C|PENT AI

# CERTIFIED PENETRATION TESTING PROFESSIONAL

Master AI-Driven Pentesting with Proven Methodologies for Real-World Success

EC-Council
Building A Culture Of Security

C|PENT AI
Certified Penetration Testing Professional

# Go Beyond Pen Testing

## AI Techniques Mapped to All Pen Testing Phases:

# Master AI Pen Testing Skills

C|PENT AI

Certified | Penetration Testing Professional

## A Complete Hands-On Penetration Testing Methodology Program:

# Master Versatile, Tactical Pen Testing Skills

# Pen Testing: A Critical and Growing Priority in Cybersecurity

## Rising Importance of Pen Testing

**99%** agree that as technology evolves, pen testing becomes increasingly important (Cobalt).

## Prioritize In-House Security Testing

**69%** of CISOs like to have dedicated in-house security testing. (Pentera)

## Pen Testing as a Critical Defense

**72%** confirm that pen testing has prevented breaches at their organization (Fortra).

# Talent Shortage – Growing Demand for Versatile Pen Testers

## Key Pen Testing Challenge: Resource Constraints

**62%** agree lack of resources to act on findings/perform remediation, a primary challenge in performing pentesting (Fortra).

## Primary Barrier to Pentesting: Shortage of Versatile Pentester

**42%** reported availability of pentesters as a primary barrier to pentesting (Core Security).

# Talent Shortage – Growing Demand for AI Pentesting Skills

## Shortage of AI Skills

**33.9%** of the cybersecurity respondents pointed to a shortage of AI skills (O'Reilly).

## AI Demand Has Outpaced Skills

**57%** of respondents say the demand for AI has outpaced their security team's ability to keep up (Cobalt).

Organizations are on the hunt for versatile, AI-powered pen testers who can lead offensive security with robust, real-world skills.

# Are You Ready to Be One of Them?

## Gain End-to-End Pen Testing Mastery and Elevate Your Career with the Certified Penetration Testing Professional (C|PENT[AI])

## Why Should You Join C|PENT[AI] ?

### C|PENT[AI] enables you to stand out as it empowers you to:

- Gain mastery in a complete hands-on pen testing methodology.
- Master AI pen testing skills mapped to all pen testing phases.
- Validate and test your skills across five unique multi-disciplinary courses, facing challenges at every level of the attack spectrum.
- Expand technical expertise in advanced penetration testing tools, techniques, methodologies, and AI tools.
- Become proficient in skills beyond the essential pen testing skills.
- Prioritize often-overlooked and critical aspects—scoping engagements, understanding design, estimating effort, and presenting findings.
- Develop the mindset of well-rounded, versatile professionals and lead red teams with offensive security skills.
- Engage in a hybrid learning model that combines guided learning and self-learning.
- Practice in diverse scenarios that mimic real-world enterprise environments with IoT systems, segmented networks, and advanced defenses.
- Participate in a highly tactical program with offensive security training.
- Gain deep practice through CTF challenges, the largest library of 100+ labs, and live cyber ranges.
- Follow and learn a rigorous, systematic approach that emulates a hacker's movement through configured target domains.
- Learn how to infiltrate organizations, evaluate risks, and write an actionable report.
- Show your prowess in a 100% practical exam, validating both your technical and non-technical skills.
- Validate your elite offensive security skills on a global scale.
- Become VAPT-ready to handle real-world challenges and compliance requirements.

## Master Every Skill. Become a Complete Pentester.

# Unique Critical Components of C|PENT AI

1. AI Pen Testing Techniques Mapped to All Pen Testing Phases
2. Complete Hands-on Pen Testing Methodology
3. The World's Most Comprehensive Pen Testing Program with Guided Learning in Labs
4. 110+ Hands-On Labs
5. Live Cyber Ranges
6. 100% Practical Exam
7. Unique Multi-Disciplinary Network Ranges
8. Advanced Penetration Testing Techniques
9. Extensive Collection of Templates and Cheat Sheets
10. Scripting Techniques for Penetration Testing
11. Industry-Recognized & Aligned with Global Frameworks

## 1. AI Pen Testing Techniques Mapped to All Pen Testing Phases

Leverage cutting-edge AI tools like ChatGPT, ShellGPT, and PentestGPT to enhance efficiency, automate tasks, and simulate real-world cyber threats. AI techniques are mapped to all technical domains of C|PENT AI, with unique labs for practical application.

