

Topics

.exe	5-45-47
//	1-29
0b00100000	1-67
16-Bit UNICODE	1-69

A

Alerts	
Unknown Unknowns	4-16
AND	1-116
args	5-96-98
Artifact	
Analysis	4-34
Third party modules	4-34
ASCII	1-68
Assignment	1-26-27
base16	1-32
base2	1-32
Authentication	4-100-101
Captchas	4-104
Kerberos	4-101
NTLM	4-101
OAuth	4-101
Session Hijacking	4-103
SSL/TSL	4-102

B

Backdoor	5-5
Alternatives	5-74, 5-81
Beacons	
Intersection	3-67
bin()	1-32
Binary	
Examples	1-67
Binary Data	
Regex	4-33
Binary executable tools	
Freeze	5-45
Nuitka	5-45
py2app	5-45
Py2exe	1-15, 5-45
PyInstaller	1-15, 5-45
bind	5-13
Bit math operators	1-33
bitwise AND	1-33
bitwise complement	1-33
bitwise OR	1-33
bitwise XOR	1-33
shift bits left	1-33
shift bits right	1-33
bool	1-118
Boolean value	1-118
break	2-61
Breakpoint	

Breakpoint options	1-129
Expression	1-126
Hit count	1-126
PDB breakpoint	1-126
Browser User Agent Strings	3-62
Bytes	1-66
convert string	1-71
bytes().decode()	1-71

C

CamelCase	5-84
Captchas	4-104
Capture Groups	3-33, 3-39
Non-capture groups	3-41
Carving	4-8-9
Categorize Data	3-65
Character Frequency	3-72
Tables	3-73-74
Checksums	3-101
chr	1-74
continue	2-61
continue → try continue	
Control statements	1-113
else/elif	1-120
if	1-114
Logical operators	1-115
CookieJar	4-95-99
Cookies	4-93
Copies	
deepcopy	2-91
Dictionaries	2-73
Lists	2-42
Sets	2-58
Counter	2-83
Long-Short Tail Analysis	3-64
Covert Channels	3-109
Current working directory	2-19

D

Date/Time Format	4-73
datetime.datetime.fromtimestamp	4-73
Debugger	
debugger breakpoint options	1-129
python -m pdb	1-126
python debugger PDB	1-126
tracebacks	1-125
visual code debugger	1-127
visual code debugger interface	1-128
Decimal	
Examples	1-67
Decompilers	
Decompyle++	1-15
uncompyle6	1-15
deep copy lists	2-91
defaultdict	2-82

Dictionary	2-71
.get	2-87
Categorize Data	3-65
copy	2-73
items	2-79
keys	2-77
looping	2-77
methods	2-74
ordered vs. unordered	2-71
Python 2 vs 3	2-75
speciality	2-81
counter	2-83
defaultdict	2-82
values	2-78
Difference	3-59
Directory	3-15
Subdirectory	3-17
dist-package	2-21
division	1-29
DNS Hostnames	3-61
DNS Queries	5-10

E

EBCDIC	1-68
Encapsulated Structures	4-14
Documents	4-14
Hard drives	4-14
Memory	4-14
Networking	4-14
enumerate	2-56, 2-58
Escape Characters	3-30
Exception handling	5-25-26
Exif tags	4-39
Exists	3-14

F

FALSE	1-118
File	
Append	3-10
binary	3-7
Directory	3-15
Find	3-19
Input	3-6
Methods	3-8
close	3-8
read	3-8
readlines	3-8
seek	3-8
tell	3-8
write	3-8
writelines	3-8
open	3-7
Operations	3-7
os.walk	3-19
Pathlib.Path	3-13

Pathlib.Path.home	3-14-15
Paths	3-12
Read	3-9
gzip	3-21
zlib	3-21
text	3-7
With	3-7
Write	3-10
File mask	3-17
Float	
approximation	2-92
floor	1-29
for	2-52
enumerate	2-56, 2-58
Forensics	4-4
Carving	
Artifact	4-5-7
Data stream	4-5
File stream	4-5
Live Hard-Drive	4-8
Images	4-44-49
Live Memory Carving	4-9
Registry	4-76-78
Format Characters	4-18
Freq.py	3-73-74
Frequency Tables	3-73-74
Function	1-89
arguments	1-92
Interactive shell	1-97
Keyword arguments	1-94
kwargs	1-94
lambda	2-89
Optional arguments	1-94
Positional assignment	1-94
return	1-89, 1-94
scope	1-89

G

Geoip2	3-68-71
GET	4-82, 4-90
Cookies	4-93-95
get()	2-87
gethostbyaddr	5-10
gethostbyname	5-10
Glob	3-15
Wildcards	3-18
Global scope	1-100
GPS	4-41-42
gzip	3-21

