Certified Penetration Testing Professional

Course Duration: 5 Days
Course ID: ECCOUNCIL_CPENT
Exam Reference: 412-80

Course Overview

The Certified Penetration Testing Professional (CPENT) course by EC-Council is a hands-on, performance-based certification program that trains cybersecurity professionals to assess and exploit complex enterprise networks. CPENT goes beyond traditional penetration testing by immersing candidates in a real-world, live, and dynamic cyber range, simulating multi-layered networks and advanced security architectures.

Unlike other pen testing certifications that focus on individual skills, CPENT challenges learners with scenarios that require full-spectrum offensive operations — from initial reconnaissance to exploitation, privilege escalation, lateral movement, and pivoting across segmented networks, cloud environments, and industrial control systems (ICS/SCADA).

The course also includes modern coverage of cloud penetration testing, IoT exploitation, binary exploitation, OT/ICS hacking, and custom exploit development, ensuring candidates are prepared for today's evolving threat landscape.

Prerequisites

1. Knowledge of Networking and Security Concepts
    - Strong grasp of TCP/IP, network protocols, and security technologies (firewalls, IDS/IPS, VPNs).
    - Familiarity with enterprise network architecture.

APPLIED TECHNOLOGY ACADEMY

Contact Us

800.674.3550

2151 W. Hillsboro Blvd., Ste 210
Deerfield Beach, FL 33442

Connect With Us

2. Experience with Penetration Testing Tools
    - Hands-on experience using tools like Nmap, Metasploit, Burp Suite, Wireshark, etc.
    - Understanding of common attack vectors and payloads.
3. Operating System Proficiency
    - Comfort with both Linux and Windows environments.
    - Skills in command-line usage, scripting, and system administration.
4. Programming/Scripting Skills (Basic)
    - Working knowledge of scripting languages like Python, Bash, or PowerShell is helpful.
    - Understanding exploit code and writing/modifying simple scripts.
5. Prior Certification or Experience (Strongly Recommended)
    - EC-Council's CEH (Certified Ethical Hacker) certification or equivalent.
    - At least 2–3 years of hands-on information security experience (pen testing, red teaming, ethical hacking).

Course Outline

Module 01: Introduction to Penetration Testing

- Penetration Testing Scoping and Engagement
- Rules of Engagement and Legal Considerations
- Penetration Testing Standards and Methodologies

Module 02: Penetration Testing Scoping and Engagement

- Scoping a Penetration Test
- Pre-engagement Interactions
- Understanding Client Requirements
- Risk Management and Mitigation

Certified Penetration Testing Professional

Module 03: Open Source Intelligence (OSINT)

- Information Gathering and Reconnaissance
- OSINT Frameworks and Tools
- Social Engineering via OSINT

Module 04: Social Engineering Penetration Testing

- Types of Social Engineering Attacks
- Email, Phone, and Physical Social Engineering
- Tools and Countermeasures

Module 05: Network Penetration Testing – External

- Network Scanning and Enumeration
- Vulnerability Analysis
- Exploitation of Internet-Facing Assets

Module 06: Network Penetration Testing – Internal

- Network Segmentation and Pivoting
- Exploiting Internal Services and Hosts
- Advanced Lateral Movement Techniques

Module 07: Web Application Penetration Testing

- OWASP Top 10 Vulnerabilities
- Authentication and Session Attacks
- Logic Flaws and Advanced Exploits

Module 08: Wireless Penetration Testing

- Wireless Network Discovery
- Attacking WPA/WPA2
- Evil Twin and Rogue Access Point Attacks

Certified Penetration Testing Professional

Module 09: IoT Penetration Testing

- Introduction to IoT Architectures
- Firmware Extraction and Analysis
- IoT Device Exploitation Techniques

Module 10: OT/SCADA Penetration Testing

- ICS/SCADA Protocols and Architectures
- Attacks on Industrial Control Systems
- Security Assessments of OT Environments

Module 11: Cloud Penetration Testing

- Cloud Service Models (IaaS, PaaS, SaaS)
- Attacking AWS and Azure Environments
- Cloud Configuration and Exploitation

Module 12: Binary Analysis and Exploitation

- Static and Dynamic Binary Analysis
- Buffer Overflows and Memory Exploits
- Writing Exploits and Using Debuggers

Module 13: Report Writing and Post-Test Activities

- Writing a Professional Penetration Test Report
- Risk Rating and Recommendations
- Post-Engagement Cleanup and Client Debrief

Bonus Labs & Challenges

- Capture the Flag (CTF)-style practical exercises
- Multi-layered engagement scenarios
- Real-world live network simulations

Certified Penetration Testing Professional

Course Objectives

1. Advanced Penetration Testing Techniques
    - Master advanced penetration testing techniques for network, web, wireless, and cloud environments.
    - Learn multi-level pivoting and advanced evasion techniques.
2. Enterprise Network Penetration Testing
    - Assess large enterprise networks, including segmentation, firewalls, and DMZs.
    - Perform exploitation in hardened and segmented environments.
3. Web Application and API Security Testing
    - Identify and exploit web application vulnerabilities including business logic flaws.
    - Test modern applications and APIs using advanced methods.
4. Cloud and IoT Penetration Testing
    - Conduct penetration testing on cloud platforms such as AWS and Azure.
    - Assess and exploit vulnerabilities in IoT and smart devices.
5. Operational Technology (OT) and ICS Security Testing
    - Learn penetration testing techniques for SCADA and ICS/OT environments.
    - Understand protocols like Modbus, DNP3, and others.
6. Binary Exploitation and Reverse Engineering
    - Analyze binaries and exploit buffer overflows.
    - Reverse engineer binaries to discover and exploit vulnerabilities.
7. Privilege Escalation and Lateral Movement
    - Use real-world techniques to escalate privileges on compromised systems.
    - Perform lateral movement across internal networks securely and stealthily.
8. Writing Exploits and Custom Scripts
    - Create and modify scripts to automate attacks.
    - Develop custom exploits in various programming languages.
9. Report Writing and Documentation
    - Document findings effectively for stakeholders.
    - Create comprehensive penetration testing reports.
10. Hands-On Challenge-Based Learning
    - Apply skills in a live, dynamic, and segmented network environment.
    - Face real-time challenges like capturing flags and performing multi-layered attacks under constraints.