

# INDEX

## A

Acunetix, 85, 102  
address space layout randomization,  
    178, 182  
argparse library, 14  
    example, NetCat, 14  
ARP  
    cache, 57  
    poisoning, 53–54, 57  
Arper class, 59–62  
    poison method, 60–61  
    restore method, 61–62  
    run method, 60  
    sniff method, 61  
ASLR. *See* address space layout  
    randomization  
ASLRCheck class (custom Volatility  
    plugin)  
    check\_aslr function, 179  
    create\_pid\_filter, method 180  
    \_generator method, 180–181  
    get\_requirements method, 179–180  
    run method, 182

## B

BeautifulSoup library, 74  
Berkeley Packet Filter (BPF), 54, 56  
    BPF syntax, 56  
BHPFuzzer class, 99–100  
    getNextPayload method, 99  
    hasMorePayloads method, 99  
    mutate\_payload method, 100  
    reset method, 99  
BHNET, 13, 26  
BHP Payload Generator, 102  
*bhservice*, 154, 166  
Bing API, 94, 104, 107

Bing search, 104  
Biondi, Philippe, 53  
BitBlt function, 132  
bit shifting, 41–42  
botnet, 121  
BPF. *See* Berkeley Packet Filter  
Brute-forcing  
    files and directories, 82, 86  
    web form passwords, 88–89  
Bruter class, 88–89  
    get\_params function, 88  
    get\_words function, 88  
    run\_bruteforce, 88  
    web\_bruter, 89  
Burp Dashboard, 113  
BurpExtender class, 97, 105, 107, 110  
    bing\_menu method, 105–106  
    bing\_query method, 107  
    bing\_search method, 106  
    createMenuItems method, 105, 111  
    display\_wordlist, method, 113  
    get\_words method, 112  
    registerExtenderCallbacks  
        method, 105, 110  
    mangle method, 112  
    wordlist\_menu method, 110  
Burp extensions, 95–97, 100, 105, 111  
Burp fuzzing, 95–96  
Burp Intruder, 97, 100, 102  
    payload parameters, 103  
Burp Suite, 93–95  
    API, 94  
    extending, 93–115  
    fuzzing, 95–104  
    GUI, 94–95  
    Jython configuration, 95  
BytesIO module, 75, 87, 128, 140

## C

- C2. *See* command and control
- Cain and Abel, 87, 90
- CANVAS, 134
- chdir context manager function, 77–79
- ClientConnected message, 28–30
- code injection, 164–166
- coding style, 5–7
- command and control, 117, 125
- computer vision library. *See* OpenCV library
- content management systems (CMS), 76
- context manager, 73, 78, 81
  - decorator, 78
- createMenuItem function, 105, 111
- createNewInstance function, 97, 98
- CreateProcess function, 157
- Cridex malware, 182
- cross-site scripting (XSS), 100
- ctypes library, 39, 132–133, 136
  - cast function, 134
  - \_fields\_ structure, 40

## D

- decrypt function, 142, 144
- decryption, 142, 151
- destination unreachable class, 46
- detect function (face detection), 68
- Detector class (sandbox detection)
  - detect method, 136–137
  - get\_key\_press method, 136–137
  - get\_last\_input function, 135–137
- dictionary dispatch, 149
- Document Object Model (DOM), 147
- Domain Name System (DNS), 45

## E

- El Jefe monitoring system, 156–157
- email, 140
  - credentials, stealing, 54–57
- encrypt function, 141–143
- encryption, 140
  - AES, 140–142
  - asymmetric, 140
  - hybrid, 140
  - RSA, 140–142
  - symmetric, 140

- enumerate function, 67
- EOF (end of file marker), 18
- exfiltration, 139, 148

## F

- face detection, 53, 63, 67
- Firefox developer tools, 86, 147
- forensics, 169
- f-strings, 75
- ftp, 140
- ftplib library, 144

## G

- gather\_paths function, 77–79
- GDI (Windows Graphics Device Interface), 131–132
- generator function, 149
- GetAsyncKeyState function, 136–137
- getGeneratorName function, 96–98
- GetLastInputInfo function, 135–136
- getNextPayload function, 98–99
- GetOwner function, 158
- getpass library, 27
- GetTickCount function, 135–136
- GetWindowDC function, 131–132
- GetWindowTextA function, 129
- GetWindowThreadProcessId, 128–129
- GitHub, 117–118, 121, 123
  - personal access token, 118–119
  - workflow, 119
- github3.py library, 118
- GitHub API, 118, 121
- GitImporter class, 124
  - find\_module method, 123–124
  - load\_module method, 124
- gobuster project, 82
- Golden, Tim, 157, 162

