CONSULTING & INFORMATIONSDIENSTE GMBH

Microsoft

2239

Ethical Hacking von Windows-Systemen mit Kali Linux, ChatGPT und Hacking-Hardware (MS IT Boot-Camp)

o Zielgruppe

Dieser strukturierte 5-Tage-Kurs bietet eine intensive Einführung in Ethical Hacking von Windows-Systemen mit Kali Linux. Die Teilnehmer lernen, wie sie theoretisches Wissen praktisch anwenden können und erhalten durch die Integration von ChatGPT Unterstützung bei der Durchführung und Optimierung von Hacking-Aufgaben.

o Voraussetzungen

Grundlegende Kenntnisse in der Datenbanktheorie
Grundkenntnisse in der Programmierung (jede Sprache)
Grundkenntnisse in SQL erforderlich, keine Vorkenntnisse in SQL-Server erforderlich

o Seminarziel

Dieser strukturierte 5-Tage-Kurs bietet eine intensive Einführung in Ethical Hacking von Windows-Systemen mit Kali Linux. Die Teilnehmer lernen, wie sie theoretisches Wissen praktisch anwenden können und erhalten durch die Integration von ChatGPT Unterstützung bei der Durchführung und Optimierung von Hacking-Aufgaben.

o Seminarinhalt

Tag 1: Grundlagen und Vorbereitung

Vormittag:

- **Einführung in Ethical Hacking**
  - **Definition und Bedeutung**: Überblick über Ethical Hacking und dessen Rolle im Bereich der Cybersicherheit
  - **Rechtliche und ethische Aspekte**: Gesetze, Vorschriften und ethische Grundsätze
  - **Rollen und Verantwortlichkeiten**: Unterschiedliche Rollen von Hackern (Black Hat, White Hat, Grey Hat)
- **Überblick über Kali Linux**
  - **Installation und Konfiguration**: Schritt-für-Schritt-Installation auf VirtualBox oder VMware
  - **Grundlegende Befehle und Werkzeuge**: Einführung in die Benutzeroberfläche und die wichtigsten Werkzeuge

Nachmittag:

- **Einführung in ChatGPT**
  - **Nutzen von ChatGPT**: Wie kann ChatGPT bei Hacking-Aufgaben helfen?
  - **Erste Schritte**: Anfragen stellen und Antworten erhalten
  - **Beispiele**: Beispiele für die Nutzung von ChatGPT in Ethical Hacking-Szenarien
- **Projektstart: Vorbereitung der Testumgebung**
  - **Installation von Kali Linux**: Einrichtung der Testumgebung
  - **Erste Schritte mit Kali Linux**: Nutzung von grundlegenden Werkzeugen
  - **Nutzung von ChatGPT**: Unterstützung bei der Einrichtung und den ersten Schritten

Tag 2: Netzwerksicherheit und Reconnaissance

Vormittag:

- **Informationsbeschaffung (Reconnaissance)**
  - **Passives und aktives Reconnaissance**: Tools und Techniken zur Informationsbeschaffung (whois, nslookup, theHarvester)
  - **Netzwerkscanning**: Verwendung von Nmap und weiteren Scanning-Tools
  - **Vulnerability Scanning**: Nutzung von OpenVAS und Nessus

Microsoft

2239

Nachmittag:

- **ARP-Spoofing und Man-in-the-Middle (MITM) Angriffe**
  - **Grundlagen von ARP-Spoofing**: Einführung und Demonstration
  - **MITM-Angriffe mit Ettercap und Wireshark**: Durchführung und Analyse
  - **Nutzung von ChatGPT**: Unterstützung bei der Durchführung und Optimierung der Angriffe
- **Projektarbeit: Scanning und Reconnaissance**
  - **Durchführung von Netzwerkscans und Schwachstellenscans**: Nutzung von Nmap, OpenVAS und Nessus
  - **Nutzung von ChatGPT zur Unterstützung**: Optimierung und Problemlösung

Tag 3: Webanwendungen und Exploitation

Vormittag:

- **Angriffe auf Webanwendungen**
  - **SQL Injections**: Einführung, Techniken und Tools (sqlmap)
  - **Cross-Site Scripting (XSS)**: Einführung und Demonstration
  - **File Inclusion Vulnerabilities**: Einführung und Demonstration

