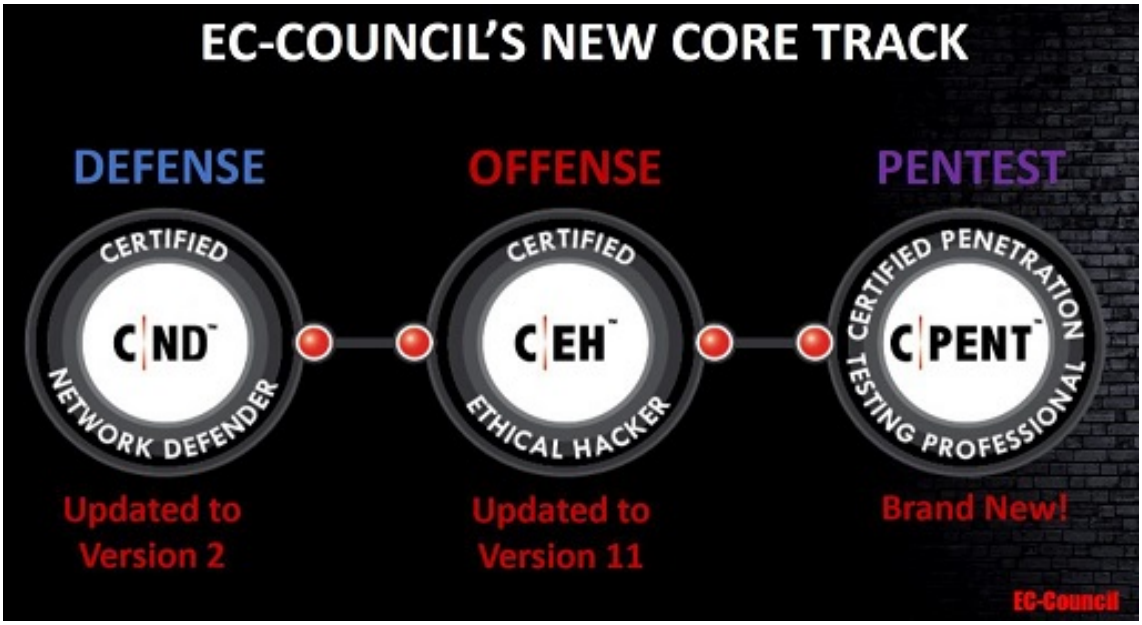
5 Days

EC-Council- Certified Penetration Testing Professional (CPENT)

Certified Penetration Testing Professional [CPENT] is a Specialization level authorization for Pen Testers among others. It covers Penetration Testing across Internet of Things [IoT] and Operating Systems. Apart from this, learners understand how to conduct advanced binaries, double pivot to access hidden networks and other technologies which aren't taught in any other certification in the world. Being 100% mapped with the NICE framework, and being a mixture of both manual and automated penetration approaches, helps all its stakeholders immensely.



After signing up for CPENT certification whose unique part is that this accreditation, an applicant is challenged to graduate from running just the Kali Linux course tools, upgrade themselves so that their organization's systems can become closer to being impenetrable from external hackers.

Training of Certified Penetration Testing Professional [CPENT] is of 40-hours and offered in the domain of Penetration Testing. Candidates sit for EC-Council's 2 practical exams of 12-hour each, which can be taken in a single session of 24 hours.

Post being authenticated as a Certified Penetration Testing Professional [CPENT], or if you manage a score of more than 90%, a Licensed Penetration Testing Master [LPT] Master certification is acquired by applicants.

Certified Penetration Testing Professional [CPENT]'s Course Objectives:

On completion of CPENT Training and clearing the exam, our clients will be able to learn new techniques and update their knowledge on the intricate tricks and terms in the following:

- Access Hidden Networks with Pivoting
- Advanced Windows Attacks
- Attack Automation with Scripts
- Attacking IOT Systems
- Bypassing a Filtered Network
- Double Pivoting
- Evading Defense Mechanisms
- Privilege Escalation

- Pentesting Operational Technology (OT)
- Weaponize Your Exploits
- Writing Exploits: Advanced Binary Exploitation
- Write Professional Reports

Course Details

Course Outline

There are 14 modules of theoretical training that have to be completed before giving the exam. These are:

Module 01: Introduction to Penetration Testing
Module 02: Penetration Testing Scoping and Engagement
Module 03: Open Source Intelligence (OSINT)
Module 04: Social Engineering Penetration Testing
Module 05: Network Penetration Testing – External
Module 06: Network Penetration Testing– Internal
Module 07: Network Penetration Testing – Perimeter Devices
Module 08: Web Application Penetration Testing
Module 09: Wireless Penetration Testing
Module 10: IoT Penetration Testing
Module 11: OT/SCADA Penetration Testing
Module 12: Cloud Penetration Testing
Module 13: Binary Analysis and Exploitation
Module 14: Report Writing and Post Testing Actions

Who Should Attend

Cybersecurity professionals can also acquire any one of the below posts and any of these can attend training for the same:

- Ethical Hackers
- Penetration Testers
- Firewall Administrators
- IT Security Administrator
- Network server Administrators
- System Administrators
- Information security Consultant
- Senior Information Assurance Specialist
- Security Specialist
- Cyber Security Forensic Analyst
- Cyber Threat Intelligence Analyst
- Information Security Analyst
- Junior Security Operations Center (SOC) Analyst
- Security Operations Center (SOC) Analyst
- Network Security Information Analyst
- Security Analysts
- Security Systems Analyst
- Cyber Security Engineer
- Cyber Security Assurance Engineer
- Information Security Engineer
- Security Engineer
- Technical Operations Network Engineer
- Security Tester

Pre Requisite

There is no criteria for enrolling for Certified Penetration Testing Professional [CPENT] exam. For an enriching experience, applicants are encouraged to have knowledge and experience of

- Bash, Python, Perl, and Ruby scripts
- Cabling techniques
- Coding
- Cross-site scripting (XSS), LFI, RFI vulnerabilities
- Hacking techniques and terms
- Firewall Fundamentals
- Industrial Control Systems [ICS],
- Supervisory Control and Data Acquisition Systems (SCADA)
- Binary analysis.
- Networking
- Open-source technologies like MySQL, Apache
- Transmission Control Protocol /Internet Protocol
- Wireless protocols and devices
- Web application architecture
- Web development
- Have out-of-the-box and lateral thinking

Exams

Certified Penetration Testing Professional [CPENT] [-]

464, Udyog Vihar Phase V,Gurgaon (Delhi NCR)-122016,India

+91 8882 233 777

training@mercury.co.in

www.mercurysolutions.co

Date - Apr 25, 2025