S E M I N A R E

Microsoft

2252

Ethical Hacking mit ChatGPT für Windows-Systeme (MS IT Boot-Camp)

Tauchen Sie in die Welt des Ethical Hackings ein – mit Unterstützung moderner KI-Technologien!

o Zielgruppe
IT-Sicherheitsexperten, Penetrationstester und Interessierte mit grundlegenden Netzwerk- und Windows-Kenntnissen, die ihre Fähigkeiten im Ethical Hacking und der Nutzung von KI-Tools erweitern möchten.

o Voraussetzungen
Laptop mit VirtualBox/VMware und Kali Linux
Grundkenntnisse in Netzwerken und Windows-Systemen
OpenAI-Account für ChatGPT erwünscht / API-Key wird während des Seminars gestellt

o Seminarziel
Erlernen Sie die Kunst des Ethical Hackings – von Netzwerksicherheit über Malware-Analyse bis hin zum Einsatz moderner KI-Tools wie ChatGPT und ShellGPT. In diesem intensiven 3-Tage-Seminar kombinieren Sie theoretische Grundlagen mit praxisnahen Übungen in einer geschützten Umgebung.

o Seminarinhalt
1: Einführung in Ethical Hacking, ChatGPT und ShellGPT
- Grundlagen des Ethical Hackings und rechtliche Aspekte
- Einrichtung von Angreifersystemen (Kali Linux) und Zielsystemen
- Einsatz von ChatGPT und ShellGPT für Automatisierung und Skripterstellung

Praxis: Installation von ShellGPT und erste Tests

2: Reconnaissance, Schwachstellensuche und Google Dorks
- Netzwerkscans mit Nmap und OSINT-Tools wie Shodan
- Schwachstellensuche mit Google-Dorking
- Analyse von Schwachstellen mit ChatGPT

Praxis: Scannen von Zielsystemen und Schwachstellenanalyse

3: Exploits, SQLmap und Man-in-the-Middle
- SQL-Injection mit SQLmap auf OWASP Juice Shop
- ARP-Spoofing und DNS-Spoofing
- Email-Spoofing und Erkennung von Angriffen

Praxis: Durchführung eines ARP-Spoofing-Angriffs und Header-Analyse gefälschter Emails

4: Malware-Analyse, Tarnung und Trojaner
- Erstellung und Tarnung eines NetBus-Trojaners
- Statische und dynamische Malware-Analyse
- Gegenmaßnahmen und PowerShell-Skripte zur Malware-Erkennung

Praxis: Tarnung eines Trojaners und Verhaltenserkennung

5: WLAN-Hacking, Hak5-Tools und Abschluss
- Deauthentifizierungsangriffe und Passwort-Cracking
- Einführung in Hak5-Tools: WiFi Pineapple, Rubber Ducky, Bash Bunny
- Diskussion der Ergebnisse und Ausblick

Praxis: WPA2-Handshake-Capturing und Passwort-Cracking

Besondere Highlights
- Nutzung von ChatGPT und ShellGPT zur Skripterstellung und Analyse
- Hands-on-Übungen in einer isolierten Umgebung
- Umfassende Unterlagen: Tools, Prompts und Anleitungen

CONSULTING & INFORMATIONSDIENSTE GMBH

München
Berghamer Straße 10
85435 Erding
Tel.: 0 81 22 / 97 40 - 0
Fax: 0 81 22 / 97 40 - 10

Erfurt
Michaelisstraße 13a
99084 Erfurt
Tel.: 03 61 / 5 65 93 - 0
Fax: 03 61 / 5 65 93 - 10

Internet
www.md-consulting.de

E-Mail
info@md-consulting.de

Bankverbindung
HypoVereinsbank
Erfurt

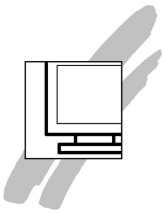
IBAN:
DE84 8202 0086
0003 9840 95

SWIFT/BIC:
HYVEDEMM 498

Geschäftsführer
Dr. Martin Diestelmann

HRB München 289362

USt.Id Nr.:
DE 150 108 446



Microsoft

2252

Tools:

- Netzwerksicherheit: Nmap, Nessus, OpenVAS
- Exploitation: Metasploit, SQLmap, WiFi Pineapple
- Malware-Analyse: Cuckoo Sandbox, Process Monitor

o Seminardauer: 3 Tage

Im Schulungspreis enthalten sind Handouts: Einführung in Ethical Hacking, WLAN-Angriffe, Malware-Analyse.
Prompts für ChatGPT und ShellGP

Lernen im Schulungshotel Gröbern am See in Muldestausee/Gröbern, in der Dübener Heide:
Seminardauer: Erster Tag ab 10:00 Uhr, letzter Tag ca. 15:00 Uhr
Kleine Gruppen mit 2-4 Teilnehmern (max. 6)
Im Preis enthalten sind:
- Übernachtungskosten im Hotel
- Vollverpflegung inkl. Getränke
- Schulungsunterlagen
- Täglich open end
- Intensive Übungs- und Nachbereitungsphasen nach Seminarende

o Preis pro Person: 1.990 EUR netto