H

Hard-Drive Carving	4-8
Hex	
Encoding	1-73
Examples	1-67

hex() 1–32

I

if 1–114
if elif 1–122
if else 1–120
if var doesn't exist - error
Images
 Analyse dead/static images 4–12
 PIL → PIL
Immutable 1–84
Init 5–87
Integers
 decoding 1–74
 encoding 1–74
Intersection 3–59
 Beacons 3–67
Interval analysis 3–66
Introspection 2–9
 dir() 2–9
 help() 2–9
 type() 2–9
io.BytesIO 3–108
io.StringIO 3–108
IP Addresses 3–63
 Geopip2 3–68–71
IPv4 5–12
IPv6 5–12
Iterable 2–46
Itertools compress 4–21

K

Kerberos 4–101
kwargs 5–96–98

L

Lab Highlights
 File Operations 3–24
 Functions Hold and Process Data 1–110
 Getting Data In and Out of Dictionaries Is
 Easy/Fast 2–87
 Most List Methods Don't Return Values 2–65
 One Possible Answer - Image resizing 4–49
 One Possible ICMP Decoder 4–31
 One Possible Solution - Socket recv 5–22
 Regular Expressions 3–51
 Scapy Packet Reassembly 3–113
 Sockets Block if There Is No Data in Buffer . 5–21
 Sum all the values 4–78
 Use of the Find Method 1–87
 We have a working backdoor 5–51
 You Can Now Download LARGE Files 5–72
 You Now Have Two More Backdoors 5–105

lambda functions 2–89
Latin-1 3–11
LEGB 1–99
len 1–81
Linux Live Network Capture 4–11
Linux Sniffing 4–11
List 2–35
 .join 2–44
 .split 2–43
 comprehension 2–93
 convert string 2–44
 copies 2–42
 deep copy 2–91
 index 2–36
 map 2–46
 methods 2–38
 append 2–38
 count 2–38
 del list 2–38
 index 2–38
 insert 2–38
 list 2–38
 remove 2–38
 sort 2–38
 slicing 2–41
 sorting 2–47
 sum 2–45
 zip 2–45
logical operators 1–115
Logs
 Analyzing 3–53
 Browser User Agent Strings 3–62
 Categorize Data 3–65
 Character Frequency 3–72
 DNS Hostnames 3–61
 Interval analysis 3–66
 IP Addresses 3–63
 Long-Short Tail Analysis 3–64
 Counter 3–64
 Slicing Timestamps 3–66
 Long-Short Tail Analysis 3–64
 Counter 3–64

M

Math Operators 1–29
 Shortcuts 1–30
Maxmind 3–68
Microsoft visual studio code 1–103
Module
 versions 2–17
Modules 2–4
 built in 2–5
 hashlib 2–5
 http.server 2–5
 pathlib 2–5
 pdb 2–5
 re 2–5

socket	2-5
subprocess	2-5
sys	2-5
import	2-11
install	2-7
Load from Web	5-99-101
main	2-13-14
name variable	2-12
third party	2-6
beautiful soup	2-6
DFF	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

Named capture groups	3-43
Namespaces	1-98
Builtin	1-99
Enclosing	1-99
Global	1-99
LEGB	1-99
Local	1-99
Scope override	1-100
netcat	5-39
non-blocking sockets	5-66
NTLM	4-101

O

OAuth	4-101
Objects	5-84
Add Attributes	5-87
Add Methods	5-85
init	5-87-89
Python	5-85-88
Operators	
AND	1-116
Bit	1-33
FALSE	1-118
logical	1-115
shortcuts	1-115
Math	1-29
OR	1-117
Regex	3-33
TRUE	1-118
Truth tables	1-117
OR	1-117
ord	1-74
Order of operations	1-31
BEDMAS	1-31
BOMDAS	1-31

