800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

EC-Council Certified Penetration Testing Professional Training (CPENT)

EC-Council Authorized Training · Applied Technology Academy

EC-Council is rewriting the standards of penetration testing skill development with the Certified Penetration Testing Professional, the CPENT certification program. What makes this program unique is our approach that allows you to attain two certifications with just one exam. The key philosophy behind the CPENT is simple – a penetration tester is as good as their skills; that's why we urge you to go beyond Kali Linux and go beyond tools.

LEVEL	DURATION	EXPERIENCE	AVERAGE SALARY	LABS
Intermediate	**5 Days**	**None with official training (2 yrs InfoSec or CEH recommended)**	**$138,650**	**Yes**

Course Overview

The Certified Penetration Testing Professional (CPENT) program is the world's most comprehensive guided penetration testing program. It offers a complete hands-on pentesting methodology and AI techniques mapped to all pentesting phases. CPENT enables you to master pentesting within an enterprise network environment, evaluating intrusion risks and compiling actionable, structured reports.

Distinguish yourself with the CPENT AI, learning beyond technical knowledge—scoping engagements, understanding design, estimating effort, and presenting findings—and thrive as a leader in offensive security with versatile skills. CPENT combines guided learning with hands-on practice while immersing you in diverse live scenarios involving IoT systems, segmented networks, and advanced defenses, with practical challenges mapped to each domain. Gain expertise in advanced skills necessary to create your tools, conduct advanced binary exploitation, double pivot, customize scripts, and write your exploits to penetrate the deepest pockets of the network.

Key Highlights:

- Hands-on course featuring CTFs, 110+ labs, live cyber ranges, and 50+ tools
- Practical exam tests skills on unique multi-disciplinary network ranges
- The only program to teach a complete pen testing methodology
- Prepares you for VAPT compliance and various regulations

Course Outline

- **Module 01: Introduction to Penetration Testing and Methodologies**
- **Module 02: Penetration Testing Scoping and Engagement**
- **Module 03: Open-Source Intelligence (OSINT)**
- **Module 04: Social Engineering Penetration Testing**
- **Module 05: Web Application Penetration Testing**
- **Module 06: API and Java Web Token Penetration Testing**
- **Module 07: Perimeter Defense Evasion Techniques**
- **Module 08: Windows Exploitation and Privilege Escalation**
- **Module 09: Active Directory Penetration Testing**
- **Module 10: Linux Exploitation and Privilege Escalation**
- **Module 11: Reverse Engineering, Fuzzing, and Binary Exploitation**
- **Module 12: Lateral Movement and Pivoting**
- **Module 13: IoT Penetration Testing**
- **Module 14: Report Writing and Post-Testing Actions**

Intended Audience

- Information Security Analyst / Administrator
- Information Assurance (IA) Security Officer
- Information Security Manager / Specialist
- Information Systems Security Engineer / Manager
- Information Security Professionals / Officers
- Information Security / IT Auditors
- Risk / Threat / Vulnerability Analyst
- System Administrators
- Network Administrators and Engineers

Prerequisites

- At least two years of IT security experience
- A strong working knowledge of TCP/IP
- Security+ Prep Course is highly recommended

Ready to enroll? Call 800.674.3550 or email Info@AppliedTechAc.com — private team cohorts, GSA MAS purchasing, military credentialing funding, VA GI Bill and VR&E and student financing available.