - listing content, 7–8, 51–52
 - naming, 2
 - and PATH variable, 76–77
 - permissions, 51–52
 - present working, 6
 - removing, 16
 - searching, 11–12
- disk space, xxix, 107–108
- dmesg command, 171
- DNS (Domain Name System), 33–35
 - changing servers, 34–35
 - information, 33–34

E

- eavesdropping, 150, 166
- echo command, 35, 83, 90
- email encryption services, 150
- encryption
 - email, 150
 - with VPNs, 149
 - wireless security (ENC), 158
- env (environment) command, 72
- environment variables. *See also* shell variables
 - changing values, 73–74
 - command directories, 76–77
 - concepts, 71–72
 - shell prompt, 75–76
 - user-defined, 77–78
 - viewing, 72–73
- espionage, xxiii, 141, 148, 149
- ESSID (extended service set identifier), 154, 158–159
 - /etc/apt/sources.list* file, 43
 - /etc/crontab* file, 174–176
 - /etc* directory, 5
 - /etc/fstab* file, 107
 - /etc/hosts* file, 36
 - /etc/init.d/rc* file, 179
 - /etc/logrotate.conf* file, 115–117
 - /etc/proxychains.conf* file, 144
 - /etc/resolv.conf* file, 34–35
 - /etc/rsyslog.conf* file, 112–115
 - /etc/shadow* file, 57
 - /etc/sysctl.conf* file, 167, 168
- eth0 interface, 30
- ethical hacking, xxii–xxiii

eval (evaluate expression) command, 90
exception handling, 201
exec command, 90
execute permissions, 55–56, 57–58,
83–84
exit command, 90
exploits, 196–197
export command, 74, 75–76, 90

F

fdisk utility, 104
fg (foreground) command, 68–69, 90
file content. *See* text
file types, 104–105
files. *See also* log files; text
archiving, 94–96
compressing, 96–97
copying, 15, 97–98
creating, 13–15
listing, 7–8, 51–52
moving, 15–16
naming, 2
ownership, 50–51
removing, 16
renaming, 15–16
searching for, 10–12
filesystems
Linux structure, 4–5
monitoring, 107–109
navigating, 6–8
searching, 9–12
storage devices in, 102–106, 107
filtering with keywords, 12–13, 22–23,
63–64, 73
find command, 11–12, 59
flash drives, 104–105, 106
for loop, 199
frequency, Wi-Fi, 154
fsck (filesystem check) command,
108–109
ftplib module, 201–202

G

getopts command, 91
git clone command, 46–47
github, 46
Google internet tracking, 140
Grand Unified Bootloader (GRUB),
xxxiv–xxxv

gray hat hackers, 86–87
grep command, 12–13, 22, 24, 63, 73
GRUB (Grand Unified Bootloader),
xxxiv–xxxv
gzip command, 96–97

H

hacking
malicious, 86–87
as profession, xxi–xxiii
and scripting skills, 183
hard drive partitions, xxxiii
hcidump command, 161
hcitool command, 161–162
head (view file) command, 20–21, 23
help commands, 8–9
hidden file switch, 8
history file size, 73–74
HISTSIZE (history file) variable, 73
home directory, 2, 5
hosts file, 36
html code example, 124–125
HTTP vs. Torrent, xxv–xxvi
HWaddr. *See* MAC address

I

IDEs (integrated development
environments), 187
if statement, 197–198
ifconfig command, 29–30, 31–32,
154–155
if...else statement, 198
import statement, 192
index.html file, 124–125
init daemon, 179
insmod (insert module) suite, 169
IP forwarding, 168–169
IP (Internet Protocol) addresses
analyzing, 29–30
changing, 31
domain name mapping, 36
requesting new, 32–33
scanner script, 87–88
tracking, 140–141
.iso file extension, xxx
iterable lists, 191
iwconfig command, 30–31, 155, 157
iwlist command, 155–156

J

job scheduling, 173–178
jobs command, 91

K

Kali
 desktop, 3–5
 downloads, xxv–xxvi
 installation, xxix–xxxi
 login, xxxv–xxxvi
 overview, 2
 setup, xxxi–xxxv
kernel, 62, 165–166, 167–169
kernel modules. *See also* loadable kernel
 modules, 166, 169–171
KEY statements, 72
kill command, 67–68
kill signals, 67
killall command, 67–68

