

INDEX

Symbols

+ (addition sign), 13
& (ampersand), 17, 45, 47, 136, 157
&>> (ampersand and double arrow), 18
&> (ampersand and right arrow), 18
` (backtick), 136
\$() (command substitution syntax), 11
{ } (curly brackets), 3
/ (division sign), 13
\$* (dollar asterisk), 22, 24, 25
\$@ (dollar at), 21, 22
(dollar hashmark), 21, 22
\$ (dollar sign), 3
. (dot), 8, 49, 129
.. (dot dot), 129
./ (dot forward slash), 9
./ (dot-slash notation), 8
&& (double ampersand), 17, 136
-- (double dash), 5
<< (double left arrow), 18
\$(()) (double parentheses syntax), 13, 14, 177
|| (double pipe), 17, 18, 136
>> (double right arrow), 18, 136
;; (double semicolon), 17
[[]] (double square brackets), 29
= (equal sign), 11
#! (hash and exclamation marks), 6
(hash mark), 7
< (left arrow), 18
% (modulo), 13
* (multiplication sign), 13
! (NOT operator), 30
() (parentheses), 11, 17, 18
| (pipe), 17, 20, 136, 137, 139
> (right arrow), 18, 136
>& (right arrow and ampersand), 18
; (semicolon), 17, 18, 29, 135, 136

- (single dash), 5
[] (square brackets), 29
~ (tilde), 8
_ (underscore), 11

A

ACME Hyper Branding, 58, 112, 121–122
ACME Impact Alliance, 58
ACME Infinity Servers, 51, 58
addition sign (+), 13
Address Resolution Protocol (ARP), 75
 arp-scan command, 75, 77
 packets, 76
Adminer, 277
Advanced Intrusion Detection Environment (AIDE), 283
Advanced Package Tool (APT), 54, 182
alias command, 48
aliases, 47, 48, 66–67
alien command, 254
 converting package formats, 254
Alpine Linux, 182
Alpine Package Keeper, 182
Amazon Simple Storage Service (S3), 157
ampersand (&), 17, 45, 47, 136, 157
ampersand and double arrow (&>>), 18
ampersand and right arrow (&>), 18
Apache, 86, 89, 99, 187
AppArmor, 283
apt command, 53, 182
arbitrary file upload vulnerability, 118
ar command, 253
arguments, 5–7, 39
 accepting, 34–35
 positional, 20–22

- arithmetic, 11
 - calculation, 14
 - expr command, 14
 - let command, 14
 - operators, 13
- arrays
 - elements, 11, 15
 - printing, 14–15
 - reassigning values, 15
 - setting, 14
 - single-dimension, 14
- asterisk/multiplication sign (*), 13
- At, 193–194
 - deny and allow files, 194
 - queue, 306
 - syntax, 193
- awk command, 43–44, 75, 81, 169

B

- background jobs
 - running after terminal exit, 47
 - sending commands to the
 - background 17, 157–158
- backtick (`), 136
- banner grabbing
 - active, 85–86
 - passive, 85
- base64 command, 139
- Bashark, 231
- bash
 - environment, 3
 - interpreter, 6–7, 9
 - scripts, 1, 6–9
 - shell, 2–3
 - syntax, 10
 - variables, 10–11
 - assigning, 11
 - scoping, 12–13
 - unassigning, 12
- bash command, 9
- BASHPID environment variable, 4
- BASH_VERSION environment variable, 4
- bg command, 46
- binaries, 47, 150
- binary staging, 155
- blackice-icecap, 89
- Bless, 124
- block devices, 184

- brace expansion, 71
- brute-force attack, dictionary-based, 160
- bug hunting, 70
- Burp Suite
 - Proxy page, 125
 - Repeater, 127, 130
 - Target tab, 126

