

## CPENT:

# EC-Council Certified Penetration Testing Professional

### Overview

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 also customize scripts/exploits to get into the innermost segments of the network.

- The course is presented through an enterprise network environment that must be attached, exploited, evaded, and defended
- EC-Council's CPENT gives the industry an ability to assess a Pen Tester's skills across a broad spectrum of "network zones"
- What makes the CPENT different is the requirement to be provided a variety of different scoped of ework so that the candidate can "think on their feet"
- The result of this is that there are different zones representing different types of testing
- Anyone attempting the test will have to perfume their assessment against these different zones

### Duration

5 Days

### Who Should Attend

- Ethical Hackers
- Penetration Testers
- Information Security Consultant
- Security Analyst
- Security Engineer
- Network server administrators
- Firewall Administrators
- Security Testers
- System Administrators and Risk Assessment professionals

## CPENT:

# EC-Council Certified Penetration Testing Professional

---

### Prerequisites

There is no defined pre-requisite for the exam, but it is strongly recommend that candidates to attempt the CEH (Practical) and/ or ECSA (Practical) prior to attempting CPENT.

Extensive knowledge of penetration testing across multiple disciplines extending from windows, IoTs, inline defenses to automation, operational technology, and advanced skills in binary exploitation. The certification tests the knowledge of tester not only on automated tools but manual testing skills as well.

# CPENT: EC-Council Certified Penetration Testing Professional

## Course Topics

|           |                                                 |
|-----------|-------------------------------------------------|
| Module 1  | Introduction to Penetration Testing             |
| Module 2  | Penetration Testing Scoping and Engagement      |
| Module 3  | Open Source Intelligence (OSINT)                |
| Module 4  | Social Engineering Penetration Testing          |
| Module 5  | Network Penetration Testing – External          |
| Module 6  | Network Penetration Testing– Internal           |
| Module 7  | Network Penetration Testing – Perimeter Devices |
| Module 8  | Web Application Penetration Testing             |
| Module 9  | Wireless Penetration Testing                    |
| Module 10 | IoT Penetration Testing                         |
| Module 11 | OT/SCADA Penetration Testing                    |
| Module 12 | Cloud Penetration Testing                       |
| Module 13 | Binary Analysis and Exploitation                |
| Module 14 | Report Writing and Post Testing Actions         |