

INDEX

=~ operator, 52
! (exclamation point), 66
** (exponentiation), 20
% (modulo) operator, 71
; (semicolon), in Linux, 43
2D (two-dimensional) mesh, 156
“403 Forbidden” error, 23

A

absolute path, 120
Aitel, Dave, 174
alternating sorts, 159
annotate method, 64
annuity factor, 20
applications, killing stuck process,
 50–53
arrays, 78
 creating, 145
 initialization of, 26
 for links, 118
attributes of user accounts,
 modifying, 49
automated SMS message, 114–115
availability, and security, 122

B

backticks, 51
BadChars (bad characters)
 for exploit, 168
 finding, 173, 174
 preventing in data, 175
banner, analyzing, 177
Bayesian spam filter, 99
begin/rescue statement, 113
benchmark library, 144, 149, 151
 measure method, 146
Big O notation, 143–144, 152
black and white, converting photo-
 graph to, 66–67

Blowfish, 5, 128
book, website for, xxiv
brute force attack on password, estimat-
 ing time for, 107
bubble sort, 144–146
 vs. selection sort, 148
buffer overflow, stack-based, 165
Burg, Edmund von der, 74

C

call method, 156
case statement, 80, 82, 122, 139, 140
cgi library, for form generation, 28
changed files, checking for, 1–5
change_geometry method, 63
chaos, calculating measure in
 password, 108
character strings. *See* string utilities
check method, 176
checkbox, on web form, 29
child process, 166
 finding for exploit, 170
chomp method, 17, 84
Classless Inter-Domain Routing, 38
CLI (Command-Line Interface), for
 Metasploit Framework, 163
client, encrypted, 122–124
command line
 accessing, 165
 arguments, 59
 names of files accessed via, 42
Command-Line Interface (CLI), for
 Metasploit Framework, 163
comma-separated value (CSV) files
 converting to XML, 101–104
 downloading from website, 100
 parsing, 35, 99–101
 script integration for automated user
 creation, 47

- comments in code, xxii
- composite method, 66
- compression of files, 15–17
- confidentiality, and security, 122
- connect_login method, 169
- console, for Metasploit Framework, 163
- consolidating scripts, 127
 - for encryption and decryption, 128–131
 - photo utilities, 135–141
 - web scraper, 131–135
- converting photograph to black and white, 66–67
- CPU time, extracting, 51
- crypt library, installing, 6
- CSV files. *See* comma-separated value (CSV) files
- csv library, 35

D

- data encryption, 5–7, 124
- data mining, 111
- data structures, 78
- debugger, 165
- decompressing files, 17–18
- decrypting files, 7–9
- define script, to retrieve word definition, 111–114
- delete_if method, 156
- dictionary attack, 109
- Dictionary.com website, 111
- Dir library, 105
- directories
 - scanning, 61
 - scripts to check for changed files, 1–5
 - searching documents in, 105
- Dir::glob method, 57
- Dir.open() command, 54
- disconnect method, 169
- division, remainder of, 71
- divmod command, 11
- .dll, choosing for exploit, 172
- documentation, xxii
 - comment section for, 134
- documents
 - searching, 105
 - word frequency in, 96–99
- .downcase, 50
- downloading CSV files from website, 100
- Draw object, 64

E

- each method, 52, 118
- each_index method, 87, 148
- each_line method, 105
- editing multiple photographs, 55–57
- efficiency, 160
- email address, on website, and spam, 27
- encrypted client, 122–124
- encrypted server, 124–126
- encrypting
 - data, 124
 - files, 5–7
- encryption key, 7
 - prompt for, 8
- English library, 105
- entropy calculation, 107
- Enumerable library, 98
- error handling, to check for file extension, 16
- Exchangeable Image File Format (EXIF), 59
- exclamation point (!), 66
- exifr library, 59
- EXITFUNC, 168
- exploit, 162
 - building, 164–165
 - choosing .dll for, 172
 - finding child process for, 170
 - Metasploit module shell for, 168–169
 - payload space for, 170–179
 - target vulnerability to, 177
 - testing, 179
 - watching in real time, 165–168
- exploit-repository website, 162
- Exploit::Remote::Ftp, 168
- Exploits/Auxiliary pane in Metasploit GUI, 163
- exponentiation (**), 20
- Extensible Markup Language (XML), CSV to, 101–104
- extname method, 57
- extract method, 122
- extracting information from photograph, 57–60

