Document Generated: 12/18/2025

Learning Style: Virtual Classroom

Technology: EC-Council

Difficulty: Intermediate

Course Duration: 5 Days

Certified Penetration Testing Professional V2 Instructor Led Training

What's Included:

- *Official EC Council Invitation to the virtual class*

- *Official EC Council Print or e-courseware included*

- *Official EC Council ilabs subscription*

- *EC Council Exam Voucher included*

About this course:

The Certified Penetration Testing Professional (CPENT) course is a rigorous and multidisciplinary program that provides hands-on training in a wide range of crucial skills for effective penetration testing. Unlike traditional courses, CPENT focuses on performing penetration tests across filtered networks, covering advanced Windows attacks, Internet of Things (IoT) and Operational Technology (OT) systems, filtered network bypass techniques, exploit writing, privilege escalation, and binary exploitation. The course is designed to bridge the gaps in skills that many penetration testing professionals have across multiple disciplines, enabling them to perform well even in complex network environments.

The C|PENT course aims to train professionals to become highly skilled penetration testers capable of tackling complex and varied targets, providing real-world experience and challenges to enhance their penetration testing abilities.

Course Objectives:

- Advanced Windows Attacks
- Attacking IoT Systems
- Writing Exploits: Advanced Binaries Exploitation
- Bypassing A Filtered Network
- Pentesting Operational Technology (OT)
- Access Hidden Networks with Pivoting
- Double Pivoting
- Privilege Escalation
- Evading Defense Mechanisms
- Attack Automation with Scripts
- Build Your Armory: Weaponize Your Exploits
- Write Professional Reports

Audience:

- Ethical Hackers / Penetration Testers / Security Testers
- Network Server Administrators / Firewall Administrators / System Administrators
- Risk Assessment Professionals / Information Security Consultants
- Cybersecurity Forensic Analysts / Cyberthreat Analysts
- Cloud Security Analysts / Application Security Analysts
- Cybersecurity Assurance Engineers / Information Security Engineers
- Security Operations Center (SOC) Analysts / Network Security Engineers
- Network Security Penetration Testers / Network Security Architects

Prerequisites:

There are no specific prerequisites for the CPENT exam, but this is not an entry-level certification. We recommend that candidates for this training and certification have at least a couple of years experience in IT and cybersecurity, and have CEH certification or equivalent.

Course Outline:

- Introduction to Penetration Testing and Methodologies
- Penetration Testing Scoping and Engagement
- Open-Source Intelligence (OSINT) and Attack
- Surface Mapping
- Social Engineering Penetration Testing
- Web Application Penetration Testing
- API and Java Web Token Penetration Testing
- Perimeter Defense Evasion Techniques
- Windows Exploitation and Privilege Escalation
- Active Directory Penetration Testing
- Linux Exploitation and Privilege Escalation
- Reverse Engineering, Fuzzing, and Binary Exploitation
- Lateral Movement and Pivoting
- IoT Penetration Testing
- Report Writing and Post-Testing Actions