L

l2ping command, 163–164
LAMP tools, 123
less command, 25–26
/lib directory, 5
libraries, 5
Linux
 advantages of, xxiv
 case sensitivity, 2
 distributions, xxv
 runlevels, 179
LKMs. *See* loadable kernel modules
 (LKMs)
lo (loopback address) information, 30
loadable kernel modules (LKMs). *See*
 also kernel modules, 166,
 169–171, 171–172
localhost, 30
locate command, 10
log files, 115–118
 rotating, 115–117
 shredding, 117–118
logging systems
 concepts, 111
 configuration and rules, 112–115
 disabling, 118–119
login checking, 6
logrotate utility, 115–117
loopback address, 30
loops, 198–199

lossy vs. lossless compression, 94
ls (list) command, 7–8, 51–52
lsblk (list block) command, 105–106
lsmod (list modules) command, 169

M

MAC address
 displaying, 30, 156
 spoofing, 32
man-in-the-middle (MITM) attacks,
 166, 168
man (manual) command, 9, 23
managed mode, 31
manual pages, 9
Mask information, 30
master mode, 155
/media directory, 5, 106–107
message logging. *See* logging systems
Metasploit, 63, 136–137
methods, 193–194, 195
military hacking, xxiii
MITM (man-in-the-middle) attacks,
 166, 168
mkdir (make directory) command, 15
/mnt directory, 5, 106
mobile devices, xxiv–xxv, xxvi
modinfo command, 170
modprobe command, 169, 170–171
monitor mode, 155, 157–158
more command, 25
mount points, 106
mounting/unmounting devices,
 106–107
mv (move/rename) file command, 16
MySQL databases, 130–135
 accessing, 132–133
 connecting to, 133–134
 information, 131–132
 tables, 134–135
MySQL Scanner script
 code example, 87–90
 scheduling, 177–178
mysql service, 130–135

N

nameservers, 33–35
National Security Agency (NSA),
 139, 143
netmask command option, 32
network cards, 155, 157

- network connection scripts, 194–197
- network intrusion detection system (NIDS), 19
- network manager, 156
- network mask
 - changing, 32
 - display, 30
- networks. *See also* Wi-Fi networks
 - analyzing, 29–31
 - changing information, 31–33
- nfnetwork module, 169
- nice (process priority) command, 65–66
- NIDS (network intrusion detection system), 19
- nl (number lines) command, 22, 23
- nmap (network map) command, 86, 87–88
- nmcli (network manager command line interface) command, 156

O

- object-oriented programming (OOP), 192–194
- objects, 193–194, 195
- octal digits, 53
- .onion addresses, 142
- Onion Router system, 141–143
- OOP. *See* object-oriented programming (OOP)
- open source code, xxiv, xxv
- OpenSSH service, 125–126

P

- packet forwarding, 168–169
- pairing Bluetooth, 160
- partitions
 - defined, xxxiii
 - labeling system, 103–104
- passwd command, 4
- passwords
 - changing, 4
 - cracking, 31, 159, 201–203
 - root user, xxxii–xxxiii, 132–133
- PATH variable, 76–77
- penetration testing, xxiii
- permissions, 49–59
 - changing, 52–57
 - checking, 51–52
 - concepts, 49–50

- granting, 50–51, 83–84
- special, 57–59
- PID (process ID), 62, 63
- pip (Pip Installs Packages) manager, 184–185
- piping, 12–13
- ports
 - banner-grabbing script, 199–201
 - connecting to, 194–195
 - scanning, 86–90
- PostgreSQL (Postgres) databases, 135–137
- postgresql service, 136–137
- power (PWR) and Wi-Fi, 154, 158, 158–159
- priority
 - message logging, 114–115
 - processes, 64–66
- privilege escalation, 58
- /proc/version file, 167
- process ID (PID), 62, 63
- processes, 61–69
 - background and foreground, 68–69
 - concepts, 61–62
 - information on, 12–13, 62–64
 - killing, 66–68
 - managing priority of, 64–66
 - scheduling, 69
- .profile file, 57
- promiscuous mode, 31
- properties, 193
- ProtonMail, 150
- proxy servers, 143–148
 - choosing, 148
 - concepts, 143–144
 - setting up, 144–148
- proxchains command, 143–148
- ps (processes) command, 12–13, 62–63
- PS1 (shell prompt) variable, 75–76
- PSK (pre-shared key), 154
- pwd (present working directory) command, 6
- Python language
 - comments, 190
 - functions, 190–191
 - installing, 184–186
 - learning, 183–184, 187, 203
 - lists, 191–192
 - modules, 192
 - variables, 187–190
- Python Package Index (PyPI), 184