## H

- hash dumping, 175
- hexdump function, 19–22
- HEXFILTER string, 20
- HookManager class, 129–130
- .htaccess files, 76
- HTML elements, 147
- HTMLParser, 90, 111
- hypervisor, 1, 171

## I

- IBurpExtender class, 97, 105, 110
- ICMP class, 46–47
  - sniff method, 47
- ICMP echo, 48
- ICMP message packet diagram, 46
- ICMP packet, 37, 42, 47
  - Destination Unreachable message, 46
- IcontextMenuFactory, 105, 110
- IDE. *See* integrated development environment
- Explore.exe* process, 147
- ifconfig, 58
- IintruderPayloadGenerator class, 96–99
- Internet Message Access Protocol (IMAP), 54, 57
- Internet Relay Chat (IRC), 117
- import customizing, 123
- inner function, 83
- integrated development environment, 1, 5
  - installing, 5
- Internet Control Message Protocol (ICMP), 36, 43
- Internet Explorer, 146, 150
- Internet Protocol (IP), 36, 39
- io module, 75
  - BytesIO module, 75, 87, 140
- IOCTL flag, 37
- ipaddress library, 41, 48, 50–51
- IP class, 39–43
  - sniff method, 44
- IP decoding, 38, 43
- IP header, 38
- IPv4 header structure, 37

## J

- Java, 94
- Jython
  - configuring Burp, 95
  - installing, 94

## K

- Kali Linux, 2, 94
  - installing, 5
  - upgrading, 2, 5

- KeyDown event, 129–130
- keylogger, 130–131
- KeyLogger class
  - get\_current\_process method, 128–129
  - mykeystroke method, 129
  - run method, 129–130
- keylogging, 128

## L

- LASTINPUTINFO structure, 135
- little-endian, 41
- lockout bypass, 80
- lxml library, 4, 74–76
  - HTMLParser, 75, 88, 90, 110

## M

- man-in-the-middle attack, 54
- mangle function, 112–113
- media access control (MAC), 57, 61–62
- memory snapshots, 171–172
- memory smear, 183
- Metasploit, 134
- Microsoft Developer Network (MSDN), 132, 158–159
- Miessler, Daniel, 87
- MITM. *See* man-in-the-middle attack
- mouse-click detection, 138
- msfvenom, 134
- multiprocessing package, 58

## N

- namedtuple, 63–66
- Nathoo, Karim, 147
- netcat, 13, 164–165
- NetCat class, 14
  - handle method, 16
  - listen method, 15–16
  - run method, 15
  - send method, 15, 17
- network basics, 10
- network sniffing, 35, 50
- \_\_new\_\_ function, 40
- Nibble. *See* nybble
- nmap, 36
- nybble, 41–42

## O

- offensive forensics, 169
- OpenCV library, 63, 68–69
  - dependencies, 69
- OWASP, 85

## P

- packet forwarding, 62
- packet sniffing, 36–38
- paramiko library, 26–29
  - channel, 33
  - installation, 25
  - rforward demo, 32, 34
  - reverse\_forward\_tunnel function, 32
  - transport, 33
- pastebin.com, 145–146, 148
- Payloads tab, Burp, 102
- pcap processing, 53, 63
- PE file, 179
- pefile library, 179
- PEP 8, 6
- pip, 4
- portable executable file, 178–181
- PortSwigger Web Security, 94
- Port Unreachable error, 46
- Positions tab, Burp, 102
- Post Office Protocol (POP3), 54, 57
- PowerShell, 153, 161, 164, 170
- privilege escalation, 153
- prn parameter, 54
- Process Environment Block (PEB), 181
- process monitor, 156–157
- promiscuous mode, 37–38
- proxy\_handler function (*TCP Proxy*), 22
- PyCharm IDE, 5
- pycryptodome library, 26, 140, 170
- pycryptodomex package, 140
- pyinstaller library, 121, 154, 165
- Python 2.x
  - web libraries, 72
  - syntax (Jython), 94
- Python 3
  - import customization, 123–124
  - setting up and installing, 3–5
  - web libraries, 72–74
- python3-venv library, 3

