# *SC425 EC-Council Certified Penetration Testing Professional (CPENT AI)*

**Kurzbeschreibung:**

Der Kurs **SC425 CPENT$^{AI}$ Certified Penetration Testing Professional** von EC-Council ist eines der weltweit umfassendsten praxisorientierten Penetrationstesting-Kurse. Es bietet eine vollständige Methodologie zur Durchführung von Sicherheitsprüfungen und kombiniert fortgeschrittene Penetrationstesting-Techniken mit der Nutzung Künstlicher Intelligenz (KI). Die Teilnehmer lernen, wie sie mit innovativen KI-Tools Prozesse automatisieren, reale Cyberbedrohungen simulieren und Sicherheitslücken identifizieren können.

Der Workshop ist speziell darauf ausgelegt, Fähigkeiten zu vermitteln, die weit über grundlegendes Penetrationstesting hinausgehen. Dazu gehören die Durchführung von Tests in heterogenen Netzwerkarchitekturen, IoT-Systemen, Cloud-Umgebungen und sogar kritischen OT und SCADA-Infrastrukturen. Die Teilnehmer lernen auch, Sicherheitsberichte zu erstellen, die für Stakeholder umsetzbar und präzise sind.

Durch praktische Übungen in über 110 Laborumgebungen, Live-Cyber-Ranges und CTF-Herausforderungen (Capture the Flag) bereitet der **CPENT$^{AI}$** die Teilnehmer auf reale Sicherheitstests vor und verleiht ihnen die Fähigkeit, als vielseitige Offensive-Security-Experten zu agieren.

**Zielgruppe:**

Der Kurs **SC425 CPENT$^{AI}$ Certified Penetration Testing Professional** richtet sich an:

IT-Sicherheitsprofis, Penetrationstester, Ethical Hacker und Cybersecurity-Spezialisten, die ihre Fähigkeiten in der Analyse, Bewertung und Absicherung komplexer Netzwerke erweitern möchten. Er ist ideal für Experten, die eine Karriere im Bereich Offensive Security und Vulnerability Assessment and Penetration Testing (VAPT) anstreben.

**Voraussetzungen:**

Um den Inhalten und dem Lerntempo des Kurses **SC425 CPENT$^{AI}$ Certified Penetration Testing Professional** gut folgen zu können, halten wir folgende Vorkenntnisse für notwendig:

- Aufgrund der umfangreichen und anspruchsvollen Kursinhalte wird die vorherige Teilnahme am Kurs **SC415 EC-Council Certified Ethical Hacker - CEH Elite v13** oder eine gleichwertige Qualifikation bzw. entsprechende Praxiserfahrung dringend empfohlen.
- Mindestens zwei Jahre Erfahrung im Bereich der Informationssicherheit.
- Tiefgehendes Verständnis von Netzwerksicherheitskonzepten wie Firewalls, VPNs, IDS/IPS-Systemen und VLANs.
- Praxiserfahrung mit Pentesting-Tools wie Metasploit, Nmap, Burp Suite und Wireshark.
- Grundkenntnisse in Programmiersprachen wie Python, Perl, PowerShell, Ruby, Metasploit und JavaScript für die Anpassung von Exploits und Skripten.
- Verständnis von Angriffsmethoden wie Buffer Overflow, SQL Injection und XSS.

Um den vollen Lerneffekt aus der Kurswoche zu ziehen, wird eine etwa zweiwöchige Befassung mit den Kursinhalten vor Kursbeginn dringend angeraten. Ebenso empfehlen wir eine intensive Nachbereitung der Kurswoche und ausführliche Übungen, bevor der Prüfungstermin angesetzt wird.

**Sonstiges:**

**Dauer:** 5 Tage

**Preis:** 3950 Euro plus Mwst.

**Ziele:**

Der Kurs **SC425 CPENT$^{AI}$ Certified Penetration Testing Professional** hat das Ziel, den Teilnehmern fortgeschrittene Penetrationstesting-Techniken wie Double Pivoting, Binary Exploitation und IoT-Pentestmethodiken zu vermitteln. Darüber hinaus werden praktische Übungen durch Cyber-Range-Simulationen, Capture-the-Flag-Challenges (CTFs) und mehr als 110 Labore angeboten, um die Fähigkeiten der Teilnehmer in realitätsnahen Szenarien zu schärfen. Ein weiteres Ziel des Kurses ist die Entwicklung maßgeschneiderter Exploits und die Automatisierung von Sicherheitsanalysen unter Einsatz von künstlicher Intelligenz (KI).

Die Teilnehmer lernen, Penetrationstests an hybriden Netzwerken, SCADA/ICS-Systemen und Cloud-Umgebungen durchzuführen und professionelle Sicherheitsberichte mit konkreten Handlungsempfehlungen für Unternehmensleitungen zu erstellen. **CPENT$^{AI}$** legt besonderen Wert auf die Kombination von theoretischem Wissen und praxisorientierten Fähigkeiten, um umfassend auf reale Sicherheitsprüfungen vorzubereiten.

