

Certified Penetration Testing Professional (CPENT v2 with AI)

Move from ethical hacker to professional penetration tester with EC-Council's fully practical, AI-augmented CPENT v2, with the official exam voucher included in your fee.

Duration: 5 to 8 evenings from 24 Aug 2026, 6 pm PKT

Prepares for: EC-Council CPENT v2 with AI

Format: Online or onsite, 1-on-1 or batch

Target exam: CPENT v2 with AI (EC-Council practical exam)

NUEXUS certificate on completion

OVERVIEW

CPENT is EC-Council's advanced penetration testing credential, and version 2 rebuilds it around AI-assisted testing workflows. This mentor-led programme, delivered by an EC-Council Master Trainer, takes you through all 14 CPENT modules the way a real engagement runs: scoping and rules of engagement, OSINT and attack-surface mapping, social engineering, web application and API testing, perimeter defense evasion, Windows and Linux exploitation and privilege escalation, Active Directory attacks, reverse engineering and binary exploitation, lateral movement and pivoting, IoT testing, and finally professional report writing. Every module is practiced hands-on in a live lab. Your enrollment fee covers the training and the official EC-Council CPENT exam voucher, so you leave with a NUEXUS completion certificate and a booked path to the CPENT credential, which EC-Council issues when you pass its 24-hour practical exam.

SKILLS YOU WILL GAIN

Engagement Scoping & RoE

OSINT & Attack-Surface Mapping

Social Engineering Testing

Web Application Pentesting

API & JWT Pentesting

Perimeter Defense Evasion

Windows Exploitation & PrivEsc

Active Directory Attacks

Linux Exploitation & PrivEsc

Reverse Engineering & Fuzzing

Binary Exploitation

Lateral Movement & Pivoting

IoT Pentesting

AI-Assisted Pentesting

Penetration Test Reporting

WHAT YOU WILL BE ABLE TO DO

- Scope, plan, and run a full penetration testing engagement under rules of engagement, from OSINT and attack-surface mapping to a client-ready report
- Test web applications, APIs, and JSON Web Tokens for authentication, authorization, injection, and business-logic weaknesses
- Exploit Windows and Linux hosts, escalate privileges, and attack Active Directory environments the way modern adversaries do
- Evade perimeter defenses, move laterally, and pivot through segmented networks to reach protected targets
- Perform reverse engineering, fuzzing, and binary exploitation, and assess IoT devices and their supporting infrastructure
- Use AI-assisted techniques to accelerate reconnaissance, analysis, and reporting, and sit the 24-hour CPENT practical exam with a tested methodology

WHO IT IS FOR

- Ethical hackers and CEH holders who want to step up to a fully practical, engagement-style penetration testing credential
- Penetration testers, red teamers, and VAPT consultants who need a recognized advanced certification for client and employer requirements
- SOC, blue team, and security engineering professionals moving into offensive security
- Security consultants and IT professionals who want to prove they can run an end-to-end penetration test, not only individual attacks
- Candidates aiming at the Licensed Penetration Tester (LPT) designation, which EC-Council awards for a score above 90%

PREREQUISITES

- Solid ethical hacking and networking fundamentals: CEH-level knowledge or equivalent hands-on experience
- Comfort at the command line on both Windows and Linux, and familiarity with common tools such as Nmap, Burp Suite, and Metasploit
- Basic scripting ability in at least one language such as Python, Bash, or PowerShell is strongly recommended
- A laptop able to run virtual machines and a stable internet connection for the live labs and the online exam range

WHAT'S INCLUDED

- The official EC-Council CPENT v2 with AI exam voucher, included in the fee
- Live, interactive, mentor-led evening sessions from Monday 24 August 2026 (5 to 8 evenings, 6:00 pm to midnight PKT, some run to 2:00 am), online or onsite in Islamabad
- Hands-on labs across all 14 CPENT modules, run in a live environment
- Recordings of your own sessions to revisit anytime
- Exam-range methodology, time management, and report-writing practice
- Doubt-clearing and revision support through the programme
- A verifiable NUEXUS completion certificate