C

- cat command, 19
- cd command, 8
- Censys, 85
- CentOS, 183
- chaining test conditions, 32
- character strings, 11
- chkconfig command, 293
- chmod command, 8
- chsh command, 2
- ClamAV, 282
- Classless Inter-Domain Routing (CIDR), 58
- clickjacking, 96
- code styling, 6
- Coles, Brendan, 61
- command language interpreter, 1
- command options, 5
- command prompt, 11
- commands, 8
 - obfuscation, 139
- command substitution syntax (\$()), 11
- comma-separated values (CSV),
 - 44, 277
- comments, 6, 7–8
- Compose file, 54
- conditions, 10
 - case statements, 41
 - else conditions, 29
 - if conditions, 29
 - linking, 31
 - AND, 31
 - OR, 31
 - subsequent conditions, 32
- Content-Type header manipulation, 124
- control operators, 16–18
- cp command, 66
- Cron
 - access control files, 192
 - crontab files, 192, 255

- jobs, 192
 - process, 192
 - syntax, 191
 - system-wide, 192
- cross-site scripting (XSS), 96
- C Shell, 166
- curl command, 54, 63, 87, 139
- curly brackets ({}), 3
- custom scripts, importing, 49
- Cygwin, 2
- Czumak, Mike (T_v3rn1x), 231

D

- data loss prevention (DLP) systems, 282
- Debian, 52, 54, 99
- DEB packaging system, 251–254
- debugging, 9
- default environment variables, 4
- default shell, 2, 3
- default wildcard pattern, 42
- delimiters, 20, 43
- denial of service (DoS), 81, 105, 112, 283
- Desktop Management Interface (DMI), 197
- df command, 6, 185, 263
- diff command, 139
- dig command, 301
- directory indexing, 97
- directory persistence, 134
- directory traversal
 - exploiting, 131
 - finding, 129
- dirsearch, 63, 100
- dirsearch command, 63, 101, 275
- Dirty COW vulnerability, 188
- Discord, 78
- division sign (/), 13
- dmesg command, 196
- DNSChef, 301–302
- Docker
 - Advanced Package Tool, 54
 - bridged networking mode, 57
 - community edition (docker-ce), 54
 - Compose, 54
 - Compose file, 54
 - containers, 54
 - deploying, 56

- images, 60
 - verifying, 67
- keyring, 54
- document redirection, 20
- dollar asterisk (\$*), 22, 24, 25
- dollar at (\$@), 21, 22
- dollar hashmark (\$#), 21, 22
- dollar sign (\$), 3
- Domain Name System (DNS)
 - network configuration, 181
 - proxy, 301
 - resolvers, 181
 - servers, 182
- Donas, Jonathan, 63
- dot (.), 8, 49, 129
- dot dot (..), 129
- dot forward slash (./), 9
- dot-slash notation (./), 8
- double ampersand (&&), 17, 136
- double dash (--), 5
- double extensions, 123
- double left arrow (<<), 18
- double parentheses syntax (\$(()), 13, 14, 177
- double pipe (|), 17, 18, 136
- double right arrow (>>), 18, 136
- double semicolon (;), 17
- double square brackets ([[]]), 29
- dpaste, 303
- dpkg command, 182
- dry-run method, 9
- du command, 38
- Dynamic Host Configuration Protocol, 182

E

- echo command, 3, 11, 14, 71
- editing streams with sed, 44
- egress controls, 144
- ELinks, 209–210
- encapsulation, 151
- encoding hexadecimal strings with Base64, 298
- encryption, 151–152, 298–299
- endpoint detection and response (EDR), 282
- env command, 3, 165

- environmental setup, 2, 166
- environment variables, 3–4, 166
- EOF, 20
- equal sign (=), 11
- errors, 5, 9
- exec bash command, 2
- executable permissions, 9, 13
- executing scripts
 - with bash command syntax, 9
 - with dot forward slash (./)
 - syntax, 8
- ExifTool, 124
- exit codes, 23–25
- exit command, 24
- expand a variable, 11
- exploit code, 6, 20
- Exploit-DB searching, 225
- export command, 49
- expr command, 14
- Extended Berkeley Packet Filter (eBPF), 283
- extended detection and response (XDR), 282
- Extensible Markup Language (XML), 83