## 2. Complete Hands-on Pen Testing Methodology

Unlike many other certifications, C|PENT AI covers the complete pen testing methodology from planning, scoping, and rules of engagement to the test execution and report writing phase of a pen testing assignment. The program includes all skill sets required to manage and execute a complete pen test assignment.

## 3. The World's Most Comprehensive Pen Testing Program with Guided Learning in Labs

Pen testing is tough. C|PENT AI differentiates itself from popular self-paced programs by combining both expert-led instruction and hands-on labs to build real-world skills and critical thinking.

## 4. 110+ Hands-On Labs

Access 110+ labs and immersive cyber ranges designed to mimic enterprise environments, including IoT systems and segmented networks.

## 5. Live Cyber Ranges

Train on complex enterprise attack scenarios featuring multi-layered network security, DMZs, VPNs, firewalls, and endpoint defenses. Tackle 12 CTF challenges to refine penetration testing skills.

## 6. 100% Practical Exam

Features five exam ranges mimicking real-world penetration tests

Choose between a 24-hour exam or a flexible format of two 12-hour sessions

Earn a dual certification: Score more than 90% and earn the Licensed Penetration Tester certification

## 7. Unique Multi-Disciplinary Network Ranges

Validate and test your skills across five unique multi-disciplinary courses with challenges across every level of the attack spectrum: Active Directory (AD) Range, Binaries Range, IoT Range, Web Range, and CTF (Capture the Flag) Range.

## 8. Advanced Penetration Testing Techniques

Gain expertise in:

- Windows & AD Attacks
- IoT System Exploits
- Advanced Binary Exploitation
- Bypassing Network Filters
- Defense Evasion & Privilege Escalation
- Lateral Movement & Data Exfiltration
- Custom Exploit Development & Automation

## 9. Extensive Collection of Templates & Cheat Sheets

Access a comprehensive repository of penetration testing methodologies, report templates, scripts, and tool cheat sheets.

## 10. Scripting Techniques for Penetration Testing

Learn to automate tasks and develop custom tools using Python, Perl, Shell/Bash, Ruby, and JavaScript for efficient vulnerability exploitation.

## 11. Industry-Recognized & Aligned with Global Frameworks

The C|PENT[AI] program is aligned with Cyber Kill Chain (CKC) and MITRE ATT&CK frameworks and is globally recognized by organizations like NCSC, NICE, CREST, and more.

# Course Outline

| Learn | Course Outline |
|---|---|
| Module 01 | Introduction to Penetration Testing and Methodologies |
| Module 02 | Penetration Testing Scoping and Engagement |
| Module 03 | Open-Source Intelligence (OSINT) and Attack Surface Mapping |
| Module 04 | Social Engineering Penetration Testing |
| Module 05 | Web Application Penetration Testing |
| Module 06 | API and Java Web Token Penetration Testing |
| Module 07 | Perimeter Defense Evasion Techniques |
| Module 08 | Windows Exploitation and Privilege Escalation |
| Module 09 | Active Directory Penetration Testing |
| Module 10 | Linux Exploitation and Privilege Escalation |
| Module 11 | Reverse Engineering, Fuzzing, and Binary Exploitation |
| Module 12 | Lateral Movement and Pivoting |
| Module 13 | IoT Penetration Testing |
| Module 14 | Report Writing and Post-Testing Actions |

# Self-Study Modules

- Penetration Testing Essential Concepts
- Mastering Metasploit Framework
- PowerShell Scripting
- Bash Environment and Scripting
- Python Environment and Scripting
- Perl Environment and Scripting
- Ruby Environment and Scripting
- Wireless Penetration Testing
- OT and SCADA Penetration Testing
- Cloud Penetration Testing
- Database Penetration Testing
- Mobile Device Penetration Testing

# What Skills Will You Gain with C|PENT$^{AI}$?

Acquire a comprehensive knowledge of SOC processes, procedures, technologies, and workflows.

