CPENT-Certified Penetration Testing Professional

Duration:40 Hrs.

Introduction to CPENT

The Certified Penetration Testing Professional or CPENT, for short, re-writes the standards of penetration testing skill development.

EC-Council's Certified Penetration Tester (CPENT) program teaches you how to perform an effective penetration test in an enterprise network environment that must be attacked, exploited, evaded, and defended. If you have only been working in flat networks, CPENT's live practice range will teach you to take your skills to the next level by teaching you how to pen test IoT systems, OT systems, how to write your own exploits, build your own tools, conduct advanced binaries exploitation, double pivot to access hidden networks, and also customize scripts/exploits to get into the innermost segments of the network.

The CPENT training program and the CPENT Challenge both come with a shot at earning your CPENT certification, so the only question is, "Do you need training or are you ready to take the CHALLENGE?"

The heart of the CPENT program is all about helping you master your pen testing skills by putting them to use on our live cyber ranges. The CPENT ranges were designed to be dynamic in order to give you a real-world training program, so just as targets and technology continue to change in live networks, both the CPENT practice and exam ranges will mimic this reality as our team of engineers continue to add targets and defenses throughout the CPENT course's lifetime.

CPENT Cyber Range - Enter if you dare!

The CPENT range consists of entire network segments that replicate an enterprise network — this is not a computer game simulation; this is an accurate representation of an enterprise network that will present the latest challenges to the pen tester. The benefit of hands on learning in a live cyber range is that candidates will encounter multiple layers of network segmentation, and the CPENT course will teach candidates how to navigate these layers, so that once access is gained in one segment, a candidate will know the latest pivoting techniques required to reach the next. However, that won't be enough on its own as the targets and segments are progressive in nature, so once you get into one machine and or segment, the next one will challenge you even more!

CPENT Live Exam - Prove you have what it takes!

CPENT is a fully online, remotely proctored practical exam that challenges candidates through a grueling 24-hour performance-based, hands-on exam. The exam is broken into 2 practical exams of 12-hours each that will test your perseverance and focus by forcing you to outdo yourself with each new challenge. Candidates have the option to choose either 2 12-hour exams or one 24-hour exam.
Candidates who score more than 70% will earn the CPENT certification. Candidates who score more than 90% attain the prestigious LPT (Master) credential!

CPENT-Certified Penetration Testing Professional

Duration:40 Hrs.

Is CEH a Pen Test Program?

The CPENT program is the next step after the Certified Ethical Hacker (CEH) certification on the journey to the Licensed Penetration Tester (LPT) Master. There is a lot of chatter out in "the ether" that refers to CEH as a Pen Test program. That information is not correct. The CEH course was designed to teach the tools and methods deployed by cyber criminals.
The CPENT and its now-retired predecessor courses, the EC-Council Certified Security Analyst (ECSA) and the Advanced Penetration Tester (APT), are pen test courses that were designed to take the concepts taught in CEH and apply them to time-proven pen test methodologies.

CPENT Benefits

- 100% mapped with the NICE framework.
- 100% methodology-based penetration testing program.
- Blends both manual and automated penetration testing approaches.
- Designed with the most common penetration testing practices offered by the best service providers.
- Maps to all major Job Portals. Role Title: Penetration Tester and Security Analyst.
- Provides strong reporting writing guidance.
- Gives a real-world experience through an Advanced Penetration Testing Range.
- Provides candidates with standard Pen test for use in the field.

CPENT… No other Pen Test Course like it!

Advanced Windows Attacks
This zone contains a complete forest that you first have to gain access to and then use PowerShell and any other means to execute Silver and Gold Ticket and Kerberoasting. The machines will be configured with defenses in place meaning you to have to use PowerShell bypass techniques and other advanced methods to score points within the zone.

Attacking IOT Systems
CPENT is the first certification that requires you to locate IOT devices and then gain access to the network. Once on the network, you must identify the firmware of the IOT device, extract it, and then reverse engineer it.

