EC – Council Certified Penetration Testing Professional (CPENT)

Course Duration: 5 Days

Course Overview

The Certified Penetration Testing Professional (CPENT) course is an advanced hands-on program designed to equip cybersecurity professionals with the skills needed to perform effective penetration testing across enterprise networks, web applications, cloud environments, OT/IoT systems, and even hybrid infrastructures. Participants learn to think and operate like real-world threat actors while applying advanced exploitation techniques, pivoting strategies, privilege escalation, evasion tactics, and post-exploitation methods in complex scenarios. With its emphasis on practical, live-range challenges, CPENT prepares learners not only to uncover vulnerabilities but also to provide actionable remediation strategies, making them highly competent penetration testers ready for today's evolving cybersecurity landscape.

Job Roles Mapped to C|PENT Certification

- Penetration Tester
- Penetration Testing Consultant
- Penetration Testing Engineer
- Security Penetration Testing Consultant / Architect
- Vulnerability Assessment and Penetration Testing (VAPT) Analyst / Engineer
- QA Security Tester
- Web Application Penetration Tester
- Vulnerability Assessment Specialist
- Red Team - VAPT Security Consultant
- Penetration Test Lead
- Network Penetration Testing Engineer
- Director of Technical Advisor
- Senior Manual Ethical Hacker
- Senior API Security Vulnerability Analyst
- Application Security Engineer (Penetration Tester)
- Senior Web Application Security Specialist
- Senior Red Team Operator
- Cyber Threat Operator

- Computer Exploitation Test Engineer (Penetration Tester)
- Security Vulnerability Management Lead
- Security Lit - AI/ML Security Engineer
- AI Cyber Security Advisory Engineer
- Cyber Security Engineer (Generative AI)

Course Outline

Learn	Course Outline
Module 01	Introduction to Penetration Testing and Methodologies
Module 02	Penetration Testing Scoping and Engagement
Module 03	Open-Source Intelligence (OSINT) and Attack Surface Mapping
Module 04	Social Engineering Penetration Testing
Module 05	Web Application Penetration Testing
Module 06	API and Java Web Token Penetration Testing
Module 07	Network Penetration Testing – Perimeter Devices
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

Additional Self-Study Modules

a) Penetration Testing Essentials Concepts
b) Fuzzing
c) Mastering Metasploit Framework
d) PowerShell Scripting
e) Bash Environment and Scripting
f) Python Environment and Scripting
g) Perl Environment and Scripting
h) Ruby Environment and Scripting
i) Active Directory Penetration Testing
j) Database Penetration Testing
k) Mobile Device Penetration Testing

Exam Details:

Exam Details	CPENT (Practical Exam)
Number of Questions/Practical Challenges	2 practical exams / 5 challenges each
Test Duration	24 Hours / 12 each
Test Format	Performance-based, hands-on exam
Test Delivery	Fully online, remotely proctored practical exam
Passing Score	Score should be at least 70% in the C|PENT practical exam

Eng. Jalal Sela

Senior Information Security Engineer/Academy Manager

Experience and Skills Summary

JS has over 16 years of experience in cyber security and software development, member of the open-source community since 2009, a respectful member in the hackers' community, done many technical security assessments on open-source projects such as PrestaShop, OpenBravo (currently Odoo) and WordPress, and over 500 network and wireless penetration testing projects, and over 100 major WAPT projects, worked as project manager for many years in Mexico, delivering high quality products and services. In Jordan he participated in many security conferences and online workshops, an author and security researcher, has many blogs and websites about hacking and technology in general.

JS is also the leader of The Hacking Minions community (https://hackingminions.com) the biggest hacking community in the middle-east.

JS delivered countless technical security assessment in KSA, Dubai, Bahrain, Jordan, Palestine, Mexico, and Denmark, for the banking, government, military, and the private sector.

JS is an author of many courses and training programs for companies in Jordan and USA related to network and system security pentesting, incident handling, secure coding, and web application security pentesting.

Currently JS is the Academy Manger and Sr. Information Security Consultant working in IT Security C&T (2014-current date).

Technical Skills and Attributes

- Web application penetration testing.
- Network devices and services penetration testing.
- Mobile application penetration testing.
- System developer (multi-languages / platforms).
- Code review and security analysis.
- Authorized EC-Council Instructor.
- Authorized CompTIA Instructor.
- Competency Assessment.

Courses, Accreditation and Certifications

- Bachelor's degree in Computer and Networks Engineering at Universidad Morelos de Cuernavaca (UMC)/Mexico
- Certified Ethical Hacker (CEH), EC-Council.
- Computer Hacking Forensics Investigator (CHFI), EC-Council.
- Certified Network Defender (CND), EC-Council.
- Certified Penetration Testing Engineer (CPTE) 272000, Mile2.
- Certified Incident Handling Engineer (CIHE) 273500, Mile2.
- Certified Application Security Engineer .NET (CASE .NET), EC-Council.
- Certified Application Security Engineer .NET (CASE Java), EC-Council.
- Certified Secure Web Application Engineer (CSWAE) 2904000, Mile2.
- Mobile Application Pentesting: eMAPT, eLearning Security.
- Certified ISO 27001 LI
- CCNA/Security.
- CompTIA Security+
- CompTIA CySA+
- Secure Coding Essentials (SCE), IT Security C&T.