Learn the fundamentals of penetration testing, including its objectives, methodologies, frameworks, and role in an organization's security strategy.

Understand how to scope penetration testing engagements, define objectives, establish clear communication with stakeholders, and adhere to legal and ethical boundaries.

Understand OSINT techniques to gather actionable intelligence and learn to identify, map, and analyze an organization's attack surface.

Learn the art of exploiting human vulnerabilities through social engineering techniques, along with preventive measures to mitigate such risks.

Cultivate techniques for testing web applications for vulnerabilities such as SQL injection, XSS, and authentication flaws, and learn methods to exploit and remediate these issues.

Understand how to assess API security by testing endpoints, exploiting misconfigurations, and identifying weaknesses in JSON Web Tokens (JWT).

Learn advanced techniques to bypass firewalls, intrusion detection systems (IDS), routers, switches, and other perimeter defenses.

Gain methods to exploit vulnerabilities in Windows systems and perform privilege escalation to gain higher-level access.

Discover how to test and exploit vulnerabilities in Active Directory environments by identifying misconfigurations and security weaknesses.

Acquire techniques for exploiting Linux systems and escalating privileges, as well as understanding common vulnerabilities and configurations.

Learn reverse engineering, fuzzing techniques, and binary exploitation to identify and exploit weaknesses in software and applications.

Obtain techniques to navigate through internal networks, gain access to additional systems, and pivot to critical assets during penetration testing.

Develop techniques to find and exploit vulnerabilities in IoT devices and ecosystems.

Learn how to create professional penetration testing reports, communicate findings effectively, and outline actionable post-testing recommendations.

# What AI Skills Do You Learn from the C|PENT$^{AI}$ Program?

- Collect and analyze open-source intelligence (OSINT) for reconnaissance.
- Automate the network scanning process by generating the script and commands using AI tools.
- Identify potential attack surfaces.
- Identify and prioritize vulnerabilities across networks, applications, and systems.
- Perform various attacks on networks, applications, and systems.
- Perform social engineering attacks using AI tools.
- Implement AI-driven tools for brute force and dictionary attacks to crack passwords efficiently.
- Perform Active Directory enumeration.
- Apply AI in reverse engineering to understand binary structures and application flows.
- Utilize AI to automate fuzzing processes to identify software bugs and vulnerabilities.

AI empowers penetration testers by automating repetitive tasks, enhancing accuracy, and uncovering complex security flaws that traditional methods might overlook, leading to:

- Enhanced efficiency
- Real-time threat detection
- Advanced vulnerability analysis
- Customization and scalability

## Supercharge Your Cybersecurity Skills with AI

### Gain the AI Advantage:

**40%** More Efficiency in Cyber Defense

**90%** Accuracy in Detecting Various Cybersecurity Threats

Double your Productivity gains

# Learn **Advanced, Unique** Pentesting Skills with C|PENT[AI]

**Advanced Windows Attacks** – Gain access to an AD forest, bypass PowerShell defenses, and execute attacks like Silver/Golden Ticket and Kerberoasting.

**Attacking IoT Systems** – Identify and exploit IoT devices by extracting and reverse-engineering firmware.

**Advanced Binary Exploitation** – The challenges faced by penetration testers today require them to use their skills to find a flaw in the code. Find vulnerable binaries, reverse engineer them, and write exploits for 32/64-bit programs while bypassing protections

**Bypassing Filtered Networks** – The C|PENT[AI] certification differs from others. It provides web zone challenges that exist within a segmentation architecture. Identify segmentation rules, penetrate web zones, and extract critical data.

**Pentesting Operational Technology (OT)** – As a first in a penetration testing certification, the C|PENT[AI] contains a zone dedicated to ICS SCADA networks. Learn to infiltrate ICS/SCADA networks, manipulate PLC data, and intercept Modbus communication.

