SEC573 – Automating Information Security with Python

Topics

- .exe 2–271-273
- 0b00100000 1–71
- 16-Bit UNICODE 1–73
- 16bit unicode 1–69
- 2to3 W–2-4, 1–224
  - division 1–229
  - issues 1–224

A

- Alerts
  - Unknown Unknowns 2–129
- AND 1–116
- args 2–320-321
- Artifact
  - Analysis 2–147
- ASCII 1–68, 1–72
- Assignment 1–26-27
- Authentication 2–214-215
  - Captchas 2–218
  - Kerberos 2–215
  - NTLM 2–215
  - OAuth 2–215
  - Session Hicjacking 2–217
  - SSL/TSL 2–216

B

- Backdoor W–5-4, 2–233
  - Alternatives 2–299, 2–306
- base16 1–32
- base2 1–32
- Beacons
  - Intersection 2–66
- Binary
  - Examples 1–71
- Binary Data
  - Regex 2–146
- bit math operators 1–33
- break 1–166
- Browser User Agent Strings 2–61
- Bytes 1–66
  - convert string 1–71

C

- Captchas 2–218
- Carving 2–120-121
- Categorize Data 2–64
- Character Frequency 2–71
  - Tables 2–72-73
- Checksums 2–100
- chr 1–74
- continue 1–166
- CookieJar 2–209-213
- Cookies 2–207
- Counter
  - Long-Short Tail Analysis 2–63
- counter 1–187
- Covert Channels 2–108

D

- Date/Time Format 2–187
- datetime.datetime.fromtimestamp 2–187
- Debugger
  - debugger breakpoint options 1–212
  - python -m pdb 1–214
  - python debugger PDB 1–214
  - tracebacks 1–213
  - visual code debugger 1–210
  - visual code debugger interface 1–211
- Debugging W–2-3
- Decimal
  - Examples 1–71
- deep copy lists 1–219
- defaultdict 1–186
- Dictionary W–2-2, 1–175
  - .get 1–191
  - 2 vs 3 1–179
  - Categorize Data 2–64
  - copy 1–177
  - items 1–183
  - keys 1–181
  - methods 1–178
  - speciality 1–185
    - counter 1–187
    - defaultdict 1–186
  - values 1–182
- Difference 2–58
- Directory 2–16
  - Subdirectory 2–18
- DNS Hostnames 2–60
- DNS Queries 2–238
- dup2 W–5-6

E

- Encapsulated Structures 2–127
- enumerate 1–161, 1–163
- Escape Characters 2–31
- Exception W–5-2, 2–253-257

F

- FALSE 1–118
- File W–3-1
  - Directory 2–16
  - Find 2–20
  - Input 2–7
  - Methods 2–9
  - Operations 2–8
  - os.walk 2–20
  - Pathlib.Path 2–14

  - Pathlib.Path.home 2–13-14
  - Paths 2–13
  - Read 2–10
    - gzip 2–22
    - zlib 2–22
  - With 2–8
  - Write 2–11
- filegrabber.py 2–250
- floats approximation 1–220
- for 1–157
  - enumerate 1–161, 1–163
- Forensics 2–115
  - Artifact Carving 2–116-118
  - Images 2–157-162
  - Live Hard-Drive Carving 2–120
  - Live Memory Carving 2–121
  - Registry 2–190-192
- Format Characters 2–131
- Function W–1-3, 1–89
  - arguments 1–92
  - lambda 1–217
  - return 1–94

G

- Generators 2–182
  - Yield 2–182
- Geoip2 2–67-70
- GET 2–196, 2–204
  - Cookies 2–207-209
- gethostbyaddr 2–238
- gethostbyname 2–238
- Glob 2–16
  - Wildcards 2–19
- global scope 1–100
- GPS 2–154-155
- gzip 2–22

H

- Hard-Drive Carving 2–120
- Hex
  - Encoding 1–77
  - Examples 1–71
- HTTP Communication W–4-4

I

- if 1–114
- if elif 1–122
- if else 1–120
- Image Forensics W–4-2
- Images
  - Analyse dead/static images 2–124
  - PIL → PIL
- Immutable 1–84
- Integers
  - decoding 1–74
  - encoding 1–74
- Intersection 2–58
  - Beacons 2–66
- io.BytesIO 2–107
- io.StringIO 2–107
- IP Addresses 2–62
  - Geoip2 2–67-70
- IPv4 2–240
- IPv6 2–240

