
EC-Council

MICROTEK LEARNING

C|PENT
Certified Penetration Testing Professional

# Master Best-in-Class Penetration Testing Skills to Safeguard Enterprises Against Advanced Cyber-Attacks

## CERTIFIED PENETRATION TESTING PROFESSIONAL

GO BEYOND | KALI | AUTOMATED TOOLS
FLAT CYBER RANGES

## WHAT IS THE C|PENT COURSE?

A rigorous Penetration Testing program that, unlike contemporary Penetration Testing courses, teaches you how to perform an effective Penetration test across filtered networks. C|PENT is a multidisciplinary course with extensive hands-on training in a wide range of crucial skills, including advanced Windows attacks, Internet of Things (IoT) and Operational Technology (OT) systems, filtered network bypass techniques, exploit writing, single and double pivoting, advanced privilege escalation, and binary exploitation. In summary, there is no program of its kind in the world!


## MIND THE GAP

Years of research indicate that the majority of Penetration Testing professionals have gaps in their skills when it comes to multiple disciplines. The metrics also prove that 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 Testing Professional (C|PENT) is about multiple disciplines and not just one or two specialty types.**

01 The course is presented through an enterprise network environment that must be attacked, exploited, evaded, and defended.

02 EC-Council's C|PENT assess a Penetration Tester's skills across a broad spectrum of "network zones".

03 What makes the C|PENT different is the requirement to be provided a variety of different scopes of work so that the candidate can "think on their feet."

04 The result of this is that there are different zones representing different types of testing.

05 Anyone attempting the test will have to perform their assessment against these different zones.

---

**The C|PENT 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 C|PENT 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 Penetration Tester. Since the targets and technology continue to change, the C|PENT 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.

# With C|PENT, Learn Next-Generation Techniques and Methodologies for Handling Real-World Threat Situations

The following are 12 reasons that make the C|PENT Program one of a 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 C|PENT Range:

### ADVANCED WINDOWS ATTACKS

**1**

This zone contains a complete forest that you first have to gain access to and once you do, 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.

### ATTACKING IOT SYSTEMS

**2**

With the popularity of 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.

### WRITING EXPLOITS: ADVANCED BINARIES EXPLOITATION

**3**

The challenges faced by Penetration Testers today require them to use their own skills to find a flaw in the 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.

## BYPASSING A FILTERED NETWORK

**4**

The C|PENT 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.

## PENTESTING OPERATIONAL TECHNOLOGY (OT)

**5**

As a first in a Penetration Testing Certification, the C|PENT 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.

## ACCESS HIDDEN NETWORKS WITH PIVOTING

**6**

Based on studies and research, few professionals 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.

## DOUBLE PIVOTING

**7**

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. C|PENT is the first certification in the world that requires you to access hidden networks using double pivoting.

## PRIVILEGE ESCALATION

**8**

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.

## EVADING DEFENSE MECHANISMS

**9**

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

### ATTACK AUTOMATION WITH SCRIPTS

**10**

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.

### BUILD YOUR ARMORY: WEAPONIZE YOUR EXPLOITS

**11**

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.

### WRITE PROFESSIONAL REPORTS

**12**

Experience how a Penetration 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.

## TARGET AUDIENCE

- Ethical Hackers
- Penetration Testers
- Network Server Administrators
- Firewall Administrators
- Security Testers
- System Administrators and Risk Assessment Professionals
- Cybersecurity Forensic Analyst
- Cyberthreat Analyst
- Cloud Security
- Analyst Information Security Consultant
- Application Security Analyst
- Cybersecurity Assurance Engineer
- Security Operations Center (SOC) Analyst
- Technical Operations Network Engineer
- Information Security Engineer
- Network Security Penetration Tester
- Network Security Engineer
- Information Security Architect

