EC-Council Certified Penetration Testing Professional (CPENT) + Exam voucher

Duration: 5 Days **Course Code: CPENT** **Version: 2.0** **Delivery Method: Company Event**

Overview:

EC-Council's Certified Penetration Tester (CPENT) program is all about the pen test and will teach you to perform in an enterprise network environment that must be attacked, exploited, evaded, and defended. If you have only been working in flat networks, CPENT's live practice range will teach you to take your skills to the next level by teaching you to pen test IoT systems, OT systems, as well as how to write your own exploits, build your own tools, conduct advanced binaries exploitation, double pivot to access hidden networks, and customization of scripts and exploits to get into the innermost segments of the network.

The CPENT range consists of entire network segments that replicate an enterprise network — this is not a computer game simulation; this is an accurate representation of an enterprise network that will present the latest challenges to the pen tester. The benefit of hands on learning in a live cyber range is that candidates will encounter multiple layers of network segmentation, and the CPENT course will teach candidates how to navigate these layers, so that once access is gained in one segment, a candidate will know the latest pivoting techniques required to reach the next. However, that won't be enough on its own as the targets and segments are progressive in nature, so once you get into one machine and or segment, the next one will challenge you even more

CPENT is a fully online, remotely proctored practical exam that challenges candidates through a grueling 24-hour performance-based, hands-on exam. The exam is broken into 2 practical exams of 12-hours each that will test your perseverance and focus by forcing you to outdo yourself with each new challenge. Candidates have the option to choose either 2 12-hour exams or one 24-hour exam.
Candidates who score more than 70% will earn the CPENT certification. Candidates who score more than 90% attain the prestigious LPT (Master) credential!

Target Audience:

Ethical Hackers, Penetration Testers, Network Server Administrators, Firewall Administrators, Security Testers, System Administrators and Risk Assessment Professionals,

Objectives:

- **After completing this course you should have gained the following Advanced Pentesting skills:**
- Advanced Windows Attacks
- Attacking IoT Systems
- Advanced Binary Exploitation.
- Bypassing Filtered Networks
- Pentesting Operational Technology (OT)
- Access Hidden Networks with Pivoting
- Pivoting & Double Pivoting
- Privilege Escalation
- Evasion Techniques
- Attack Automation
- Weaponizing Exploits
- Professional Reporting

Prerequisites:

Attendees should meet the following prerequisites:

- It is recommended but not mandated that students have followed the EC-Council CEH Course and CEH Practical exam before enrolling for this course.
- Advanced knowledge in Networking Protocols
- Knowledge in Kali or ParrotOS and common Penetration Testing Tools
- Knowledge in Exploiting Windows and Linux Hosts

Testing and Certification

Recommended as preparation for the following exam:

- **CPENT - Certified Penetration Testing Professional**

Please note:

CPENT is a fully online, remotely proctored practical exam that challenges candidates through a grueling 24-hour performance-based, hands-on exam. The exam is broken into 2 practical exams of 12-hours each that will test your perseverance and focus by forcing

- Knowledge in Privilege Escalation in Linux and Windows
- Knowledge in Wireless Penetration Testing
- Knowledge in Web Application Penetration Testing
- CND - EC-Council Certified Network Defender (CND) + Exam voucher
- CEH - EC-Council Certified Ethical Hacker (CEH) + Exam voucher

you to outdo yourself with each new challenge. Candidates have the option to choose either 2 12-hour exams or one 24-hour exam.

Candidates who score more than 70% will earn the CPENT certification. Candidates who score more than 90% attain the prestigious LPT (Master) credential!

Content:

Introduction to Penetration Testing and Methodolgies

- 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

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

Open Source Intelligence (OSINT) and Attack Surface Mapping

- Collecting Open-source Intelligence (OSINT) on Target's Domain Name
- Collecting OSINT about Target Organization on the Web
- Open Source Intelligence (OSINT) using Automation Tools
- Attack Surface Mapping

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

Web Application Penetration Testing

- Security Frame vs. Vulnerabilities vs. Attacks
- OWASP Penetration Testing Framework
- 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

API and Java Web Token Penetration Testing

- API and Java Web Tokens (JWT) 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

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

Windows Exploitation and Privilege Escalation

- Windows Pen Testing Methodology
- 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

Active Directory Penetration Testing

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

Linux Exploitation and Privilege Escalation

- Linux Exploitation and Penetration Testing Methodologies
- Linux Reconnaissance and Vulnerability Scanning
- Techniques to Gain Initial Access to

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

Lateral Movement and Pivoting

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

IoT Penetration Testing

- Fundamental Concepts of IoT Pen Testing
- 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 Pen Testing Reports

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

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

Linux Systems
- Linux Privilege Escalation Techniques

Further Information:

For More information, or to book your course, please call us on 00 971 4 446 4987

training@globalknowledge.ae

www.globalknowledge.com/en-ae/

Global Knowledge, Dubai Knowledge Village, Block 2A,First Floor, Office F68, Dubai, UAE