PEMDAS	1-31
Ordinal values	2-48
os.dup2	5-80
os.listdir	3-16
os.walk	3-19

P

Packet Analysis	
Assembly Issues	3-102
IDS evasion	3-102
IP fragmentation	3-102
Bad Checksums	3-101
BSD Reassembly	3-105
Custom single purpose analyzer	3-94
Duplicate Packets	3-100
IP Packet Fragmentation	3-103
Linux Reassembly	3-105
OS Dependent Reassembly	3-105
Overlapping Fragments	3-104
Packet Order	3-98
PacketLists	3-82
Printer/HP Reassembly	3-105
Reassemble Payloads	3-97
reassemble.py	3-106-107
Scapy	3-80
Sorting Packets	3-99
Streams	3-95
Windows Reassembly	3-105
Packet Fields	3-92
Packet Layers	3-91
Parser	4-15
Unknown Unknowns	4-16
Path	3-12, 2-15, 2-18
.pth file	2-21
Glob	3-15
lib	2-23
lib-dynload	2-23
os.listdir	3-16
os.py	2-23
os.walk	3-19
Path.exists	3-14
Pathlib.Path	3-13
Pathlib.Path.home	3-14-15
pyenf.cfg	2-23
rGlob	3-17
sys.path	2-23
PCAP	4-13
Structure	4-13
PcapReader	3-84
PDB	1-126
Pen Test	
Use case	5-4
PEP	1-13-14
PEP8	
ClassNames	5-84
PhysicalDrive0	4-8
PIL	4-36

Key functions	4–38
Metadata	4–39–40
Open	4–37
PILLOW	4–36
pip	2–7–9
help	2–9
install	2–9, 2–26
list	2–9
show	2–9
Pipe	5–37
Popen	5–37
POST	4–83–84, 4–90
Cookies	4–93–95
Print	1–20
Format Specifier	1–62–64
Process Execution	5–35–40
Proxies	4–92
pupy.py	5–102
PyInstaller	5–45–47
Pypcap	4–10
Pyterpreter	5–81
stdio control	5–98
Python	
Backdoor	5–5
environments	2–17
Interactive shell	1–17–18
hotkeys	1–18
Interpreter	1–15
path	2–18
python -m pdb	1–126
Virtual environments	2–17
Year developed	1–11
Python -c	1–16
Python Image Library	4–36
Python objects	
Comments	1–21
Delimiters	1–21
Keywords	1–21
Literals	1–21
Operators	1–21
Variables	1–21
PYTHONPATH	2–15

R

Randomness	
Character Frequency	3–72
range	2–55
RAT	5–102
Raw sockets	4–11
rdpcap	3–82
re → Regex	
reassembler.py	3–106–107
recv	5–14
limitations	5–57
recvall	5–60–62
delimiter-based	5–64
fixed-byte	5–63

select.select() based	5–68–69
timeout-based non-blocking sockets	5–65
REG-BINARY	4–73
Regex	3–26
.	3–36
Back referencing	3–45–46
Binary Data	4–33
Capture group	3–33
Capture Groups	3–39
Named	3–43
Custom Character Sets	3–32
Escape Characters	3–30
Flags	3–35
Greedy Matching	3–36
Logical OR	3–33
Match	3–42
Match characters	3–29–31
Match object	3–42
Modifiers	3–35
case sensitivity	3–35
match newlines	3–35
multiline matching	3–35
NOT custom set	3–37
re	3–27
findall	3–27
match	3–27
search	3–27
Repeating Characters	3–34
Rules	3–28–29
Search	3–42
Testing tools	3–48
Registry	4–65–69
Registry → Windows	
Registry	
Regular expressions	3–26
Remote Python	5–102
Reputation	
Filters	5–52
Requests	4–80, 4–86–88
Authentication	4–100–101
Cookie object	4–96
CookieJar	4–93
Cookies	4–93–95
https	4–102
Kerberos	4–101
NTLM	4–101
OAuth	4–101
Proxies	4–92
Response object	4–88
Session	4–89
SSL/TLS	4–102

