Certified Penetration Testing Professional (C|PENT AI)

Duration 5 days

COURSE DESCRIPTION

EC-Council's Certified Penetration Tester (CPENT) program teaches you how to perform an effective penetration test 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 how to pen test IoT systems, OT systems, how to write your own exploits, build your own tools, conduct advanced binaries exploitation, double pivot to access hidden networks, and customize scripts/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.

COURSE OBJECTIVE

- Acquire a comprehensive knowledge of SOC processes, procedures, technologies, and workflows.
- Learn the fundamentals of penetration testing, including its objectives, methodologies, frameworks, and role in an organization's security strategy.
- Understand how to scope penetration testing engagements, define objectives, establish clear communication with stakeholders, and adhere to legal and ethical boundaries.
- Understand OSINT techniques to gather actionable intelligence and learn to identify, map, and analyze an organization's attack surface.
- Learn the art of exploiting human vulnerabilities through social engineering techniques, along with preventive measures to mitigate such risks.
- Cultivate techniques for testing web applications for vulnerabilities such as SQL injection, XSS, and authentication flaws, and learn methods to exploit and remediate these issues.
- Understand how to assess API security by testing endpoints, exploiting misconfigurations, and identifying weaknesses in JSON Web Tokens (JWT).
- Learn advanced techniques to bypass f irewalls, intrusion detection systems (IDS), routers, switches, and other perimeter defenses.
- Gain methods to exploit vulnerabilities in Windows systems and perform privilege escalation to gain higher-level access
- Discover how to test and exploit vulnerabilities in Active Directory environments by identifying misconfigurations and security weaknesses.
- Acquire techniques for exploiting Linux systems and escalating privileges, as well as understanding common vulnerabilities and configurations.
- Learn reverse engineering, fuzzing techniques, and binary exploitation to identify and exploit weaknesses in software and applications.

- Obtain techniques to navigate through internal networks, gain access to additional systems, and pivot to critical assets during penetration testing.
- Develop techniques to find and exploit vulnerabilities in IoT devices and ecosystems.
- Learn how to create professional penetration testing reports, communicate findings effectively, and outline actionable post-testing recommendations.

COURSE OUTLINE

Module 1: 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 2: 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 3: 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

Labs:

- Collect OSINT on Target's Domain Name, Web, and Employees
- Collect OSINT Using Automation Tools
- Identify and Map Attack Surface

Module 4: 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

Labs:

- Sniff credentials using the Social-Engineer Toolkit (SET)

Module 5: Web Application Penetration Testing

- Web Application Foot printing 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

Labs:

- Perform Website Foot printing
- Perform Web Vulnerability Scanning Using Al
- Perform Various Attacks on Target Web Application

Module 6: 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 Vulnerabities
- 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

Labs:

- Perform API Reconnaissance Using Al
- Scan and Identify Vulnerabilities in APIs
- Exploit Various Vulnerabilies to Gather Information on the Target Application

Module 7: 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

Labs:

- Identify and Bypass a Firewall
- Evade Perimeter Defenses Using Social-Engineer Toolkit (SET)
- Perform WAF Fingerprinting

Module 8: 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

Labs:

- 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 9: 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

Labs:

- Explore the Active Directory Environment
- Perform Active Directory Enumeration
- Perform Horizontal Privilege Escalation and Lateral Movement
- Retrieve Cached Active Directory Credentials

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

Labs:

- Perform Reconnaissance and Vulnerability Assessment on Linux
- Gain Access and Perform Enumeration
- Identify Misconfigurations for Privilege Escalation

Module 11: Reverse Engineering, Fuzzing, and Binary Exploitation

- Concepts and Methodolology for Analyzing Linux Binaries
- Methodologies for Examining Windows Binaries
- Buffer Overtlow Attacks and Exploitation Methods
- Concepts, Methodologies, and Tools for Application Fuzzing

Labs:

- Perform Binary Analysis
- Explore Binary Analysis Methodology
- Write an Exploit Code
- Reverse Engineering a Binary
- Identify and Debug Stack Buffer Overflows
- Fuzzing an Application

Module 12: Lateral Movement and Pivoting

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

Labs:

- Perform Pivoting
- Perform DNS Tunneling and HTTP Tunneling

Module 13: IoT Penetration Testing

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

Labs:

- Perform loT Fireware Acquisition, Extraction, Analysis, and Emulation
- Probe IoT Devices

Module 14: Report Writing and Post-Testing Actions

- Purpose and Structure of a Penetration Testing Report

NETWORK TRAINING CENTER CO.,LTD. (NTC) | www.trainingcenter.co.th

Call us today 0-2634-7993-4

177/1 BUI Bldg., 14th Fl., Unit 1, 3 & 4, Surawongse Rd., Suriyawongse, Bangrak, Bangkok, THAILAND | Email: sales@trainingcenter.co.th

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

Labs:

- Generate Penetration Test Reports

WHO SHOULD ATTEND

Penetration Testers, Ethical Hackers, Information Security Consultant, Security Testers, Security Analysts, Security Engineers, Network Service Administrators, Firewall Administrators, System Administrators, Risk Assessment Professionals

EXAM INFORMATION

The CPENT exam is a 100% practical exam and includes a penetration testing report submission.
Exam features:

- Choose your challenge: Either two sessions of 12 hours each or a single 24-hour exam
- Pen Test Report Submission (Within seven days of final session)
- Proctored exam
- Score at least 70% to earn the CPENT certification
- Score more than 90% and earn the highly regarded Licensed Penetration Testing (LPT) certification

NETWORK TRAINING CENTER CO.,LTD. (NTC) | www.trainingcenter.co.th
Call us today 0-2634-7993-4
177/1 BUI Bldg., 14th Fl., Unit 1, 3 & 4, Surawongse Rd., Suriyawongse, Bangrak, Bangkok, THAILAND | Email: sales@trainingcenter.co.th