F

- Fedora, 182
- ffuf command, 113
- fg command, 46
- file
 - descriptor numbers, 16, 19
 - headers, 123
 - modification, 4
 - signatures, 123
- file access control lists (ACLs), 204
- file command, 287
- file integrity monitoring (FIM), 131, 282
- Filesystem Hierarchy Standard (FHS), 164
- File Transfer Protocol (FTP), 80, 86
- find command, 187, 207, 211, 263
- Firefox, 119
- firewall rules, 144, 180
- Flask, 90, 104, 129
- foreground jobs, 45
- foreign address, 179

- ftp command, 108
- functions
 - accepting arguments, 35
 - defining, 33
 - returning values, 34
- Fuzz Faster U Fool (ffuf), 113
- fuzzing
 - for arbitrary file uploads, 119
 - with ffuf, 113
 - with Wfuzz, 113–114

G

- getfacl command, 204
- git command, 54, 55, 103
- GitHub
 - Gists, 72
 - OAuth token, 211
- Gitjacker, 64, 102
- GitLab, 157
- Git repository, 101–103, 106
- globbing, 140–141
- GNOME, 230
- GNU Compiler Collection (GCC), 221
- GNU nano, 2
- GNU Privacy Guard (GnuPG)
 - brute-forcing key passphrases, 215
 - exporting keys, 214
 - generating keys, 213
 - keyring, 213
 - private keys, 213
 - RFC, 213
- Google
 - Cloud Storage, 157
 - DNS, 181
 - Drive, 157
 - search engine, 99
 - Shell Style Guide, 6
- Go programming language, 62
- gpg command, 54, 214
- graphical text editors, 2
- grep command, 20, 42–43, 75, 80, 103
- grip points, 234
- groupadd command, 204
- group ID (GID), 167, 206
- group owners, 12
- GROUPS environment variable, 4
- GTFOBins project, 228

H

- Hammond, John, 64
- HAProxy, 215
- hash and exclamation marks (#!), 6
- hash mark (#), 7
- head command, 112
- here document redirection, 20
- hexadecimal, 75
- Hex Fiend, 124
- hidden files, 5, 112
- history
 - audit log, 134
 - clearing, 295
 - disabling, 295
 - environment variables, 294
 - files, 175
 - manipulating, 294
- home directory, 3
- honeypot servers, 86, 284
- Horton, Andrew, 61
- hostname command, 173
- hostnamectl command, 173
- HOSTNAME environment variable, 4, 173
- hotkeys, 134
- HxD, 124
- HyperText Transfer Protocol (HTTP)
 - method, 42
 - GET, 98, 100, 119
 - HEAD, 87, 89, 105
 - POST, 78, 118
 - path, 42
 - redirects, 98
 - requests, 100, 105, 133
 - responses, 100
 - secure, 158
 - server, 156
 - status code, 42, 134
 - uniform resource locator, 78
 - encoding, 132
 - User Agent field, 42
- hypervisors, 52

I

- ifconfig command, 178
- ImageMagick, 124
- index numbers, 14
- ingress controls, 144

- input prompting, 22–23
- Internet Control Message Protocol, 75
- internet protocol (IP) address, 15, 39
- intrusion detection and prevention
 - systems (IDS/IPS), 284
- ip command, 59, 178
- iptables command, 180

J

- JavaScript Object Notation (JSON), 64, 92, 110
- job control, 17, 45–47
 - background jobs, 45
 - foreground jobs, 45
- jobs command, 46
- JPEG image file header, 123–124
- jq command, 64, 92, 93

K

- Kali, 2, 52–54
- kernels, 188–189

L

- lab
 - architecture, 57–60
 - backup, 52
 - deployment, 56
 - machine details, 59
 - rebuilding, 60–61
 - setup, 51
 - shutting down, 60
 - testing and verification, 57
- lastb command, 296
- last command, 296
- left arrow (<), 18
- let command, 14
- libjpeg, 124
- libpng, 124
- libprocesshider, 288
- line breaks, 19
- LinEnum, 65, 198, 229
- linking conditions, 31–32
- Linux, 2, 5
 - distributions, 2, 7, 181, 254
- Linux Exploit Suggester, 2, 63–64
- Linuxprivchecker, 231
- Living Off Trusted Sites (LOTS) Project, 78