K

- Kerberos 2–215
- kwargs 2–320-321

L

- lambda functions 1–217
- legb 1–99
- len 1–81
- Linux Live Network Capture 2–123
- Linux Sniffing 2–122
- List 1–141
  - .join 1–150
  - .split 1–149
  - comprehension 1–221
  - convert string 1–149
  - copies 1–148
  - deep copy 1–219
  - index 1–142
  - map 1–152
  - methods 1–144
  - slicing 1–147
  - sorting 1–153
  - sum 1–151
  - zip 1–151
- Log file analysis W–3-3
- logical operators 1–115
- Logs
  - Analyzing 2–53
  - Browser User Agent Strings 2–61
  - Categorize Data 2–64
  - Character Frequency 2–71
  - DNS Hostnames 2–60
  - IP Addresses 2–62
  - Long-Short Tail Analysis 2–63
    - Counter 2–63
  - Slicing Timestamps 2–65
- Long-Short Tail Analysis 2–63
  - Counter 2–63

M

- Math Operators 1–29
- Microsoft visual studio code 1–208
- Module
  - versions 1–194
- Modules W–1-2, 1–125

  - built in 2–5
    - hashlib 2–5
    - http.server 2–5
    - https 2–5
    - pdb 2–5
    - re 2–5
    - socket 2–5
    - subprocess 2–5
    - sys 2–5
    - urllib 2–5
  - import 2–11
  - install 2–7
  - Load from Web 2–323-325
  - main 2–13-14
  - third party 2–6
    - beautiful soup 2–6
    - gmail 2–6
    - impacket 2–6
    - pexpect 2–6
    - plaso 2–6
    - requests 2–6
    - scapy 2–6
  - vs scripts 2–12
- Mutable 1–84

N

- Namespaces 1–98
- non-blocking sockets 2–291
- NTLM 2–215

O

- OAuth 2–215
- Objects 2–309
  - init 2–315-316
  - Python 2–310-313
- Operators
  - AND 1–116
  - Bit 1–33
  - FALSE 1–118
  - logical 1–115
    - shortcuts 1–116
  - Math 1–29
  - OR 1–117
    - Regex 2–34
  - TRUE 1–118
- OR 1–117
- ord 1–74
- os.dup2 2–305
- os.listdir 2–17
- os.walk 2–20

P

- Packet Analysis W–3-4
  - Assembly Issues 2–101
  - Bad Checksums 2–100
  - Custom single purpose analyzer 2–93
  - Duplicate Packets 2–99
  - IP Packet Fragmentation 2–102
  - OS Dependent Reassembly 2–104
  - Overlapping Fragments 2–103
  - Packet Order 2–97
  - PacketLists 2–81
  - Reassemble Payloads 2–96
  - reassembly.py 2–105-106
  - Scapy 2–79
  - Sorting Packets 2–98
  - Streams 2–94
- Parser 2–128
  - Unknown Unknowns 2–129
- Parsing Data Structures W–4-1
- Path 2–13, 1–195
  - Glob 2–16
  - os.listdir 2–17
  - os.walk 2–20
  - Path.exists 2–15
  - Pathlib.Path 2–14
  - Pathlib.Path.home 2–13-14
  - rGlob 2–18
- PCAP 2–126
- PcapReader 2–83
- Pen Test
  - Use case 2–232
- PEP 1–14
- PhysicalDrive0 2–120
- PIL 2–149
  - Key functions 2–151
  - Metadata 2–152-153
  - Open 2–150
- pip 2–7-9
- Pipe 2–265
- Popen 2–265
- POST 2–197-198, 2–204
  - Cookies 2–207-209
- Print 1–20
  - Format Specifier 1–62-64
- Process Execution W–5-3, 2–263-268
- Proxies 2–206
- PyInstaller 2–271-273
- Pyterpreter W–5-6, 2–206
  - stdio control 2–322
- Python
  - Backdoor 2–233
  - environments 1–193
  - Interpreter 1–15
  - path 1–195
  - python -c 1–21, 1–131
  - python -i 1–214
  - python -m pdb 1–214

R

- Randomness

  Character Frequency 2–71
range 1–160
rdpcap 2–81
re → Regex
reassembly.py 2–105-106
recv 2–242
  limitations 2–283
  recvall W–5-5, 2–286-287
    delimiter-based 2–289
    fixed-byte 2–288
    select.select() based 2–293-294
    timeout-based non-blocking sockets 2–290
Regex W–3-2, 2–27
  Back referencing 2–45-46
  Binary Data 2–146
  Capture Groups 2–40
    Named 2–44
  Custom Sets 2–33
  Escape Characters 2–31
  Flags 2–36
  Greedy Matching 2–37
  Logical OR 2–34
  Match 2–43
  Modifiers 2–36
  NOT custom set 2–38
  re 2–28
    findall 2–28
    match 2–28
    search 2–28
  Repeating Characters 2–35
  Rules 2–29-30
  Search 2–43
  Testing 2–48
Registry → Windows
  Registry
Registry Forensics W–4-3
Remote Python 2–326
Requests 2–194, 2–200-202
  Authentication 2–214-215
  Cookies 2–207-209
  https 2–216
  Proxies 2–206
  Session 2–203
  SSL/TLS 2–216

