Certified Penetration Testing Professional Program

Course Duration: 40 Hrs. **Course code: CPENT 10**

Course Overview

A rigorous Penetration Testing program that, unlike contemporary Penetration Testing courses, teaches you how to perform an effective Penetration test across filtered networks.

C|PENT is a multidisciplinary course with extensive hands-on training in a wide range of crucial skills, including advanced Windows attacks, Internet of Things (IoT) and Operational Technology (OT) systems, filtered network bypass techniques, exploit writing, single and double pivoting, advanced privilege escalation, and binary exploitation.

What you'll learn?

- ❖ Advanced Windows Attacks: Learn to exploit vulnerabilities in Windows environments.
- ❖ Penetration Testing IoT and OT Systems: Gain expertise in testing Internet of Things (IoT) and Operational Technology (OT) systems.
- ❖ Exploit Writing and Binary Exploitation: Develop the ability to write your own exploits and conduct advanced binary exploitation.
- ❖ Bypassing Network Filters: Learn techniques to bypass firewalls and other security mechanisms to access hidden networks.
- ❖ Pivoting and Double Pivoting: Master the art of pivoting to access hidden networks and segments, including double pivoting.
- ❖ Privilege Escalation: Learn how to escalate privileges to gain higher access levels within a system.
- ❖ Evading Security Mechanisms: Understand and learn how to evade security mechanisms like firewalls and intrusion detection systems.

Target Audience

- Security Testers.
- Security Analysts.
- Security Engineers.
- Network Server Administrators.

Pre-Requisites

- EC-Council, the organization offering CPENT, does not require any specific certifications or training to take the CPENT exam.
- EC-Council strongly recommends candidates have at least a couple of years of experience in IT and cybersecurity.
- They suggest completing the CEH (Practical) or ECSA (Practical) before attempting the CPENT challenge.

Course content

Module 01 - Introduction to Penetration Testing and Methodologies

Cover the fundamentals of penetration testing, including penetration testing approaches, strategies, methodologies, techniques, and various guidelines and recommendations for penetration testing.

Module 02 - Penetration Testing Scoping and Engagement

Learn the different stages and elements of scoping and engagement in penetration testing.

Module 03 - Open-Source Intelligence (OSINT)

Learn how to use techniques and tools to gather intelligence about the target from publicly available sources such as the World Wide Web (WWW), through website analysis, by using tools/frameworks/scripts, and so on.

Module 04 - Social Engineering Penetration Testing

Learn different social engineering techniques and perform social engineering penetration testing on a target organization.

Module 05 - Network Penetration Testing – External

Learn how to implement a comprehensive penetration testing methodology for assessing networks from outsiders' perspectives.

Module 06 - Network Penetration Testing – Internal

Learn how to implement a comprehensive penetration testing methodology for assessing networks from insider's perspectives.

Module 07 - Network Penetration Testing - Perimeter Devices

Learn how to implement a comprehensive penetration testing methodology for assessing the security of network perimeter devices, such as Firewalls, IDS, Routers, and Switches.

Module 08 - Web Application Penetration Testing

Learn how to analyze web applications for various vulnerabilities, including the Open Web Application Security Project (OWASP) Top 10, and determine the risk of exploitation.

Module 09 - Wireless Penetration Testing

Learn how to test various components of wireless networks, such as WLAN, RFID devices, and NFC technology devices.

Module 10 - IoT Penetration Testing

Understand various threats to Internet of things (IoT) networks and learn how to audit security controls for various inherent IoT risks.

Module 11 - OT and SCADA Penetration Testing

Understand OT and SCADA concepts and learn the process of testing various components of OT and SCADA networks.

Module 12 - Cloud Penetration Testing
Understand various security threats and concerns in cloud computing and learn how to perform cloud penetration testing to determine the probability of exploitation.

Module 13 - Binary Analysis and Exploitation
Understand the binary analysis methodology and reverse engineer applications to identify vulnerable applications that may lead to the exploitation of an information system.

Module 14 - Report Writing and Post Testing Actions
Learn how to document and analyze the results of a penetration test and recommend post-penetration test actions.

Exam preference

Length Of Test	24 Hours You can choose to take two 12-hour exams or one 24-hour exam.
Exam Type	100% practical, hands-on, remotely proctored.
Passing Score	Min. 70%