EC-Council

Are You Ready to Challenge the Toughest **Penetration Testing** Exam on the Planet?

C|PENT

Certified Penetration Testing Professional

CERTIFIED PENETRATION TESTING PROFESSIONAL

GO BEYOND | KALI | AUTOMATED TOOLS
FLAT CYBER RANGES

What is the CPENT Course?

A rigorous Pen Testing program that, unlike contemporary Pen Testing courses, teaches you how to perform an effective penetration test across filtered networks. The course requires you to Pen Test IoT systems, OT systems, builds on your ability to write your own exploits, build your own tools, conduct advanced binaries exploitation, double pivot to access hidden networks, and various technologies. In summary, there is no program of its kind in the world!

Mind the Gap

Years of research indicate that the majority of Pen Testing candidates have gaps in their skills when it comes to multiple disciplines. The metrics also prove when the targets are not located on the same or a directly connected and reachable segment, very few can perform as well as they do when it is direct and on a flat network.

That's why, for the first time in the industry, the assessment for the Certified Penetration Tester (CPENT) is about multiple disciplines and not just one or two specialty types.

▶ The course is presented through an enterprise network environment that must be attacked, 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 scopes of work 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 perform their assessment against these different zones

The **CPENT** range, which is where our penetration testers gain real-world skills is designed to provide challenges across every level of the attack spectrum. Additionally, the range contains multiple layers of network segmentation, and once access is gained in one segment, the latest pivoting techniques are required to reach the next segment. Many of the challenges will require outside-the-box thinking and customization of scripts and exploits to get into the innermost segments of the network. The key to being a highly skilled penetration tester is to go up against various targets that are configured in a variety of ways. The CPENT 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. Since the targets and technology continue to change, the CPENT is dynamic, and machines and defenses will be added as they are observed in the wild. Finally, the targets and segments are progressive in nature. Once you get into one machine and or segment, the next one will challenge you even more.

To train for the CPENT challenge, EC-Council has introduced the CPENT Program.

The following are 12 reasons that make the CPENT Program one of its kind. This exceptional course can make you one of the most advanced penetration testers in the world. The course has one purpose: To help you overcome some of the most advanced obstacles that real-world practitioners face when conducting penetration tests. Here are some examples of the challenges you will face when you are exposed to the CPENT Range:

1. Advanced Windows Attacks

This zone contains a complete forest that you first have to gain access to and once you do then your challenge is to use PowerShell and any other means to execute Silver and Gold Ticket and Kerberoasting. The machines will be configured with defenses in place; therefore, you will have to use PowerShell bypass techniques and other advanced methods to score points within the zone

2. Attacking IOT Systems

With the popularity of the IOT devices, this is the first Program that requires you to locate the IOT device(s) 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.

3. Writing Exploits: Advanced Binaries Exploitation

The challenges faced by the penetration testers today require them to use their own skills to find a flaw in code. In this zone you will be required to find the flawed binaries, reverse engineer them once found, and then write exploits to take control of the program execution.

The task is complicated and requires penetration from the perimeter to gain access then discover the binaries. Once successful, you must reverse engineer the code.

Unlike other certifications, this will not just be a simple 32-bit code. There will be 32- and 64-bit code challenges, and some of the code will be compiled with the basic protections of non-executable stacks.

Furthermore, 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 that include the latest debugging concepts and egg hunting techniques. You are required to craft input code first to take control of program execution and second to map an area in memory to get your shellcode to work and bypass system protections.

4. Bypassing a Filtered Network

The CPENT Certification differs from the others. It provides web zone challenges that exist within a segmentation architecture. As a result, you have to identify the filtering of the architecture, leverage it to gain access to the web applications that you will have to compromise, and then extract the required data to achieve points.

5. Pentesting Operational Technology (OT)

As a first in a penetration testing certification, the CPENT contains a zone dedicated to ICS SCADA networks. The candidate will have to penetrate them from the IT network side, gain access to the OT network, and once there, identify the Programmable Logic Controller (PLC) and then modify the data to impact the OT network. The candidate must be able to intercept the Mod Bus Communication protocol and communication between the PLC and other nodes.

6. Access Hidden Networks with Pivoting

Based on studies and research, few have been able to identify the rules 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, and from there, attempt pivots into the hidden network using single pivoting methods, but through a filter. Most certifications do not have a true pivot across disparate networks and a few, if any, have the requirement into and out of a filtering device.

7. Double Pivoting

Once you have braved the challenges of the pivot and mastered it, then you can test your luck at 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.

8. Privilege Escalation

The latest methods of privilege escalation are covered as well as there will be challenges that require you to reverse engineer code and take control of execution, then break out of the limited shell and gain root/admin.

9. Evading Defense Mechanisms

The different methods of evasion are covered so that you can try and get your exploits past the defenses by weaponizing them.