**Access Hidden Networks with Pivoting** – Identify filtering rules, penetrate the network, and pivot into hidden segments using single pivoting through a filter. Unlike most certifications, C|PENT[AI] challenges you to pivot across disparate networks and bypass filtering devices. 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.

**Pivoting & Double Pivoting** – Move across hidden networks by identifying filtering rules and manually setting up advanced pivoting techniques. C|PENT[AI] is the first certification in the world that requires you to access hidden networks using double pivoting.

**Privilege Escalation** – The latest methods of privilege escalation are covered. There will also 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.

**Evasion Techniques** – Learn to bypass modern security defenses by weaponizing exploits.

**Attack Automation** – Master scripting for penetration testing with Python, PowerShell, Bash, and Metasploit.

**Weaponizing Exploits** – Build custom tools and develop offensive security strategies.

**Professional Reporting** – Writing pentesting reports is a critical part of the pentesting process. Learn to document findings effectively and provide impactful security recommendations.

# Key Features/Advantages of C|PENT[AI]

## Gain technical pentesting skills:

- 3,000+ pages comprehensive student manual
- 14 modules covering all aspects of penetration testing
- Real-world multi-dimensional testing
- Focus on modern attack vectors

## Practical learning – job-ready skills:

- 110+ advanced labs
- 50+ pen testing tools
- Live cyber ranges (real-world experience)
- Multiple layers of network segmentation
- CTF challenges on pentesting
- Test skills on five multi-disciplinary domains

## AI penetration testing:

- Learn AI tools and techniques for pentesting
- Unique labs to practice AI skills
- AI techniques mapped to all C|PENT[AI]'s pentesting technical domains

## Critical skills beyond technical pentesting:

Any pen test assignment comprises technical knowledge, but a major part of it includes non-technical knowledge, requiring aspects like:

- Scoping the engagement.
- Understanding the design.
- Estimating the effort.
- Presenting findings.

C|PENT[AI] covers the complete pen testing methodology from planning, scoping, and rules of engagement to test execution and the report writing phase of a pen testing assignment.

# Job Roles Mapped to C|PENT$^{AI}$ Certification

1. Penetration Tester
2. Penetration Testing Consultant
3. Penetration Testing Engineer
4. Security Penetration Testing Consultant / Architect
5. Vulnerability Assessment and Penetration Testing (VAPT) Analyst / Engineer
6. QA Security Tester
7. Web Application Penetration Tester
8. Vulnerability Assessment Specialist
9. Red Team - VAPT Security Consultant
10. Penetration Test Lead
11. Network Penetration Testing Engineer
12. Director of Technical Advisor
13. Senior Manual Ethical Hacker
14. Senior API Security Vulnerability Analyst
15. Application Security Engineer (Penetration Tester)
16. Senior Web Application Security Specialist
17. Senior Red Team Operator
18. Cyber Threat Operator
19. Computer Exploitation Test Engineer (Penetration Tester)
20. Security Vulnerability Management Lead
21. Security Lit - AI/ML Security Engineer
22. AI Cyber Security Advisory Engineer
23. Cyber Security Engineer (Generative AI)

# C|PENT[AI] Exam Information

| | | |
|---|---|---|
| **Exam Code** | : | 312-39 |
| **Duration** | : | 24 Hours or Choose 2 Sessions of 12 Hours Each |
| **Report Submission** | : | Submit Pentesting Report within 7 Days of Examination |
| **Test Format** | : | 100% Practical Exam |
| **Dual Certification** | : | Score more than 90% and get one more certification: Licensed Penetration Tester |

# C|PENT[AI] Training Information

**Training: 5 days**

**Training Options**

## iLearn (Self-Study)

An asynchronous, self-study environment delivered in a video-streaming format.

## iWeek (Live Online)

A live, online training course led by an instructor.

## Training Partner (In-Person)

In-person training that enhances learning through peer collaboration.