## SUGGESTED DURATION

**5 DAYS**
(9:00 AM – 5:00 PM)

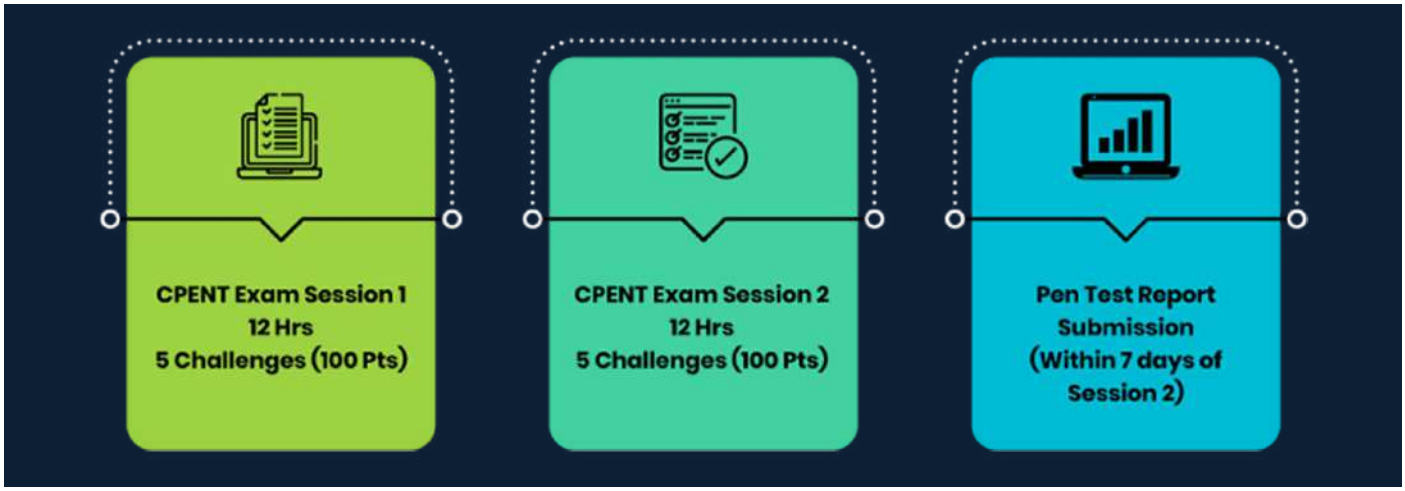
**MINIMUM** 40h **TRAINING** + 24h **EXAM**

# ATTAINING THE C|PENT CERTIFICATION

## SINGLE EXAM, DUAL CERTIFICATION?

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

C|PENT is a fully online, remotely proctored practical exam, which 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 the Penetration Testing Masters and attain the prestigious LPT (Master) credential!**

# C|PENT IS RESULTS ORIENTED

**01**
100% mapped with the NICE framework.

**02**
Maps to the job role of a Penetration Tester and security analyst, based on major job portals.

**03**
100% methodology-based Penetration Testing program.

**04**
Provides strong reporting writing guidance.

**05**
Blended with both manual and automated Penetration Testing approach.

**06**
Gives a real-world experience through an Advanced Penetration Testing Range.

**07**
Designed based on the most common Penetration Testing services offered by the best service providers in the market.

**08**
Offers standard templates that can help during a Penetration test.

# PROGRAM 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 |

# ADDITIONAL SELF-STUDY MODULES

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

# EC-COUNCIL'S VULNERABILITY ASSESSMENT AND PENETRATION TESTING (VAPT) LEARNING TRACK

## C|PENT
Certified Penetration Testing Professional

**OUTCOMES**

› Mastery of Penetration Testing skills.
› Perform the repeatable methodology.
› Commitment to the code of ethics.
› Present analyzed results through structured reports.

## CEH ETHICAL HACKER PRACTICAL

**OUTCOMES**

› Mastery of ethical hacking skills.
› Useful in real-life cyber attack scenarios.

## C|EH
Certified Ethical Hacker

**OUTCOMES**

› A thorough introduction to ethical hacking.
› Exposure to threat vectors and countermeasures.

## C|ND
Certified Network Defender

**OUTCOMES**

› Protect, detect, respond, and predict approach.
› Vendor-neutral certification with no tools/technologies restrictions.
› Learn general network security concepts, tools, and procedures.
Design, develop, and maintain secure networks.

# EC-Council