COURSE CURRICULUM

1 Introduction to Penetration Testing and Methodologies

Penetration testing types, phases, and industry methodologies

Legal, ethical, and compliance considerations for testers

Where AI fits in a modern, AI-augmented testing workflow

How the CPENT exam range and scoring work

2 Penetration Testing Scoping and Engagement

Pre-engagement, scoping, and rules of engagement

Contracts, authorization, and communication plans

Building the test plan and managing engagement risk

Evidence handling and engagement documentation

3 Open-Source Intelligence (OSINT)

Passive reconnaissance and attack-surface mapping

Domain, DNS, certificate, and infrastructure intelligence

People, email, and social media OSINT

AI-assisted collection and analysis of open sources

4 Social Engineering Penetration Testing

Social engineering attack vectors and pretexting

Phishing, vishing, and physical-security testing

Running an authorized social engineering assessment

Measuring results and recommending controls

5 Web Application Penetration Testing

Web application reconnaissance and mapping

Authentication, session, and access-control flaws

Injection, XSS, SSRF, and file-handling attacks

Business-logic testing and OWASP-aligned reporting

6 API and Java Web Token Penetration Testing

REST and GraphQL API enumeration and testing

Broken object-level and function-level authorization

JSON Web Token weaknesses: algorithm, signature, and claims attacks

Rate-limiting, mass-assignment, and API misconfiguration

7 Perimeter Defense Evasion Techniques

Firewall, IDS, and IPS detection and evasion

Bypassing web application firewalls and filters

Tunneling and encoding techniques

Testing perimeter devices without tripping controls

8

Windows Exploitation and Privilege Escalation

Windows enumeration and vulnerability identification

Exploiting services, misconfigurations, and credentials

Local privilege escalation techniques on Windows

Post-exploitation and persistence

9

Active Directory Penetration Testing

AD enumeration and mapping trust relationships

Kerberos attacks: Kerberoasting, AS-REP roasting, and delegation abuse

Credential attacks, pass-the-hash, and lateral movement in AD

Domain privilege escalation and domain dominance

10

Linux Exploitation and Privilege Escalation

Linux enumeration and service exploitation

SUID, sudo, cron, and capability abuse

Kernel and misconfiguration-based escalation

Post-exploitation on Linux hosts

11

Reverse Engineering, Fuzzing, and Binary Exploitation

Static and dynamic analysis of binaries

Fuzzing to discover crashes and vulnerabilities

Buffer overflows and exploit development basics

Bypassing common binary protections

12

Lateral Movement and Pivoting

Pivoting through compromised hosts

Port forwarding, SSH tunneling, and proxy chains

Reaching segmented and double-pivot networks

Maintaining access across the environment

13

IoT Penetration Testing

IoT architecture, protocols, and attack surface

Firmware extraction and analysis

Testing IoT devices, apps, and cloud back ends

Reporting IoT findings and mitigations

14

Report Writing and Post-Testing Actions

Structuring a professional penetration test report

Writing findings, evidence, risk ratings, and remediation

Executive summaries and client debriefs

Retesting, cleanup, and the CPENT report submission

CAREER OUTCOMES

	Penetration Tester	Red Team Operator	Offensive Security Engineer	VAPT Consultant	Security Consultant
Entry	USD 60,000 to 90,000				
Mid	USD 90,000 to 130,000				
Senior	USD 130,000 to 170,000				

Global averages from Glassdoor and PayScale, 2025, for penetration testing roles. Actual pay varies by country, employer and experience.

CERTIFICATION PATH

NUEXUS training certificate	EC-Council CPENT v2 with AI
-----------------------------	-----------------------------

Issued by NUEXUS on course completion. Verifiable at nuexus.com/verify.

Earned by passing the official exam. Issued and verified by the certification body itself, not by NUEXUS.

Exam	CPENT v2 with AI (EC-Council practical exam)
Questions	Live-range challenges across the CPENT domains, plus a written penetration test report
Format	Fully practical, proctored, on EC-Council's live cyber range; report submitted within seven days of the final session
Duration	24 hours, taken as one 24-hour session or two 12-hour sessions
Passing score	EC-Council sets the cut score per exam form (its published range is 60% to 85%); a score above 90% also earns the LPT designation
Delivery	EC-Council online proctored exam over the CPENT cyber range

The official EC-Council CPENT exam voucher is included in the enrollment fee for this cohort. Even when NUEXUS arranges your exam voucher, the resulting certification is issued and verified by the certification body directly.