F

- FasterCSV library, 99, 101, 103
- field-programmable gate arrays (FPGAs), 108

- file extension, error handling to
 - check for, 16
- FileCOPA FTP server, vulnerability in
 - LIST function, 164
- FileCOPA module, 179
- filecopa_exploit.rb* file, 169
- filecprt process, 166
- filecpt process, 166
- File.extname method, 57
- file_list.txt* file, 4
- File.makedirs method, 70
- filenames
 - changing, 56
 - extension, 43
 - fixing, 41–44
- file_report.txt* file, 4
- files
 - checking for changes, 1–5
 - compression, 15–17
 - creating in Ruby, 7
 - decompressing, 17–18
 - decrypting, 7–9
 - encrypting, 5–7
 - finding unlinked, 24–27
 - integrity validation, 1–5
 - joining, 11–13
 - preventing script from overwriting, 7
 - retrieving in directory, 4
 - security for, 128–131
 - splitting large into multiple, 9–11
- financial reporting website, downloading CSV file from, 100
- financing, mortgage calculator, 19–20
- find method, 4
- flash cards, 76–79
- font, for PDF:Writer library, 96
- FPGAs (field-programmable gate arrays), 108
- ftools, 69
- FTP server
 - exploit for closed-source, 161
 - process, 166
- FTP session, beginning, 165
- fuzzer, 174

G

- games
 - Hangman, 85–87
 - Number-Guessing, 79–80
 - Pig, 87–91
 - Rock, Paper, Scissors, 81–83
- Sudoku, 73–76
- Word Scramble, 83–84
- generating forms, 27–30
- GetoptLong library, 127, 130, 131, 140
- gets statement, 50
- graphical user interfaces (GUIs)
 - and file names, 42
 - for Metasploit Framework, 163
- graphics. *See* picture utilities
- Grep, Ruby, 104–106
- groups, in Unix-style systems, 46
- GUIs. *See* graphical user interfaces (GUIs)

H

- handler method, 169
- Hangman, 85–87
- hash data structure, 78
 - to change filename, 43
- hashing process, 4
- header, in CSV file, 101
- heap sort, 152–154
- heapSort method, 154
- here-doc, 70
- home directory, 46
- Hpricot, 118
- HTML method, 30
- HTML output
 - documentation generation for source code, 127–128
 - for photo gallery, 69
- HTML/XML parser, for Ruby, 23
- HTTP requests, error messages as response, 113
- hyperlinks. *See* links

I

- if statement, 75, 105
- ImageMagick library, 61
- images. *See* picture utilities
- tag (HTML), 119
- Immunity Debugger, 165
- include statement, 59
- information extraction, from picture, 57–60
- initialization
 - of arrays, 26
 - of *winnmgmts*, 14
- initialization method, for Metasploit module shell, 168–169

- input by user, verification of, 63
- insertion sorting algorithm, 148
 - vs. shell sort, 149
- installing
 - crypt library, 6
 - PDF:Writer library, 96
- integrity, and security, 122
- Internet. *See also* website scripts
 - automated SMS message, 114–115
 - define script to retrieve word definition, 111–114
 - encrypted client, 122–124
 - encrypted server, 124–126
 - scraping from website
 - data, 120–122
 - images, 118–120
 - links, 115–118
- IP address generation, 35–38
- IP class, 38
- ipaddr library, 39
- ips.txt* file, 37

J

- Jobs pane in Metasploit GUI, 163
- join method, 84
- joining files, 11–13

K

- killing stuck process, 50–53

L

- learning tools, 27–30
 - flash cards, 76–79
- libraries, for website automation, 115
- links
 - arrays for, 118
 - scraping, 115–118
 - validator of, 22–24
- Linux system administration
 - adding user accounts, 44–47
 - fixing bad filenames, 41–44
 - killing stuck process, 50–53
 - validating symlinks, 53–54
- LIST command, 166, 175
 - vulnerability in FileCOPA FTP server, 164
- little-endian byte order, 175
- logarithmic method, 159