S

Scapy	3–80
PacketLists	3–82
Fields	3–92
Layers	3–90–92

Sessions	3-88-89	SOCK-RAW	5-9, 4-11
Structure	3-90	SOCK-STREAM	5-12
PcapReader	3-84	socket.ntohs(0x0003)	4-11
plist	3-85	TCP	5-12
rdpcap	3-82	timeout-based non-blocking sockets	5-65-67
Read	3-82	Transmit	5-14
Sniff	3-83	UDP	5-11
Sorting Packets	3-99	sort vs sorted	2-48
time Order	3-95	Sorting	2-47
Timestamp Order	3-95	sorting packets → Packet Analysis	
Write	3-82	SQL	4-51
wrpcap	3-82	Basic Statements	4-54-55
Scapy → Packet Analysis		Database Modules	4-61
scripts vs modules	2-12	Joins	4-56
send	5-14	sqlite3	4-62-63
limitations	5-57	Subqueries	4-59
sendall	5-58-59	Union	4-57-58
vs sendall	5-58	sqlite3	4-62-63
Session Hijacking	4-103	SSL/TSL	4-102
Sets	3-55	Standard libraries	2-20
Cardinality	3-56	stderr	5-75-78
Copy	3-58	stdin	5-75-58
Difference	3-59	stdout	5-75-58
Intersection	3-59	str().encode()	1-71
Beacons	3-67	String	
Methods	3-56	convert bytes	1-71
difference	3-56	Escape Characters	3-30
intersection	3-56	Strings	1-59
isdisjoint	3-56	.format	1-61
issubset	3-56	byte strings	1-65
issuperset	3-56	Codecs	1-82
len	3-56	base64	1-82
symmetric_difference	3-56	bz2	1-82
union	3-56	HEX	1-82
Operators	3-57	ROT-13	1-82
Union	3-59	ZIP	1-82
Update	3-59	encoders and decoders	1-82
Shortcut operators	1-119	encoding	1-72
site modules	2-21	find	1-87
site packages	2-21	fstring	1-64
Sniff	3-83	len	1-81
Sockets	5-9	methods	1-77
AF-INET	5-12	count	1-78
AF-INET6	5-12	in	1-78
AF-PACKET	4-11	lower	1-78
bind listen accept	5-13	replace	1-78
Connections	5-13	replace(old, new, count)	
gethostbyaddr	5-10	split	1-78
gethostbyname	5-10	title	1-78
IPv4	5-12	upper	1-78
IPv6	5-12	raw strings	1-65
non-blocking sockets	5-66	slicing	1-75
RCVALL-ON	4-10	strings convert list	2-43
Receiving	5-14	Struct	4-17
recv	5-14	Ether Header Struct	4-23
send	5-14	Format Characters	4-18
SIO-RCVALL	4-10	ICMP Header Struct	4-27-29
SOCK-DGRAM	5-11	IP Header Struct	4-24

Itertools compress	4-21
Pack	4-22
TCP Header Struct	4-25
UDP Header Struct	4-26
Unpack	4-19-20
Unpack Bits as Flags	4-21
Subprocesses	5-35
Pipe	5-37
Popen	5-37
run	5-38
wait	5-36-37
Syntax	
namespaces	1-98
spacing	1-96
white space	1-96
sys	5-75-58
sys.meta-path	5-100
sys.path	2-15

T

TCP	5-9
Client	5-15
Server Example	5-16
Sockets	5-12
TCP Streams	3-87
Timestamps	
Slicing	3-66
TRUE	1-118
Truth tables	1-117
try continue	5-28
try/except/else	5-27-29
Tuple	2-67
Immutable	2-67
packing	5-92
sorted	2-69
Types	
Reassign	1-27

U

UDP	5-9
Sockets	5-11
unichr	1-74
UNICODE	1-69
Union	3-59
Unknown Unknowns	4-16
Unpack	5-93-95
args	5-96-98
kwargs	5-96-98
Urllib	4-82, 4-84
user-site	2-21
UTF-8	1-70
Continuation	1-70-72

V

Variable	1-23
Byte	1-24
Dictionary	1-24
Float	1-24
Function	1-25
global scope	1-100
Integer	1-24
List	1-24
Namespace	1-23
Override scope	1-100
resolution legb	1-99
String	1-24
Tuple	1-24
typing	1-101
venv	2-24
Virtual environment	2-24
Activating	2-25
Deactivating	2-25
Windows	2-29
Virtual environments	2-17
venv	2-17
virtualenv	2-17

W

Web	
Encoding	4-81
GET	4-82
POST	4-83
Requests	4-80, 4-86-88
Session	4-89
Urllib	4-82
Websites	4-80
Web Browser	
GET/POST	4-90
Webimport	5-101
while	2-52, 2-59
Windows	
Registry	4-65-69
Date/Time Format	4-73
Forensics	4-76-78
Network Profiles	4-72
REG-BINARY	4-73
Retrieving keys and subkeys	4-68
WiFi	4-70-71, 4-74
Wireless history	4-70-71
Windows Live Network Capture	4-10
pypcap	4-10
Windows Sniffing	4-10
Windows virtual environment	2-29
Wireshark	
TCP Streams	3-87
With	3-7
Workshop	
Backdoor	W-5-4
Debugging	W-1-4
Dictionary	W-2-3
dup2	W-5-6

Exception	W-5-2
File I/O	W-3-1
Function	W-1-3
HTTP Communication	W-4-4
Image Forensics	W-4-2
Lists	W-2-2
Log file analysis	W-3-3
modules	W-2-1
Packet Analysis	W-3-4
Parsing Data Structures	W-4-1
Process Execution	W-5-3
Pyterpreter	W-5-6
recv	
recvall	W-5-5
Regex	W-3-2
Registry Forensics	W-4-3
Socket Essentials	W-5-1
Strings	W-1-2
virtual environment	W-2-1
wrpcap	3-82
XOR	2-57
Zlib	3-21