

Inhaltsverzeichnis

- 1 Vorwort..... 5**
 - 1.1 Über mich..... 5
 - 1.2 FAQ..... 6
 - 1.3 Wie liest man dieses Buch? 10
- 2 ChatGPT 13**
 - 2.1 Was ist künstliche Intelligenz?..... 13
 - 2.2 Starke vs. schwache KI..... 15
 - 2.3 KI-Winter..... 16
 - 2.4 Von Turing-Tests und chinesischen Zimmern 21
 - 2.5 Was ist ChatGPT? 25
 - 2.6 Machine Learning, Deep Learning und neuronale Netze..... 31
 - 2.7 Wie funktioniert ChatGPT? 35
 - 2.8 ChatGPT einrichten 37
 - 2.9 Was kann ChatGPT? 43
 - 2.10 Was kann ChatGPT nicht? 55
 - 2.11 GPTs 60
- 3 Einführung ins Ethical Hacking..... 68**
 - 3.1 Was ist Ethical Hacking?..... 68
 - 3.2 Disclaimer..... 69
 - 3.3 Arten von Hackern 72
 - 3.4 Schutzziele der Informationssicherheit..... 76
 - 3.4.1 Vertraulichkeit (Confidentiality) 76
 - 3.4.2 Integrität (Integrity) 77
 - 3.4.3 Verfügbarkeit (Availability)..... 77
 - 3.4.4 Erweiterte Schutzziele der Informationssicherheit 77
 - 3.4.5 ChatGPT bestimmt die Schutzziele..... 78
 - 3.5 Die Phasen eines Hacking-Angriffs..... 79
 - 3.6 Im Spannungsfeld zwischen „Gut“ und „Böse“ 83

4 Arbeitsumgebung einrichten	89
4.1 VirtualBox und Kali Linux installieren	89
4.2 NAT-Netzwerk einrichten	101
4.3 OWASP Juice Shop	105
4.4 Metasploitable 2	107
4.5 API-Key von OpenAI	110
4.6 Shell GPT	112
5 Prompt Engineering	118
5.1 Warum Python?	118
5.2 Installation	119
5.3 Was ist pip?	124
5.4 Wichtige pip-Befehle	124
5.5 pip installieren	127
5.6 Code mit ChatGPT generieren	130
5.7 ChatGPT-API mit Python	134
5.8 Was ist Prompt Engineering?	138
5.9 Anatomie eines Prompts	142
5.10 Custom Instructions	146
5.11 Prompts für verschiedene Use Cases	150
5.11.1 Beantworten von Fragen	150
5.11.2 Textzusammenfassung	154
5.11.3 Codegenerierung	156
5.12 Techniken des Prompt Engineerings	158
5.12.1 Zero-Shot Prompting	159
5.12.2 Few-Shot Prompting	159
5.12.3 Chain-of-Thought Prompting	162
5.12.4 Zero-Shot und Few-Shot Chain-of-Thought Prompting	163
5.13 Prompt-Engineering-Challenge: Musik-Player „Musixx“	166
6 Phishing	168
6.1 Was ist Phishing?	168
6.2 Was ist Typosquatting?	173
6.3 Wie meldet man Phishing?	176
6.4 Wie erkennt man Phishing?	178
6.5 Der Enkeltrick mit ChatGPT	181
6.6 Nigeria Connection	187
6.7 VirusTotal	190
6.8 Vorsicht! Geheimnisverrat!	195
6.9 Analyse von Phishing-Mails mit ChatGPT	199

6.10	Wie erkennt man Texte, die von ChatGPT geschrieben wurden?	211
6.10.1	GPTZero	212
6.10.2	GPT Radar.....	213
6.10.3	Content at Scale	214
6.11	Erstellen von Phishing-Mails mit ChatGPT.....	215
6.12	OSINT-Recherche mit ChatGPT (GPT-4)	221
7	Passwörter knacken mit ChatGPT	229
7.1	Was sind Passwörter?	229
7.2	Was sind sichere Passwörter?	231
7.3	Wie kann man sich Passwörter merken?	237
7.4	Hashfunktionen.....	241
7.5	Wie werden Passwörter gespeichert?.....	247
7.6	Passwörter knacken mit Hashcat	250
7.6.1	Installation von Hashcat	250
7.6.2	Aufbau eines Befehls in Hashcat.....	255
7.6.3	Hashalgorithmen erkennen	263
7.6.4	Bute-ForceAttacke	266
7.6.5	Dictionary-Attacke	270
7.6.6	Mask-Attacke	273
7.7	Hashcat-Befehle mit ChatGPT prompten	280
7.8	Hashcat-Befehle mit Shell GPT generieren.....	282
7.9	Passwörter automatisiert mit ChatGPT knacken	286
7.10	Code-Execution durch eine „böartige“ KI absichern	291
7.11	Passwort-Cracker mit ChatGPT	307
7.12	Passwort Guessing mit ChatGPT.....	311
8	Nmap mit ChatGPT.....	319
8.1	Nmap	319
8.2	ISO-OSI-Schichtenmodell	319
8.3	Ports.....	324
8.4	TCP und UDP	327
8.5	Der Three-Way Handshake von TCP.....	329
8.6	Der TCP-Header im Detail.....	332
8.7	Nmap-Scan-Techniken.....	334
8.7.1	SYN-Scan	337
8.7.2	TCP-Connect-Scan.....	338
8.7.3	UDP-Scan	339
8.7.4	Null-Scan.....	340
8.7.5	FIN-Scan	341

8.7.6 XMAS-Scan	342
8.7.7 Version-Scan	342
8.8 Portscanning legal üben	343
8.9 Reconnaissance mit Shell GPT	346
8.10 Schwachstellenanalyse mit Shell GPT	349
8.11 Interpretation von Nmap-Outputs mit ChatGPT	354
9 Sicherheitslücken im Code erkennen	359
9.1 Wie ist eine Webanwendung aufgebaut?	359
9.2 Cross-Site-Scripting (XSS)	361
9.3 SQL-Injection	371
9.4 Buffer Overflow	384
9.5 Mit ChatGPT Code automatisiert analysieren	396
9.6 Der OWASP-Prompt	400
9.7 Logdateien mit ChatGPT analysieren	404
9.8 Honeypot mit ChatGPT	407
10 Angriffe auf Large Language Models	418
10.1 OWASP Top 10 für LLM-Anwendungen	418
10.2 Prompt-Injection (LLM01)	421
10.3 Prompt-Injection-Training und Gegenmaßnahmen	429
10.3.1 Level 1	431
10.3.2 Level 2	432
10.3.3 Level 3	433
10.3.4 Level 4	434
10.3.5 Level 5	435
10.3.6 Level 6	435
10.3.7 Level 7	436
10.4 Prompt-Leaking	437
10.5 Training Data Poisoning (LLM03)	441
10.6 Model Stealing / Model Theft (LLM10)	444
11 Die Zukunft	446
11.1 Die Gefahr von ChatGPT für die Cybersicherheit	446
11.2 Böartige KI-Modelle	448
11.2.1 WormGPT und Evil-GPT	449
11.2.2 FraudGPT	452
11.2.3 XXXGPT und Wolf GPT	453
11.2.4 Wie schützt man sich vor schadhaften Sprachmodellen?	453
11.3 Werden Ethical Hacker bzw. Pentester arbeitslos?	454
12 Lösungen der Übungsaufgaben	457