M

- makedirs method, 70
- make_nops method, 175
- map function, 59
- mask method, 39–40
- match method, 52
- Matsumoto, Yukihiro, xxi
- measure method, 146
- mechanize library, 118
- merge method, 152
- merge sort, 150–152
- merge_sort method, 152
- Metasploit 3 Web, 163
- Metasploit Framework (MSF), 161–179
 - building exploit, 164–165
 - installing, 162–164
 - introduction, 162
 - module shell explained, 168–170
 - watching in real time, 165–168
 - ways of operating, 163
 - writing module, 164
- methods, recursive call, 75
- min method, 148
- Module Information/Output pane in Metasploit GUI, 163
- modulo (%) operator, 71
- mortgage calculator, 19–20
- mpg123 (Linux), 123
- mplayer2.exe*, 123
- MSF. *See* Metasploit Framework (MSF)
- MSF Operation Code (opcode) database, for address, 172
- Msf::Exploit::Remote, 168
- multiple processors, for shear sort, 158

N

- netcat, 165
- next unless statement, 54
- NOP sled, 174
- Number-Guessing game, 79–80

O

- OllyDbg, 165
 - list of running processes, 166
 - showing access violation, 171
- open() command, 54
- open method, 119
 - for web page, 113
- Open Source Vulnerability Database, 161

- open_uri library, 23, 35, 113
- operations, in consolidated script, 130
- orphan file checker, 24–27
- orphan symlinks, 53
- orphans.txt* file, 26
- out method (cgi), 30
- output, formatting, 20
- output_bubble_sort.txt* file, 145
- output_heap_sort.txt* file, 154
- output_merge_sort.txt* file, 151
- output_quick_sort.txt* file, 155
- output_selection_sort.txt* file, 147
- output_shear_sort.txt* file, 158
- output_shell_sort.txt* file, 149

P

- pack method, 175
- Paros web proxy, 114
- parse() method (CSV), 35
- parsing, 30–33
 - comma-separated value files, 35, 99–101
- password
 - changing for new account, 46
 - checking security of, 106–109
 - for encrypted file, 7
- pattern_create.rb tool, 170
- pattern_offset.rb* file, 171, 175
- payload, 162
- payload space for exploit, 170–179
 - size of, 168
- payload_badchars method, 175
- PDF (Portable Document Format) files,
 - generating, 93–96
- PDF:Writer library, installing, 96
- Perl, xxi, 162
- permissions, groups for, 46
- photos. *See* picture utilities
- picture utilities, 55
 - adding watermark, 63–66
 - consolidating, 135–141
 - converting to black and white, 66–67
 - image information extraction, 57–60
 - mass editing, 55–57
 - photo gallery creation, 68–71
 - resizing pictures, 62–63
 - thumbnail creation, 60–61
- Pig, 87–91
- ping sweep, 35
- pivot element, for quick sort, 154–155

- platform
 - determining which is used, 126
 - independence from, 162
- Portable Document Format (PDF) files,
 - generating, 93–96
- pretty method, 30
- private RSA key, generating, 126
- private_decrypt method (RSA), 126
- process viewer, in Windows Task Manager, 13
- processes, killing stuck, 50–53
- processors, multiple for shear sort, 158
- prompt
 - for converting CSV file to XML, 103
 - for encryption key, 8
- proxy, for web traffic, 113
- ps command (Unix), 13, 51
- public_encrypt method, 124
- Python, xxi

Q

- quality assurance testing, of web applications, 115
- quantized image, 67
- quick sort, 154–156
- quick_sort method, 144, 156

R

- Rails framework, 21
- rand function, 78, 82, 84, 91
- RDoc, 127–128, 131
 - standard format, 135
- rdoc/ri/ri_paths library, 131
- rdoc/usage library, 131
- Really Simple Syndication (RSS), 30
- recursion, 76
 - in merge sort, 152
 - in quick sort, 155
- regression testing of web applications, 115
- regular expressions, 24
 - for converting time, 53
 - to find tags, 120
 - for IP address integrity, 39
- renaming files, 56
- require msf/core statement, 168
- resizing photographs, 62–63
- return method, 175
- reverse_shell connection, 175
- RHOST (remote host), 169

- rio command, 122
- RMagick library, 61, 63, 69
- Rock, Paper, Scissors, 81–83
- .rotate! method, 66
- RSA key
 - generating private, 126
 - public_encrypt method, 124
- RSS (Really Simple Syndication), 30
- Ruby, HTML/XML parser for, 23
- Ruby CSV library, 99
- Ruby Grep, 104–106
- Ruby on Rails, 21
- Rubyful Soup, 118
- rubyful_soup, 23, 24
- RUBY_PLATFORM, 126
- rubyzip library, 15, 17
- ruby-zlib library, 15