Writing Exploits: Advanced Binary Exploitation
Finding flawed code is a skill competent pen testers need. In this zone you will be required to find the flawed binaries then reverse engineer them to write exploits to take control of the program execution. The task is complicated by the requirement of penetrating from the perimeter to gain access then discover the binaries. Once that is done you have to reverse engineer the code. Unlike other certifications, CPENT includes 32 and 64 bit code challenges and some of the code will be compiled with basic protections of non-executable stacks. You must be able to write a driver program to exploit these binaries, then discover a method to escalate privileges. This will require advanced skills in binary exploitation to include the latest debugging concepts and egg hunting techniques. You are required to craft input code to

CPENT-Certified Penetration Testing Professional

Duration:40 Hrs.

first take control of program execution and second, map an area in memory to get your shell code to work and bypass system protections.

Bypassing a Filtered Network
The CPENT certification provides web zone challenges that exist within a segmentation architecture, so you have to identify the filtering of the architecture then leverage this knowledge to gain access to web applications. The next challenge is to compromise and then extract the required data from the web apps to achieve points.

Pentesting Operational Technology (OT)
The CPENT range contains a zone that is dedicated to ICS SCADA networks that the candidate will have to penetrate from the IT network side and gain access to the OT network. Once there, you will have to identify the Programmable Logic Controller (PLC) and then modify the data to impact the OT network. You must be able to intercept the Mod Bus Communication protocol and communication between the PLC and other nodes.

Access Hidden Networks with Pivoting
Based on our beta testing, pen testers struggle to identify the rules that are in place when they encounter a layered network. Therefore, in this zone you will have to identify the filtering rules then penetrate the direct network. From there, candidates have to attempt pivots into hidden networks using single pivoting methods, but through a filter. Most certifications do not have a true pivot across disparate networks and few (if any) have the requirement into and out of a filtering device.

Double Pivoting
Once you have braved and mastered the challenges of the pivot, the next challenge is the double pivot. This is not something that you can use a tool for; in most cases the pivot has to be set up manually. CPENT is the first certification in the world that requires you to access hidden networks using double pivoting.

Privilege Escalation
In this challenge, the latest methods of privilege escalation reverse engineering code to take control of execution then break out of the limited shell are required to gain root/admin.

Evading Defense Mechanisms
The range requires your exploits be tested by different defenses you are likely to see in the wild. Candidates are required to get their exploits past the defenses by weaponizing them.

Attack Automation with Scripts
Prepare for advanced penetration testing techniques and scripting with seven self-study appendices: Penetration testing with Ruby, Python, PowerShell, Perl, BASH, Fuzzing, and Metasploit.

Weaponize Your Exploits
Customize your own tools and build your armory with your coding expertise to hack the challenges presented to you as you would in real life.

Write Professional Reports
Experience how a pen tester can mitigate risks and validate the report presented to the client to really make an impact. Great pen testing doesn't mean much to clients without a clearly written report!

CPENT-Certified Penetration Testing Professional

Duration:40 Hrs.

CPENT- Is this course for you?

CPENT Candidates will be:

- Ethical Hackers
- Penetration Testers
- Network server administrators
- Firewall Administrators
- Security Testers
- System Administrators and Risk Assessment professionals

CPENT Maps to the following Industry Job Roles:

- Cyber Security Forensic Analyst
- Cyber Threat Analyst Tier 2
- Cyber Threat Intelligence Analyst
- Information Security Analyst
- Cyber Security Engineer
- Application Security Analyst
- Cyber Security Assurance Engineer
- Senior Information Assurance/ Security Specialist
- Security Systems Analyst
- Security Operations Center (SOC) Analyst
- Penetration Tester
- Technical Operations Network Engineer
- IT Security Administrator
- Security Engineer
- Information Security Engineer
- Network Security Information Analyst
- Mid Level Penetration Tester
- IT Security Analyst III
- Junior Security Operations Center (SOC) Analyst

CPENT Course Outline

- 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