**Inhalte/Agenda:**

- ♦ **Module 01: Introduction to Penetration Testing and Methodologies**
- ♦ ◊ Principles and Objectives of Penetration Testing
  ◊ Penetration Testing Methodologies and Frameworks
  ◊ Best Practices and Guidelines for Penetration Testing
  ◊ Role of Artificial Intelligence in Penetration Testing
  ◊ Role of Penetration Testing in Compliance with Laws, Acts, and Standards
- ♦ ◊
- ♦ **Module 02: Penetration Testing Scoping and Engagement**
- ♦ ◊ Penetration Testing: Pre-engagement Activities
  ◊ Key Elements Required to Respond to Penetration Testing RFPs
  ◊ Drafting Effective Rules of Engagement (ROE)
  ◊ Legal and Regulatory Considerations Critical to Penetration Testing
  ◊ Resources and Tools for Successful Penetration Testing
  ◊ Strategies to Effectively Manage Scope Creep
- ♦ ◊
- ♦ **Module 03: Open-Source Intelligence (OSINT) and Attack Surface Mapping**
- ♦ ◊ Collect Open-Source Intelligence (OSINT) on Target's Domain Name
  ◊ Collect OSINT About Target Organization on the Web
  ◊ Perform OSINT on Target's Employees
  ◊ OSINT Using Automation Tools
  ◊ Map the Attack Surface
- ♦ ◊
- ♦ **Module 04: Social Engineering Penetration Testing**
- ♦ ◊ Social Engineering Penetration Testing Concepts
  ◊ Off-Site Social Engineering Penetration Testing
  ◊ On-Site Social Engineering Penetration Testing
  ◊ Document Findings with Countermeasure Recommendations
- ♦ ◊
- ♦ **Module 05: Web Application Penetration Testing**
- ♦ ◊ Web Application Footprinting and Enumeration Techniques
  ◊ Techniques for Web Vulnerability Scanning
  ◊ Test for Vulnerabilities in Application Deployment and Configuration
  ◊ Techniques to Assess Identity Management, Authentication, and Authorization Mechanisms
  ◊ Evaluate Session Management Security
  ◊ Evaluate Input Validation Mechanisms
  ◊ Detect and Exploit SQL Injection Vulnerabilities
  ◊ Techniques for Identifying and Testing Injection Vulnerabilities
  ◊ Exploit Improper Error Handling Vulnerabilities
  ◊ Identify Weak Cryptography Vulnerabilities
  ◊ Test for Business Logic Flaws in Web Applications
  ◊ Evaluate Applications for Client-Side Vulnerabilities
- ♦ ◊
- ♦ **Module 06: API and Java Web Token Penetration Testing**
- ♦ ◊ Techniques and Tools to Perform API Reconnaissance
  ◊ Test APIs for Authentication and Authorization Vulnerabilities
  ◊ Evaluate the Security of JSON Web Tokens (JWT)
  ◊ Test APIs for Input Validation and Injection Vulnerabilities
  ◊ Test APIs for Security Misconfiguration Vulnerabilities
  ◊ Test APIs for Rate Limiting and Denial of Service (DoS) Attacks
  ◊ Test APIs for Security of GraphQL Implementations
  ◊ Test APIs for Business Logic Flaws and Session Management
- ♦ ◊

- ♦ **Module 07: Perimeter Defense Evasion Techniques**
- ♦ ◊ Techniques to Evaluate Firewall Security Implementations
  ◊ Techniques to Evaluate IDS Security Implementations
  ◊ Techniques to Evaluate the Security of Routers
  ◊ Techniques to Evaluate the Security of Switches
- ♦ ◊
- ♦ **Module 08: Windows Exploitation and Privilege Escalation**
- ♦ ◊ Windows Pen Testing Methodology
  ◊ Techniques to Perform Reconnaissance on a Windows Target
  ◊

- ◊ Techniques to Perform Vulnerability Assessment and Exploit Verification
- ◊ Methods to Gain Initial Access to Windows Systems
- ◊ Techniques to Perform Enumeration with User Privilege
- ◊ Techniques to Perform Privilege Escalation
- ◊ Post-Exploitation Activities
- ◊ Exploit Windows OS Vulnerability
- ◊ Exploit and Escalate Privileges on a Windows Operating System
- ◊ Gain Access to a Remote System
- ◊ Exploit Buffer Overflow Vulnerability on a Windows Machine
- ◊

**Module 09: Active Directory Penetration Testing**

- ◊ Architecture and Components of Active Directory
- ◊ Active Directory Reconnaissance
- ◊ Active Directory Enumeration
- ◊ Exploit Identified Active Directory Vulnerabilities
- ◊ Role of Artificial Intelligence in AD Penetration Testing Strategies
- ◊

**Module 10: Linux Exploitation and Privilege Escalation**

- ◊ Linux Exploitation and Penetration Testing Methodologies
- ◊ Linux Reconnaissance and Vulnerability Scanning
- ◊ Techniques to Gain Initial Access to Linux Systems
- ◊ Linux Privilege Escalation Techniques
- ◊

**Module 11: Reverse Engineering, Fuzzing, and Binary Exploitation**

- ◊ Concepts and Methodology for Analyzing Linux Binaries
- ◊ Methodologies for Examining Windows Binaries
- ◊ Buffer Overflow Attacks and Exploitation Methods
- ◊ Concepts, Methodologies, and Tools for Application Fuzzing
- ◊

**Module 12: Lateral Movement and Pivoting**

- ◊ Advanced Lateral Movement Techniques
- ◊ Advanced Pivoting and Tunneling Techniques to Maintain Access
- ◊

**Module 13: IoT Penetration Testing**

- ◊ Fundamental Concepts of IoT Pentesting
- ◊ Information Gathering and Attack Surface Mapping
- ◊ Analyze IoT Device Firmware
- ◊ In-depth Analysis of IoT Software
- ◊ Assess the Security of IoT Networks and Protocols
- ◊ Post-Exploitation Strategies and Persistence Techniques
- ◊ Comprehensive Pentesting Reports
- ◊

**Module 14: Report Writing and Post-Testing Actions**

- ◊ Purpose and Structure of a Penetration Testing Report
- ◊ Essential Components of a Penetration Testing Report
- ◊ Phases of a Pen Test Report Writing
- ◊ Skills to Deliver a Penetration Testing Report Effectively
- ◊ Post-Testing Actions for Organizations
- ◊