- logfile
 - filesystem locations, 164
 - filtering logs, 43
 - searching for, 186
 - writing logs to file, 19
- logout, running jobs after, 46–47
- long-form argument syntax, 5, 6
- long-running command, 10, 18
- loops and loop controls, 35
 - break keyword, 40
 - continue statement, 40
 - for loop, 38
 - until loop, 37
 - while loop, 35
- lsblk command, 184
- lsb_release command, 173
- ls command, 4, 5
- lshw command, 194
- Lua, 89

M

- macOS, 2
- magic bytes, 123–124
- make command, 54, 57
- Makefile, 56
- man command, 4, 50
- MariaDB, 267
- Media Access Control (MAC) address, 75–76
- medusa command, 267
- metadata, 8, 12
- Metasploit auxiliary module, 273
- Microsoft
 - Hyper-V, 196
 - OneDrive, 157
 - SQL, 260
 - Teams, 78
- Mimikatz, 230
- MimiPenguin, 230
- minification, 150
- MITRE Common Vulnerabilities and Exposures (CVE) database, 183
- mkdir command, 5
- modulo (%), 13
- Moore, H.D., 273
- mount command, 185, 263, 292
- Mozilla, 44

- msfconsole command, 273
- multi-homed host, 175
- multiline comment, 8
- multiplication sign (*), 13
- Multipurpose Internet Mail Extensions (MIME), 121
- MySQL, 189, 261
- mysql command, 267

N

- National Security Agency (NSA), 283
- National Vulnerability Database (NVD), 184
- ncat command, 151
- nc command, 86–87, 146, 259
- NetCat, 78, 81, 146
- netstat command, 272
- networking utilities, 32
- nginx, 86, 187
- Nikto, 95–97
- nikto command, 96
- Nmap, 48, 75, 78
- nmap command, 48, 75
- Nmap Scripting Engine (NSE), 89, 114–115, 159
- nohup command, 47
- nonexistent command, 19
- NOT operator (!), 30
- Nuclei
 - clustering, 108
 - fingerprinting, 108
 - hardcoded credentials, searching for, 211
 - parsing, 111
 - protocols, 105
 - scan, running a, 105–110
 - tags, 108
 - templates, 105, 106, 107
- nuclei command, 63, 107
- null byte poisoning, 124

O

- OffSec, 52
- OpenSSH, 115
 - private keys, 212
- OpenSSL
 - decrypting, 298, 299
 - encrypting, 298

- Open Systems Interconnection (OSI)
 - model, 75–76, 283
- operating system, 1, 3, 4
- operators
 - file test, 28
 - integer comparison, 29
 - string comparison, 28
- optional arguments, 7
- Oracle VirtualBox, 52, 195
- OS command injection, 135, 137, 147
- OSSEC, 283, 284, 285
- OSTYPE environment variable, 4
- output format, 20

P

- parameters, 9, 20
- parentheses, 11, 17, 18
- passwd command, 251
- Pastebin, 302
- PATH environment variable, 165
 - hijacking, 211
- payload, 144
- pentestmonkey, 65
- Peripheral Component Interconnect, 176
- Perl, 63–64
- perl command, 64
- permissions, 12
 - ACL, 205
 - setting, 203
 - viewing, 202
- personally identifiable information (PII), 95
- phishing emails, 15
- PHP files, 99, 118
- ping command, 21, 73
- pipe (|), 17, 20, 136, 137, 139
- pluggable authentication modules, 238
- polyglot files, 123–124
- Portable Operating System Interface, 29
- port forwarding, 266
- port hopping, 152
- PortSwigger, 125
- positional arguments, 20, 22
- Postfix, 78
- Pretty Good Privacy (PGP) format, 213
- printenv command, 165
- printf command, 54, 71