R

- Raspberry Pi
 - architecture, xxvi
 - Spy project, 125–129
- Raspbian operating system, 126, 129
- raspistill application, 129
- rc* scripts, 178–180
- rcconf tool, 180–181
- read command, 85, 91
- readonly command, 91
- reconnaissance, 160–164, 197
- renice command, 65, 66
- repositories, 40, 43–44, 185
- resource usage, 64
- rm (remove) command, 16
- rmdir (remove directory) command, 16
- rmmmod (remove module) command, 169
- /root* directory, 5
- root user
 - defined, 2
 - passwords, xxxii–xxxiii, 130–131, 132
 - privileges, 5, 6, 50, 65, 66
- rootkits, 166, 171
- rsyslog daemon, 112, 119
- runlevels, 179

S

- /sbin* directories, 76
- scheduling
 - with *at*, 69
 - with *crond*, 174–178
 - at startup, 178–181
- script variables, 84–85, 89
- scripts
 - concepts, 2, 81
 - examples, 86–90
 - executing (running), 83–84
 - scheduling, 174–178
 - writing, 82–85
- SDP (Service Discovery Protocol), 163
- sdptool* command, 163
- security. *See also* permissions
 - and loadable kernel modules, 171–172
 - and surveillance, 142–143, 148, 149
 - Wi-Fi protocol, 154
- sed (stream editor) command, 23–24
- SELECT command, 135
- service command, 119, 122
- Service Discovery Protocol (SDP), 163

- services
 - defined, 121
 - scheduling at startup, 179–181
 - starting, stopping, restarting, 122
- set command, 72–73, 91
- SGID bit, 58–59
- .sh* file extension, 85
- shebang (#!), 82
- shell prompt, 75–76
- shell variables, 71–72
- shells, 2, 82
- shift command, 91
- show command, 134
- shred command, 117–118
- Snort, 19–20, 20
- socket module, 194–196
- software managers and installers, 40, 45–46
- software packages
 - defined, 39
 - installing, 40–41
 - removing, 41–42
 - updating and upgrading, 42–43
- sources.list* file, 43–44
- spy camera project, 125–129
- SQL (Structured Query Language)
 - commands, 131
- SSH (Secure Shell), 125–126
- SSID (service set identifier), 154
- sticky bit permission bit, 58
- storage devices, 102–109
 - monitoring and checking, 107–109
 - mounting and unmounting, 106–107
 - representation of, 102–106
- strip() function, 202
- su (switch user) command, 136
- SUID bit, 57–59
- surveillance concerns, 142–143, 148, 149
- Synaptic Package Manager, 45–46
- sysctl command, 167–169
- syslogd daemon, 112
- system administrator. *See* root user

T

- tail (view file) command, 21–22, 23
- tar (archive) command, 94–96
 - .tar* file extension, 95
- tarballs/tar files, 94–96
- TCP client script, 194–195

- TCP connect scan, 86, 88–90
- TCP listening script, 195–197
- terminals, 2, 4, 68
- test command, 91
- text
 - concatenating to file, 13–14
 - displaying, 20–23, 24–26
 - find and replace, 23–24
- text editors, 82, 187
- .tgz file extension, 96
- times command, 91
- top (resource usage) command, 64, 66
- Tor network, 141–143
- torrent downloads, xxv–xxvi
- touch command, 14–15
- traceroute command, 140
- trap command, 91
- try/except statements, 201–202
- type command, 91

U

- UGO (user, group, and others) syntax, 54–55
- umask (unmask) values, 56–57, 91
- umount (unmount) command, 107
- uname command, 167
- uncompress command, 97
- unset command, 72–73, 78, 91
- update-rc.d command, 179
- USB flash drives, 104–105, 106
- use command, 134
- user-defined variables, 77–78
- user land, 165
- user types, 50

V

- variables. *See also* environment variables
 - Python, 187–190
 - script, 84–85, 89
 - shell, 71–72
- virtual machines, concepts and installation, xxvi–xxvii
- virtual private networks (VPNs), 148–149
- VirtualBox
 - installation and setup, xxvi–xxix
 - installing Kali on, xxix–xxxi
- virtualization software, xxxi
- VPNs (virtual private networks), 148–149
- vulnerability assessments, xxiii

W

- wait command, 91
- web server services, 122–125
- WEP (Wired Equivalent Privacy) protocol, 154
- wget command, 185–186
- whereis command, 10
- which command, 10
- while loops, 198
- white hat hacking, xxiii
- whoami command, 6
- Wi-Fi networks, 154–159
 - basic commands, 154–157
 - hacking, 157–159
- wildcards, 12
- Windows vs. Linux, xxiv–xxv, 101
- wireless network devices, 30–31, 153
- wireless range, 154
- wlan0 interface, 30, 31, 155
- wordlists, 27, 159, 202
- WPA (Wi-Fi Protected Access) protocol, 154
- WPA2-PSK protocol, 154

Z

- zombie processes, 66, 67