Module Title : EC-Council Certified Penetration Testing Professional

Duration : 5 days

Overview

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 course is presented through an enterprise network environment that must be attached, exploited, evaded, and defended
- EC-Council's CPENT gives the industry an ability to assess a Pen Tester's skills across a broad spectrum of "network zones"
- What makes the CPENT different is the requirement to be provided a variety of different scoped of ework so that the candidate can "think on their feet"
- The result of this is that there are different zones representing different types of testing
- Anyone attempting the test will have to perfume their assessment against these different zones

Is this course for you?

CPENT Candidates will be:

- Ethical Hackers
- Penetration Testers
- Information Security Consultant
- Security Analyst
- Security Engineer
- 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 II
- 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

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

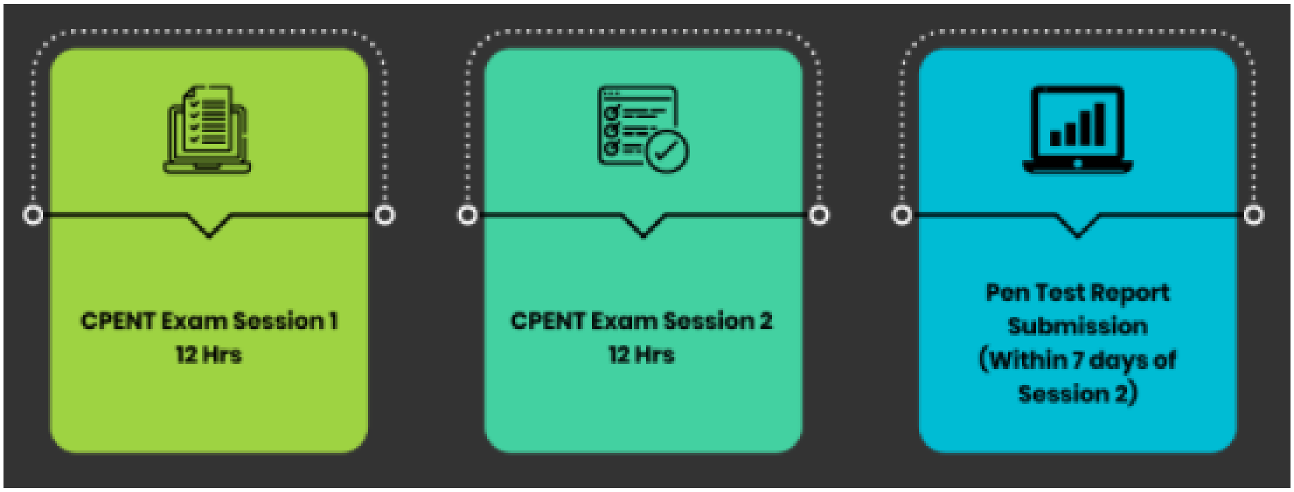
CPENT Cyber Range

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!

Single Exam, Dual Certification

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!



Exam features:

- Choose your challenge! Either two 12-Hour sessions or a single 24-Hour exam!
- EC-Council specialists proctor the entire exam – Validity is not in question.

- Score at least 70% and become a CPENT
- Score at least 90% and earn the highly regarded LPT (Master) designation!

To be a LPT (Master) means that you can find chinks in the armor of defense-in-depth network security models with the help of network pivoting, making exploit codes work in your favor, or by writing Bash, Python, Perl, and Ruby scripts. The live range CPENT exam demands that you think on your feet, be creative in your approach, and not rely on the conventional techniques.

Outsmarting and out maneuvering the adversary is what sets you apart from the crowd. The CPENT's hands-on exam offers a challenge like no other by simulating a complex network in real time. This experience will test your perseverance and focus by forcing you to outdo yourself with each new challenge.

LPT (Master) certified professional can:

- Demonstrate a repeatable and measurable approach to penetration testing
- Perform advanced techniques and attacks to identify SQL injection, Cross site scripting (XSS), LFI, RFI vulnerabilities in web applications
- Submit a professional and industry accepted report that achieves management and technical buy-in
- Get access to proprietary EC-Council penetration testing methodologies
- Write exploit codes to gain access to a vulnerable system or application
- Exploit vulnerabilities in Operating systems such as Windows, Linux
- Perform privilege escalation to gain root access to a system
- Demonstrate 'Out-of-the-box' and 'lateral' thinking
- Ensure the integrity and value of the penetration testing certification, in a fully online, remotely proctored certification exam

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.

What makes CPENT unique

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 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 need to find flawed binaries and reverse engineer them to write exploits to take control of the program execution. The task is complicated as you must first penetrate the perimeter to gain access, then discover the binaries. Once that is done, you will need 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 first craft an input code to take control of program execution, and second, map an area in memory to get your shellcode 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 you 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, you will 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 must be implemented to take control of the execution, then break out of the limited shell are required to gain root/admin.

Evading Defense Mechanisms

The range requires your exploits to be tested by different defenses you are likely to see in the wild. You are required to get these 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!