- Privacy-Enhanced Mail (PEM)
 - format, 212
- private network, 41
- privileged actions, 34
- privilege escalation
 - actions permitted by, 202
 - automating, 229–231
 - definition, 201
 - exploiting SetUID files, 208–210
 - finding privileged files, 207–208
 - GTF0Bins project, 228
 - hijacking the PATH, 220–222
 - kernel exploits, 224–226
 - searching for credentials, 210–215
- processes, 170–173
 - init process, 170
 - process files, viewing, 170–172
 - process identifier, 170
 - root, examining, 173
- process IDs, 148
- process masquerading, 289
- programming languages, 11
- Project Discovery, 62
- proxy intercept, 125
- ps command, 6, 18, 25, 148, 172
- pseudo-terminal, 154
- PWD environment variable, 4
- pwncat, 64, 145, 149
 - uploading files, 157
- pwncat-cs command, 65, 149
- Python, 6, 64, 87, 104, 120, 156
 - pty module, 154

R

- race condition vulnerability, 225
- RANDOM environment variable, 4
 - random number, 41
- read command, 23
- real-time response, 134
- reconnaissance, 69
 - banner grabbing, 85
 - using Nmap scripts, 89
 - host discovery, 75–76
 - operating system detection, 90–91
 - port scanning, 78–83
 - reusable target lists, creating, 70–71
 - website analysis with WhatWeb, 92–93

- Red Hat, 182
- redirection operators, 18–20
- Redis, 271
 - application configuration, 190
 - application logs, 187
 - compromising a server, 271–272
 - INFO command, 260
 - raw CLI commands, 272
 - used port, 260
- redis-cli command, 272
- regular expression, 41
- remote address (*rem_address*), 179
- restricted bash shell, 7
- returning values, 34
- reverse shell, 144–146
 - destination ports, alternating between, 152–154
 - encrypting and encapsulating traffic, 151
 - listener, 149
 - Netcat listener setup, 146
 - pwncat, uploading files with, 157
 - pwncat-cs listener setup, 149
 - spawning a TTY shell with socat, 155
- right arrow (>), 18, 136
- right arrow and ampersand (>&), 18
- Rivest-Shamir-Adleman (RSA), 152
- rm command, 17
- rmdir command, 64
- root directory, 12, 164
- ROT13, 299
- Ruby, 6, 61
- runtime application self-protection (RASP), 284
- Rust programming language, 62
- RustScan, 62, 80, 84

S

- scheduled tasks, 191
- scope, 70
- scp command, 287
- script, 6
- script command, 49
- SearchSploit, 225
- Secure Shell (SSH), 80
 - brute-forcing, 160
 - key-based authentication, 159
 - managing connections, 161
 - password-based authentication, 159
 - server, 159
 - service management, 236
- Secure Sockets Layer (SSL), 151
- Security-Enhanced Linux (SELinux), 283
- sed command, 44, 45, 71, 296
- semicolon (;), 17, 18, 29, 135, 136
- sendmail command, 77
- sensitive environment variables, 7
- seq command, 70
- Server Message Block, 117
- Shearing, Owen, 65
- shebang line, 6–7
- ShellCheck, 224
- SHELL environment, 3, 4
- shell listener, 144
- Shodan, 85
- short-form syntax, 5–6
- SIGHUP signal, 74
- signal spec (sigspec), 243, 291
- single dash (-), 5
- single-dimension arrays, 14
- Skerritt, Autumn, 62
- Slack, 78, 303
- sleep command, 17, 36, 37, 46
- SlimToolkit project, 150–151
- socat command, 153, 155
- Socket Cat (socat), 145
- Soria, Mauro, 100
- sort command, 103
- source command, 48–49, 223, 243
- split command
 - chunks, 305
 - lines, 304
 - size, 304
- Sprunge, 302
- SQLite, 97, 275
- square brackets ([]), 29
- SSH. *See* Secure Shell
- ssh command, 266, 273
- ssh-keygen command, 239
- stat command, 209
- status codes, 42
- Stewart, Caleb, 64
- sticky bit, 206