10. Attack Automation with Scripts

Prepare for advanced penetration testing techniques/scripting with seven self-study appendices – Penetration testing with Ruby, Python, PowerShell, Perl, BASH, and learn about Fuzzing and Metasploit.

11. Build Your Armory: Weaponize Your Exploits

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

12. Write Professional Reports

Experience how a Pen Tester can mitigate risks and validate the report presented to the client that makes an impact. The best part of it all is that during this rigorous process, you would be carrying your own tools, building your armory with your coding expertise and hacking the challenges presented to you as you would in real life.

DO YOU HAVE WHAT IT TAKES?

Inviting all the OSCP's, GPEN's and OSCE's

Apply to take on the Challenge!

If you are selected, your Exam Fee is on Us

#DareToChallengeCPENT

Target Audience

Penetration Testers, Ethical Hackers, Information security Consultant, Security Testers, Security Analysts, Security Engineers, Network Server Administrators, Firewall Administrators, System Administrators, Risk Assessment Professionals

Suggested Duration

5 days (9:00 AM – 5:00 PM)
Minimum 40 hours Training + 24 Hours Exam

Attaining the CPENT Certification

Single Exam, Dual Certification?

Should you score at least 70% in the CPENT practical exam, you shall attain the CPENT credential. However, if you are one of the few rare experts on the planets, you may be able to hit the minimum 90% to earn the right to be called a Licensed Penetration Tester (Master)!

CPENT is a fully online, remotely proctored practical exam that challenges candidates through a grueling 24-hour performance-based, hands-on exam, categorized into 2 practical exams of 12-hours each, which will test your perseverance and focus by forcing you to outdo yourself with each new challenge. Candidates have the option to choose either two 12-hour exams or one 24-hour exam depending on how straining they would want the exam to be.

Candidates who score more than 90% will establish themselves as Penetration Testing Masters and win a chance to attain the prestigious LPT (Master) credential!

CPENT is Results Oriented

01 100% mapped with the NICE framework.

02 100% methodology-based penetration testing program.

03 Blended with both manual and automated penetration testing approach

04 Designed based on the most common penetration testing services offered by the best service providers in the market.

05 Maps to the job role of a penetration tester and security analyst, based on major job portals.

06 Provides strong reporting writing guidance.

07 Gives a real-world experience through an Advanced Penetration Testing Range.

08 Offers standard templates that can help during a penetration test.

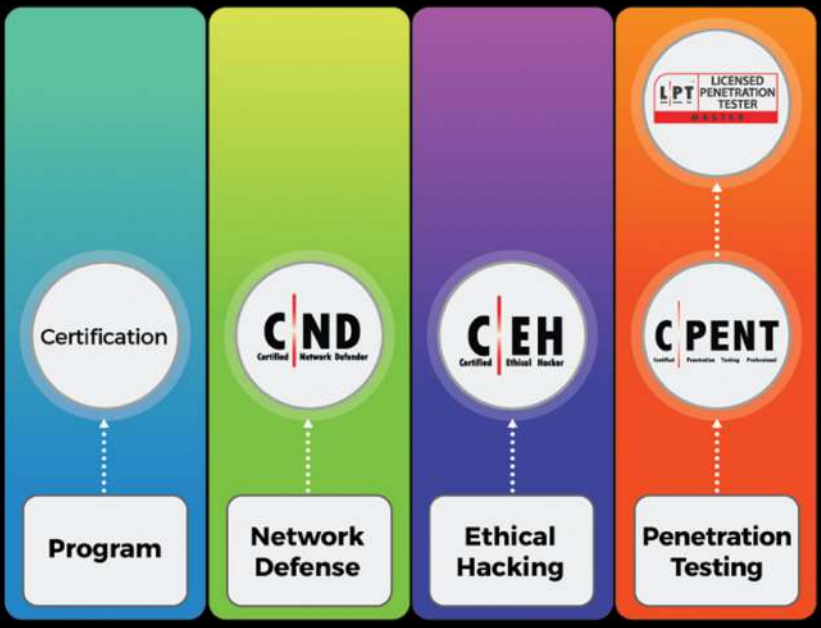
Hint – Knowledge of a CEH Practical and/or an ECSA Practical will help make the CPENT Challenge easier

Program Outline

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

Appendix A: Penetration Testing Essential Concepts	Appendix G: Perl Environment and Scripting
Appendix B: Fuzzing	Appendix H: Ruby Environment and Scripting
Appendix C: Mastering Metasploit Framework	Appendix I: Active Directory Pen Testing
Appendix D: PowerShell Scripting	Appendix J: Database Penetration Testing
Appendix E: Bash Environment and Scripting	Appendix K: Mobile Device Penetration Testing
Appendix F: Python Environment and Scripting	

EC-Council VAPT Learning Track



EC-Council

www.eccouncil.org