- pywin32 library, 131, 140, 154
- PyWinHook library, 128, 136

## Q

- Queue object, 76–80, 82–84

## R

- ReadDirectoryChangesW, 162–163
- Recapper class, 63–67
  - get\_responses method, 65–67
  - write method, 67
- registerIntruderPayloadGenerator
  - Factoryfunction, 96–97
- Repeater tool, Burp, 96
- requests library, 74, 146
  - get request, 74
  - post request, 74
  - session object, 87
- response\_handler function, 21–23
- reverse SSH tunnel example, 34
- rforward demo, 32
- RTLMoveMemory, 133–134

## S

- sandbox, 135–138
- Scanner class, 48–49
  - sniff method, 48
- Scapy library, 53–54
  - packet\_callback example, 56
- Scope tab, Burp, 109
- screenshot function, 132
- screenshots, 131–132
- SecLists, 87
- SelectObject function, 131–132
- SeLoadDriver, 159–160
- server\_loop function (*TCP Proxy*), 23
- SetWindowsHookEx, 128
- shellcode, 132–134
- shellcode execution, 132
  - get\_code function, 133
  - run function, 133
  - write\_memory function, 133
- shlex library, 13, 28
- Simple Mail Transfer Protocol (SMTP), 54, 57, 143
- slice syntax, 69
- smtplib library, 142–143

- sniffing network, 35, 36, 54
- SOCK\_DGRAM parameter, 11, 48
- socket library, 10
- SOCK\_STREAM parameter, 10–12, 14, 22–23, 29
- SQL injection, 100, 104
- SSH client, 26–27, 30–31
- ssh\_command
  - direct connection with Paramiko, 26–27
  - reverse connection with Paramiko, 26–27
  - SSH server with Paramiko, 28
- SSH tunneling, 30–34
  - reverse, 31
  - reverse\_forward\_tunnel function, 32–33
- SSH with Paramiko, 26
- SSL, 118
- struct library, 39, 41
- subprocess library, 13, 27–28
  - call method, 155
  - check\_output method, 28
- SVNDigger, 82

## T

- TagStripper class, 110–111, 112
  - handle\_comment method, 110
  - handle\_data method, 110
  - strip method, 110
- Target tab, Burp, 109, 114
  - TCP. *See* Transmission Control Protocol
- testphp.vulnweb.com, 82–85
- threads, 81–82
  - thread.join method, 81
- tokens
  - privileges, 159–160
- Transmission Control Protocol (TCP), 10
  - client, 10, 12
  - proxy, 19
  - server, 12
- trojan, 117–125, 127
  - configuration, 120–121
  - github-aware, 121–123
  - Windows, 127

- Trojan class, 122
  - get\_config method, 122
  - get\_file\_contents function, 121–122
  - github\_connect function, 121–123
  - module\_runner method, 122–123
  - run method, 122–123
  - store\_module\_result method, 122–123
- try/except syntax, 78
- try/finally syntax, 78

## U

- User Datagram Protocol (UDP), 10–11
  - client, 11
  - datagram, 36, 49
  - host discovery, 36
- urllib library, 73–74, 76, 90, 105, 133
- urllib2 library, 72–73, 76
- urlopen function, 72–74, 133

## V

- VBScript, 153, 161–162, 164
- venv package, 4
- VirtualAlloc, 133–134
- VirtualBox, 1
- virtual environment, 3–5, 170
- virtual machine (VM), 1–2, 38, 85
- Visual Studio Code IDE, 5
- VMWare, 1
- Volatility
  - framework, 169
  - installing, 170
  - plug-ins, 171, 177–178
  - Volumetric interface, 170
- volshell interface, 170, 177
- vulnerability reconnaissance, 176

## W

- web application
  - analyzing, 71
  - attacks, 72
  - scraping for passwords, 110–115
  - tools, 71
- win32api package, 131, 135, 157
- win32com package, 140, 143–146
- win32con package, 131–132, 157, 160, 162–163

- win32file package, 144
- win32security package, 157, 160
- Windows
  - Graphic Device Interface (GDI), 131–132
  - Handle, 132
  - Outlook Application, 143
  - privilege escalation, 145
  - registry, 172
  - Services, 154
  - Sockets, 37
  - Token, 159
  - virtual machine (VM), 1
- WingIDE, 5
- Windows Management
  - Instrumentation (WMI), 154, 157
  - WMI library, 154
  - Wireshark, 35, 63, 67
- word list creation, 110–113
- WordPress, 76, 81, 86–87, 90–91
  - brute forcing login, 85–89
  - captchas, 86
  - installing, 76
  - mapping, 76–81
- Wuergler, Mark, 157

**X**

XSS. *See* cross-site scripting

**Z**

zlib library, 64, 66, 140