- stream editor (*sed*) command, 44–45, 71, 296
- streams
 - standard error, 16, 19, 147
 - standard input, 16, 19
 - standard output, 16, 19, 147
- string comparison, 28, 30
- strings, 10
- strings command, 252
- style guide, 6
- Sublime Text, 2
- subsequent conditions, checking, 32
- substitution cipher, 299
- su command, 53
- sudo command, 53, 54, 56, 217, 218, 219
- synchronization (SYN) scan, 79
- syntax, 5–6
 - highlighting, 2–3
- system administrators, 134, 165, 169, 192, 210, 234, 245, 254, 263
- system-call functionalities, 2
- systemctl command, 55, 293
- systemd, 47, 237
- systemd-detect-virt, 196
- System V, 234, 235

T

- tail command, 56
- tar command, 223, 253
- TCP (Transmission Control Protocol)
 - fingerprinting, 90
 - listener, 153
 - raw, 300
 - sockets, 63, 146
 - socket table, 179
- tee command, 54
- Telnet, 86, 174
- terminal, 2, 4, 9, 11, 12
 - emulator, 53
 - session activity, 49
- test conditions, 29, 32
- testing command success, 32
- test operators, 27
 - file test, 28
 - integer comparison, 28
 - string comparison, 28

- text editors, 2, 3, 8
- text processing and parsing
 - awk filtering, 43
 - grep filtering, 42
- tilde (~), 8
- timeout command, 74
- timestamp, 12
- top command, 289
- touch command, 10, 17, 30
- trap command, 242
- tr command, 81, 103
- tree command, 255
- TTY, 154

U

- UDP (User Datagram Protocol), 79
- UI redressing (clickjacking), 96
- uname command, 148, 173
- unassigning variables, 12
- Uncomplicated Firewall (UFW), 283
- underscore (_), 11
- uniq command, 178
- Unix, 29, 66
- unix-privesc-check command, 66, 230
 - detailed scanning, 229–230
 - standard scanning, 229–230
- unset command, 12, 15
- untyped variables, 11
- useradd command, 204
- User Agent field, 42
- User Datagram Protocol (UDP), 79
- user ID (UID), 4, 166, 205
- usermod command, 53, 55
- utmpdump command, 175

V

- values, assigned, 3, 10–13
- variables, 2, 10, 11
 - assigned, 12
 - global, 12
 - local, 12, 13
 - scoped, 12
 - special, 24
- verbose mode, 9
- version
 - of bash, 3
 - in comment metadata, 8
- vi (terminal text editor), 2

- Vim, 245
- virtualization, 52
- virt-what command, 196
- VMware Workstation, 52
- vsFTPD, 86
- vulnerabilities
 - browsing FTP server content, 109
 - brute-forcing with dirsearch, 100
 - connecting to an anonymous FTP server, 108–109
 - identifying open Git repositories with dirsearch, 101
 - scanning with Nikto, 96–97
 - scanning with Nuclei, 105–110
 - full scan, 108
 - scan by tag, 108
 - template system, 105–106
 - writing a custom template, 106–107
 - SSH server assessment with Nmap NSE, 114–115

W

- watch command, 264–265
- wc command, 183
- web application firewall
 - API security, 284
 - definition, 283
 - detection abilities, 129
 - drawbacks 284
- webhooks, 78, 303
- web shell
 - building an interface, 133
 - limitations of, 134
- Werkzeug, 87, 90

- Wfuzz, 113–114
- wfuzz command, 114
- wget command, 65, 98
- WhatWeb
 - extracting JSON keys, 93
 - with JSON output, 92
 - scanning, 92
- whatweb command, 92
- which command, 66
- whitespace, 12
- Windows Subsystem for Linux (WSL), 2
- wordlist of filenames, creating, 112–113
- WordPress
 - admin panel, 270
 - configuration files, 189
 - database, 268
 - login page, 108, 109
 - user enumeration, 110

X

- XDR (extended detection and response), 282
- XML (Extensible Markup Language), 83
- xxd command, 296

Y

- YAML, 54, 63, 105
- Yellowdog Updater Modified, 182

Z

- ZoomEye, 85
- Z Shell (zsh), 2, 53, 166, 175