

Inhaltsverzeichnis

1 Einführung	7
1.1 Rechtlicher Hinweis (Disclaimer)	7
1.2 Was erwartet dich in diesem Buch?	8
2 Ethical Hacking	13
2.1 Was ist Hacking?	13
2.2 Schutzziele der Informationssicherheit	14
2.2.1 Vertraulichkeit (Confidentiality)	15
2.2.2 Integrität (Integrity)	15
2.2.3 Verfügbarkeit (Availability)	16
2.2.4 Erweiterte Schutzziele der Informationssicherheit	16
2.3 Arten von Hackern	16
2.4 Die fünf Phasen eines Hacking-Angriffs	19
2.5 Advanced Persistent Threats (APT)	20
2.6 Blue-Team	22
2.7 Red-Team	23
2.8 Wie wird man ein Hacker?	25
3 Malware	30
3.1 Biologische Viren vs. Computerviren	30
3.2 Computerwurm	33
3.3 Keylogger	34
3.4 Trojaner	35
3.5 Ransomware	36
3.6 Software als Kriegswaffe	38
3.7 VirusTotal	41
4 Python-Grundlagen für Einsteiger	46
4.1 Was ist Python?	46
4.2 Wie man Python zum Hacken nutzen kann	47

4.3	Installation von Python	47
4.3.1	Installation unter Windows	47
4.4	Installation von pip unter Windows	52
4.5	Das erste Programm	56
4.6	Der interaktive Modus	57
4.7	Variablen und Datentypen	60
4.8	String-Operationen	63
4.9	Operatoren und Operatorrangfolge	67
4.9.1	Die vier Grundrechenarten	67
4.9.2	Potenzieren	71
4.9.3	Modulo (Teilen mit Rest)	72
4.9.4	Vergleichsoperatoren	73
4.9.5	Logische Operatoren	74
4.10	Zahlensysteme	77
4.10.1	Das Dezimalsystem	77
4.10.2	Stellenwertsysteme	78
4.10.3	Das Binärsystem	79
4.10.4	Das Hexadezimalsystem	81
4.10.5	Little Endian vs. Big Endian	85
4.11	Bitweise Operatoren	87
4.11.1	Binärzahlen darstellen	87
4.11.2	Bitweise and-Verknüpfung (&)	90
4.11.3	Bitweise or-Verknüpfung ()	91
4.11.4	Bitweise xor-Verknüpfung (^)	92
4.11.5	Das Einerkomplement	93
4.11.6	Das Zweierkomplement	95
4.11.7	Bitweiser not-Operator (~)	98
4.11.8	Bit-Verschiebung (<< und >>)	99
4.11.9	Anwendung von bitweisen Operatoren	101
4.11.10	Operatorrangfolge	104
4.12	Funktionen	105
4.12.1	Was sind Funktionen?	105
4.12.2	Definition von Funktionen	106
4.12.3	*args und **kwargs	108
4.12.4	if __name__ == "__main__"	112
4.12.5	eval	117
4.13	Interaktion mit dem Benutzer	119
4.14	Datenstrukturen	121
4.14.1	Listen	121

4.14.2	Tupel	131
4.14.3	Sets.....	136
4.14.4	Dictionaries	140
4.15	Kontrollstrukturen	146
4.15.2	for-Schleife.....	153
4.15.3	while-Schleife	160
4.16	Dateien lesen und schreiben.....	168
4.17	Bibliotheken.....	173
4.18	Objektorientierte Programmierung.....	177
4.18.1	Was ist objektorientierte Programmierung?.....	177
4.18.2	Klassen und Objekte	180
4.18.3	Methoden vs. Funktionen	187
4.18.4	Vererbung.....	193
4.19	Fehler und Ausnahmen.....	199
4.19.1	Warum müssen Fehler und Ausnahmen behandelt werden?	199
4.19.2	try und except.....	202
4.19.3	finally.....	205
4.20	Kommandozeilenprogramme	207
4.20.1	Übergabeparameter am Beispiel „Netcat“	207
4.20.2	argv	211
4.20.3	argparse	214
4.21	CMD-Befehle mit Python ausführen (subprocess).....	225
4.21.1	Popen	226
4.21.2	getoutput	228
4.22	Fortschrittsbalken (tqdm).....	230
5	Hacking-Labor	235
5.1	VirtualBox und Kali Linux installieren	235
5.2	NAT-Netzwerk einrichten	247
5.3	OWASP Juice Shop	251
5.4	Metasploitable 2.....	253
6	Passwörter von ZIP-Dateien wiederherstellen mit Python	257
6.1	Was ist eine ZIP-Datei?	257
6.2	ZIP-Dateien verpacken, verschlüsseln, entpacken und entschlüsseln	258
6.3	ZIP-Bomben	266
6.4	fcrackzip	267
6.5	ZIP-Cracker mit Python	271