S

- save_as method, 96
- scale method, 61
- scraping from website
 - consolidated script, 131–135
 - data, 120–122
 - images, 118–120
 - links, 115–118
- screen resolution, and image size, 71
- scripts, xxi
 - consolidating, 127
 - for encryption and decryption, 128–131
 - photo utilities, 135–141
 - for web scraping, 131–135
- security
 - for files, 128–131
 - of password, checking, 106–109
- selection sort, 146–148
- semicolon (;), in Linux, 43
- server
 - crash from exploit, 164–165
 - encrypted, 124–126
- Sessions pane in Metasploit GUI, 163
- SHA1 hash, creating, 126
- shade method, 66
- Shannon entropy, 107, 108
- shared library trampoline, 175
- shear sort, 156–159
- Shear_sort class, 158
- shell module, creating, 167
- shell preference, for user account, 46
- shell sort, 148–150
- shift method, 101
- Short Message Service (SMS), auto-
 - ated message, 114–115
- sift_down method, 154
- SIGTERM, 52
- Simple Mail Transfer Protocol (SMTP), 27
- SimpleTable object, 96
- size of photographs, changing, 62–63
- SMS (Short Message Service), auto-
 - ated message, 114–115
- SMTP (Simple Mail Transfer Protocol), 27
- solver method, 75
- sort method, 158
- sort_by method, 84, 98
- sorting, 143–160
 - bubble sort, 144–146
 - vs. selection sort, 144–146
 - heap sort, 152–154
 - merge sort, 150–152
 - quick sort, 144, 154–156
 - selection sort, 146–148
 - shear sort, 156–159
 - shell sort, 148–150
- “spaghetti-code” syndrome, 141
- spam, email address on website and, 27
- SPIKE, 174
 - .split command, 51–52
- split method, 75, 84, 107, 126
- splitting files, 9–11
- stack-based buffer overflow, 165
- stock exchange grep, 33–35
- string objects, 131
- string utilities
 - CSV parser, 99–101
 - CSV to XML, 101–104
 - password check, 106–109
 - PDF generator, 93–96
 - Ruby Grep, 104–106
 - word frequency, 96–99
- string variable, 78
- strings
 - generating, 173
 - script to create, 170
- su command, 50
- submit button, 27
- subnet calculator, 38–40
- Sudoku solver, 73–76
- symlinks (symbolic links), validating, 53–54
- system() command, 47

T

- tags in XML document, 103
- Targets section, for Metasploit module shell, 169
- Task Manager (Windows), process viewer, 13
- TCP connection, opening, 123
- <td> tag (HTML), 71
- TERM, 52
- ternary operator, 4
- testing
 - exploit, 179
 - Metasploit Framework (MSF) module, 169
- thumbnail, creating for photograph, 60–61, 71
- time, converting to seconds, 52
- to_hash function, 59
- transferring large files, dividing files for, 10
- two-dimensional (2D) mesh, 156

U

- user32.dll* file, 172
- Unix. *See* Linux system administration
- unless statement, 59
- URI.extract method, 122
- URL error, 24
- user accounts
 - adding, 44–47
 - modifying, 47–50
- user input, verification of, 63
- useradd command, 46
- username, for new account, 46

V

- validating
 - symlinks, 53–54
 - web page links, 22
- variables, initialization of, 4
- verification, of user input, 63
- vulnerabilities, 161
 - of exploit target, 177

W

- watermark, adding to picture, 63–66
- Watir, 115
- web proxy, Paros, 114
- website scripts, 21
 - form generator, 27–30
 - IP address generation, 35–38
 - link validator, 22–24
 - orphan file checker, 24–27
 - parsing, 30–33
 - stock exchange grep, 33–35
 - subnet calculator, 38–40
- wget command, 23
- when clause, 140
- while loop, 87
- whitespace, in filenames, changing, 43
- wicked cool scripts, xxii
- win32ole* library, 14, 115
- win32_process, script iteration of
 - instances, 14
- Windows, process viewer, 13–15
- Windows Management Interface (WMI), 14
 - properties class, 15
- wingmgt*, initialization of, 14
- WMI (Windows Management Interface), 14
 - properties class, 15
- word frequency, 96–99
- Word Scramble, 83–84
- wrapper, 11
- write method, 67

X

- XML (Extensible Markup Language),
 - CSV to, 101–104
 - .xml* file extension, 103

Y

- Yahoo! Finance, 34