## Why Do Top Cybersecurity Professionals Love C|PENT[AI] ?

"C|PENT[AI] is very advanced and hard as compared to other certificates. I took the OSCP and CompTIA PenTest exams, but they can't be compared to C|PENT[AI]."

**Hesham Mohamadin**
Cybersecurity Specialist

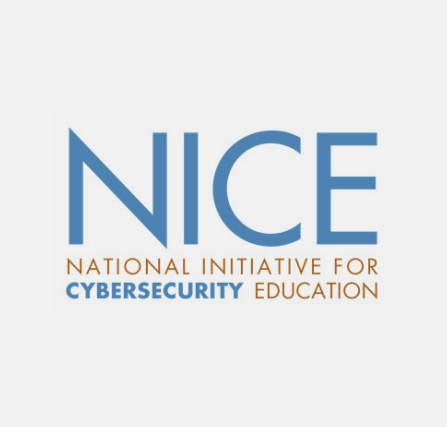
"I regard C|PENT[AI] as the highest certification if you're looking for hands-on experience in cybersecurity and penetration testing."

**Alfred Basta**
Author, Professor, Researcher, 13 books on Cybersecurity, 28 years teaching Cybersecurity

"C|PENT[AI] is a big plus in proper scaling methodology and its processes, which a penetration tester needs. So, this is how C|PENT[AI] adds special value to a portfolio."

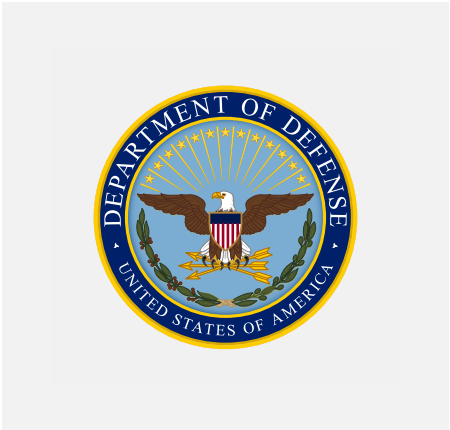
**Malav Parikh**
Cyber Crime Advisor

# EC-Council Recognition, Endorsement, and Mapping











# About EC-Council


EC-Council's sole purpose is to build and redefine the cybersecurity profession globally. We help individuals, organizations, educators, and governments address global workforce problems by developing and curating world-class cybersecurity education programs and their corresponding certifications. We also provide cybersecurity services to some of the largest businesses globally. Trusted by 7 of the Fortune 10, 47 of the Fortune 100, the Department of Defense, the intelligence community, NATO, and over 2,000 of the best universities, colleges, and training companies, our programs have certified people in over 140 countries, and set the bar in the field of cybersecurity education. Best known for the Certified Ethical Hacker (C|EH) program, we are dedicated to equipping over 380,000 information-age soldiers with the knowledge, skills, and abilities required to fight and win against cyber adversaries.

EC-Council builds individual and organization-wide cyber capabilities through our other programs as well, including Certified Secure Computer User (C|SCU), Computer Hacking Forensic Investigator (C|HFI), Certified Network Defender (C|ND), Certified SOC Analyst (C|SA), Certified Threat Intelligence Analyst (C|TIA), Certified Incident Handler (E|CIH), and the Certified Chief Information Security Officer (C|CISO). We are an ANAB ISO/IEC 17024 accredited organization and have earned recognition by the DoD under Directive 8140/8570, in the UK by the GCHQ, CREST, and various other authoritative bodies. Founded in 2001, EC-Council employs over 400 individuals worldwide, with 10 global offices in the U.S., UK, Malaysia, Singapore, India, and Indonesia. Our U.S. offices are in Albuquerque, NM, and Tampa, FL. Learn more at **www.eccouncil.org.**

C|PENT AI

Certified Penetration Testing Professional

WE DON'T JUST TEACH

# PEN TESTING

| | |
|---|---|
| WE BUILD | CYBER CAREERS |
| | TACTICAL LEADERS OF OFFENSIVE SECURITY |