7	Passwörter knacken mit Python	277
7.1	Was sind Passwörter?	277
7.2	Was sind sichere Passwörter?	279
7.3	Passwortmythen	283
7.3.1	Mythos Nr. 1	283
7.3.2	Mythos Nr. 2	283
7.3.3	Mythos Nr. 3	284
7.3.4	Mythos Nr. 4	284
7.3.5	Mythos Nr. 5	285
7.3.6	Mythos Nr. 6	285
7.3.7	Mythos Nr. 7	286
7.3.8	Mythos Nr. 8	286
7.3.9	Mythos Nr. 9	287
7.3.10	Mythos Nr. 10	287
7.4	Passwortkarten	287
7.5	Hashfunktionen	290
7.6	Wie werden Passwörter gespeichert?	296
7.7	Passwörter knacken mit Hashcat	298
7.7.1	Installation von Hashcat	298
7.7.2	Aufbau eines Befehls in Hashcat	303
7.7.3	Hashalgorithmen erkennen	309
7.7.4	Bute-Force-Attacke	310
7.7.5	Dictionary-Attacke	314
7.7.6	Mask-Attacke	318
7.8	Passwörter mit Python generieren	324
7.9	Passwörter mit Python knacken	329
7.10	CVE-2023-32784	337
7.11	CVE-2023-32784 mit Python automatisieren	348
7.12	PDF-Dateien mit Python schützen	353
7.13	Word-Dateien mit Python schützen	356
7.14	Excel-Dateien mit Python schützen	359
7.15	Das Herz der Passwortkarten	361
8	Netzwerktechnik-Crashkurs	367
8.1	Was ist ein Netzwerk?	367
8.2	OSI-Schichtenmodell	368
8.3	LAN vs. MAN vs. WAN vs. GAN	371
8.4	Client-Server-Modell	373
8.5	MAC-Adressen	376

8.6	IP-Adressen	379
8.6.1	Was ist eine IP-Adresse?	379
8.6.2	Aufbau einer IPv4-Adresse	380
8.6.3	Wie findet man IP-Adressen heraus?	381
8.6.4	IP-Adressen verschleiern	383
8.6.5	127.0.0.1 vs. 0.0.0.0	384
8.7	Ports	385
8.8	Sockets	388
8.9	Address Resolution Protocol (ARP)	391
8.10	Internet Control Message Protocol (ICMP)	393
8.11	UDP vs. TCP	396
8.12	Der Three-Way-Handshake von TCP	398
8.13	Der TCP-Header im Detail	401
8.14	Nmap-Scan-Techniken	404
8.14.1	SYN-Scan	406
8.14.2	TCP-Connect-Scan	408
8.14.3	UDP-Scan	409
8.14.4	Null-Scan	410
8.14.5	FIN-Scan	411
8.14.6	XMAS-Scan	412
8.14.7	Version-Scan	412
8.15	HTTP	412
8.15.1	GET	415
8.15.2	POST	415
8.15.3	PUT	416
8.15.4	DELETE	416
8.15.5	HEAD	416
8.16	Persistente und nicht persistente Verbindungen	417
8.17	Network Address Translation (NAT)	419
8.18	Portscanning legal üben	422
8.19	Domain Name System (DNS)	424
8.20	Dynamic Host Configuration Protocol (DHCP)	430
8.21	File Transfer Protocol (FTP)	433
8.22	FTP-Exploit	437
8.23	Secure Shell (SSH)	439
8.24	SSH-Honeypot in Python	449
9	Portscanner mit Python	455

10 Metadatenanalyse mit Python	460
10.1 Was sind Metadaten?	460
10.2 exiftool	464
10.3 pymeta	467
11 Directory Enumeration mit Python	472
11.1 Fuzzing	472
11.2 DirBuster	473
11.3 GoBuster in Python	478
12 SSH Brute Forcer mit Python	484
13 Reverse Shell mit Python	489
13.1 Was ist eine Reverse Shell?	489
13.2 Wie funktioniert eine Reverse Shell?	490
13.3 Wie wird eine Reverse Shell aufgebaut?	491
13.4 Reverse Shell mit Python	495
14 Sicher verschlüsseln mit Python	504
14.1 Symmetrische vs. asymmetrische Verschlüsselung	504
14.2 Symmetrische Verschlüsselung mit Python	510
14.3 Asymmetrische Verschlüsselung mit Python	515
14.4 One-Time-Pad-Verschlüsselung mit Python	524
14.5 BND Ransomware-Decryptor Challenge	532
15 Lösungen zu den Übungsaufgaben	540