S

Scapy 2–79
  PacketLists 2–81
    Layers 2–90-92
    Sessions 2–87-88
    Structure 2–89
  PcapReader 2–83
  plist 2–84
  rdpcap 2–81
  Read 2–81
  Sniff 2–82
  time Order 2–82
  Timestamp Order 2–94
  Write 2–81
  wrpcap 2–81
scripts vs modules 2–12
send 2–242
  limitations 2–283
  sendall 2–284-285
Session Hijacking 2–217
Sets 2–54
  Copy 2–57
  Difference 2–58
  Intersection 2–58
    Beacons 2–66
  Methods 2–55
  Operators 2–56
  Union 2–58
  Update 2–58
Shortcut operators 1–119
site modules 1–198
site packages 1–198
Sniff 2–82
Socket Essentials W–5-1
Sockets 2–237
  AF-INET 2–240
  AF-INET6 2–240
  AF-PACKET 2–123
  bind listen accept 2–241
  Connections 2–241
  gethostbyaddr 2–238
  gethostbyname 2–238
  IPv4 2–240
  IPv6 2–240
  non-blocking sockets 2–291
  RCVALL-ON 2–122
  Receiving 2–242
  recv 2–242
  send 2–242
  SIO-RCVALL 2–122
  SOCK-DGRAM 2–239
  SOCK-RAW 2–123
  SOCK-STREAM 2–240
  socket.ntohs(0x0003) 2–123
  TCP 2–240
  timeout-based non-blocking sockets 2–290-292
  Transmit 2–242
  UDP 2–239
sort vs sorted 1–155
sorting 1–153
SQL 2–164
  Basic Statements 2–166-167
  Database Modules 2–173
  Joins 2–168
  sqlite3 2–174-175
  Subqueries 2–171
  Union 2–169-170
sqlite3 2–174-175
SSL/TSL 2–216
Standard libraries 1–197

stderr 2–300-303
stdin 2–300-303
stdout 2–300-303
String
  convert bytes 1–71
  Escape Characters 2–31
Strings W–1-2, 1–59
  .format 1–61
  encoders and decoders 1–82
  encoding 1–72
  find 1–87
  fstring 1–64
  len 1–81
  methods 1–77
    count 1–78
    in 1–78
    lower 1–78
    replace 1–78
    split 1–78
    title 1–78
    upper 1–78
  raw strings 1–65
  slicing 1–75
strings convert list 1–149
STRUCT 2–130
  Ether Header Struct 2–136
  Format Characters 2–131
  ICMP Header Struct 2–140-144
  IP Header Struct 2–137
  Pack 2–135
  TCP Header Struct 2–138
  UCP Header Struct 2–139
  Unpack 2–132-133
  Unpack Bits as Flags 2–134
Subprocesses 2–263
  Pipe 2–265
  Popen 2–265
  wait 2–264-265
Syntax
  namespaces 1–98
  spacing 1–96
  white space 1–96
sys 2–300-303
sys.metapath 2–324
sys.path 1–200

T

TCP 2–237
  Client 2–243
  Server Example 2–244
  Sockets 2–240
TCP Streams 2–86
Timestamps
  Slicing 2–65
TRUE 1–118
try/except/else 2–255-257
Tuple 1–171
  sorted 1–173
Types
  Reassign 1–27

U

UDP 2–237
  Sockets 2–239
unichr 1–74
UNICODE 1–73
Union 2–58
Unpack 2–316-319
  args 2–320-321
  kwargs 2–320-321
Urllib 2–196, 2–198
utf8 1–70

V

Variable 1–23
  global scope 1–100
  resolution legb 1–99
  typing 1–101
venv 1–201
virtual environment W–2-3, 1–202

W

Web
  Browser
    GET/POST 2–204
  Encoding 2–195
  GET 2–196
  POST 2–197
  Requests 2–194, 2–200-202
  Session 2–203
  Urllib 2–196
  Websites 2–194
Webimport 2–325
while 1–164
Windows
  Registry 2–177-181
    Date/Time Format 2–187
    Forensics 2–190-192
    Network Profiles 2–186
    WiFi 2–184-185, 2–188
Windows Live Network Capture 2–122
Windows Sniffing 2–122
Wireshark
  TCP Streams 2–86
With 2–8
wrpcap 2–81

X

XOR 1–162

Z

zlib 2–22