Nachmittag:

- **Exploitation von Windows-Systemen**
  - **Einführung in Metasploit Framework**: Nutzung und Anwendung
  - **Durchführung von Exploits**: Praktische Anwendung von Exploits gegen Windows-Systeme
- **Projektarbeit: Webanwendungen und Exploitation**
  - **Durchführung von SQL Injections und XSS-Angriffen**: Nutzung von Tools wie sqlmap und Burp Suite
  - **Nutzung von ChatGPT**: Unterstützung bei der Auswahl und Durchführung von Exploits

Tag 4: Hacking-Hardware und fortgeschrittene Angriffe

Vormittag:

- **Hacking-Hardware**
  - **Einführung in DigiSpark**: Nutzung und Anwendung
  - **Übersicht der wichtigsten Tools von Hak5**: USB Rubber Ducky, WiFi Pineapple, LAN Turtle
  - **Demonstration und Einsatz der Tools**: Praktische Anwendungen
- **WLAN-Hacking**
  - **Grundlagen und Techniken**: Einführung in WPA/WPA2-Angriffe
  - **Tools und Techniken**: Aircrack-ng, Reaver

Nachmittag:

- **Pass-the-Hash Angriffe**
  - **Einführung und Grundlagen**: Funktionsweise und Anwendung
  - **Tools und Techniken**: Mimikatz, Impacket
- **Projektarbeit: Hacking-Hardware und WLAN**
  - **Anwendung von Hacking-Hardware**: Durchführung von Angriffen mit Hak5-Tools
  - **Durchführung von WLAN-Angriffen**: Nutzung von Aircrack-ng und Reaver
  - **Nutzung von ChatGPT**: Unterstützung bei der Durchführung und Optimierung der Angriffe

Microsoft

2239

Tag 5: Passwort-Cracking und Abschlussprojekt

Vormittag:

- **Passwort-Cracking**
  - **Einführung in Passwort-Cracking**: Techniken und Tools
  - **Brute-Force und Dictionary-Angriffe**: Verwendung von Tools wie John the Ripper, Hashcat
- **Email Spoofing**
  - **Grundlagen und Techniken**: Einführung und Demonstration
  - **Tools und Techniken**: Verwendung von SET (Social Engineering Toolkit)

Nachmittag:

- **Abschlussprojekt**
  - **Durchführung eines vollständigen Penetrationstests**: Planung und Durchführung eines Tests gegen ein Windows-System
  - **Dokumentation und Präsentation der Ergebnisse**: Erstellung eines Berichts und Präsentation
- **Review und Abschlussdiskussion**
  - **Präsentation der Projektergebnisse**: Diskussion und Feedback
  - **Zertifikatverleihung**: Zusammenfassung der Seminarinhalte und Verleihung der Teilnahmezertifikate

Methodik und Ressourcen

Methodik

- **Vorträge und Präsentationen:** Vermittlung der theoretischen Grundlagen
- **Hands-on-Übungen:** Praktische Übungen zur Anwendung des Gelernten
- **Diskussionen und Q&A-Sessions:** Interaktive Diskussionen zur Vertiefung des Verständnisses
- **Projektsession:** Eigenständige Projektentwicklung mit individueller Betreuung
- **Integration von ChatGPT:** Unterstützung bei Fragen und Codegenerierung

Ressourcen

- **Kali Linux:** Betriebssystem für Penetrationstests und Ethical Hacking
- **Metasploit Framework:** Werkzeug zur Durchführung von Exploits
- **Hacking-Hardware von Hak5:** USB Rubber Ducky, WiFi Pineapple, LAN Turtle
- **DigiSpark:** Mikrocontroller für Hacking-Szenarien
- **Aircrack-ng und Reaver:** Tools für WLAN-Hacking
- **John the Ripper und Hashcat:** Tools für Passwort-Cracking
- **SET (Social Engineering Toolkit):** Tool für Social Engineering und Email Spoofing
- **ChatGPT-Zugang:** Nutzung zur Unterstützung und Vertiefung des Gelernten

o Seminardauer: 5 Tage

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 Teilnehmer (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: 3.290 EUR netto