Gain unmatched pentesting skills with the C|PENT ᴬᴵ

The Certified Penetration Testing Professional (CPENT ᴬᴵ) program is the world's most comprehensive guided penetration testing program. It offers a complete hands-on pentesting methodology and AI techniques mapped to all pentesting phases. CPENT ᴬᴵ enables you to master pentesting within an enterprise network environment, evaluating intrusion risks and compiling actionable, structured reports. Distinguish yourself with the CPENT ᴬᴵ, learning beyond technical knowledge—scoping engagements, understanding design, estimating effort, and presenting findings—and thrive as a leader in offensive security with versatile skills. CPENT ᴬᴵ combines guided learning with hands-on practice while immersing you in diverse live scenarios involving IoT systems, segmented networks, and advanced defenses, with practical challenges mapped to each domain. Gain expertise in advanced skills necessary to create your tools, conduct advanced binary exploitation, double pivot, customize scripts, and write your exploits to penetrate the deepest pockets of the network.

- **Hands-on course** featuring CTFs, 110+ labs, live cyber ranges, and 50+ tools
- **Practical exam** tests skills on unique multi-disciplinary network ranges
- **The only program** to teach a complete pen testing methodology
- Prepares you for **VAPT compliance** and various

regulations

Brochure

Course Inquiry

First Name *

Last Name *

Email *

Enter Phone Number*

I would like to inquire for*

Individual

What are you interested in ?*

Cybersecurity Certifications

Which course are you interested in?*

Ethical Hacking

Which degree are you interested in?*

Select Option *

Please let us know how we can help!

By clicking the Submit button below, I hereby agree to the Terms of Use
and Privacy Policy

Submit

What's unique about the C|PENT ^{AI} program

Complete hands-on pentesting methodology

Master comprehensive skills beyond pentesting, including scoping, rules of
engagement, end-to-end methodology, and more.

AI techniques mapped to all pentesting phases

Master AI skills mapped to all pentesting phases, enhancing your efficiency and productivity.

Hands-on course

Build your job-ready skills by immersing yourself in deep practice via CTF challenges, access to 110+ labs, and live cyber ranges.

Unique multi-disciplinary network ranges

Validate and test your skills on five unique multi-disciplinary courses with challenges across every level of the attack spectrum.

Advanced pentest skills

Master advanced Windows and AD attacks, IoT systems, writing exploits, social engineering, writing your scripts, double pivoting, and more.

Collection of templates and cheat sheets

Get access to the largest repository of pentesting scripts, methodology templates, report templates, and tool cheat sheets.

Become a pen tester with AI skills

Lead and advance your offensive security career with AI pentesting skills

Master systematic, versatile pen testing and AI skills to emulate a hacker's movements, identify and exploit vulnerabilities, assess risks, and craft actionable reports to guide organizations in addressing security threats.

Inquire now

99% say pen testing is more crucial as tech evolves (Cobalt).
33.9% highlight an AI skills shortage (O'Reilly).
57% say AI demand exceeds security team capacity (Cobalt).
39% struggle with talent shortages in pen testing (Fortra).

Get AI penetration testing skills

CPENT ^{AI} **opens doors to 23 job roles and is recognized worldwide across industries**
Increase your job opportunities with CPENT ^{AI}

Course information

The Certified Penetration Testing Professional (CPENT ^{AI}) is globally

recognized, offering flexible learning options tailored to fit your schedule and goals. It equips you with the skills necessary for a rewarding career in penetration testing, VAPT, and offensive security.

Course brochure
Certified Penetration Testing Professional (C|PENT ^{AI})
Download

What pentesting skills you'll learn

Engagement Planning & Ethics

The approach to scoping penetration testing engagements, defining objectives, establishing clear communication with stakeholders, and adhering to legal and ethical boundaries.

Information Gathering & Reconnaissance

Open-Source Intelligence (OSINT) techniques for gathering actionable intelligence and identifying, mapping, and analyzing an organization's attack surface.

Social Engineering

The techniques and preventive measures related to exploiting human vulnerabilities through social engineering.

Web & API Security Testing

Web app and API security testing: SQL injection, XSS, authentication flaws, JSON Web Tokens (JWT), testing endpoints and exploiting misconfigurations.

Network & Perimeter Security

Bypassing firewalls and IDS, navigating networks, accessing systems,

pivoting between assets, navigating internal networks, and pivoting to critical assets during penetration testing.

Windows & Active Directory Exploitation

Exploiting Windows vulnerabilities for privilege escalation, and testing and exploiting active directory weaknesses.

Linux Exploitation & Privilege Escalation

Techniques for exploiting Linux systems and escalating privileges while understanding common vulnerabilities and configurations.

Binary Exploitation & Reverse Engineering

Techniques for reverse engineering, fuzzing, and binary exploitation to identify and exploit weaknesses in software and applications.

IoT Security Testing

Techniques to find and exploit vulnerabilities in IoT devices and ecosystems.

Reporting & Post-Testing Actions

Creating professional penetration testing reports, communicating findings effectively, and outlining actionable post-testing recommendations.

What AI skills you'll learn

AI empowers you by automating repetitive tasks, enhancing accuracy, and uncovering complex security flaws that traditional methods might overlook. Here are some key skills and benefits:

Enhanced efficiency	Improved accuracy
Real-time threat detection	Advanced vulnerability analysis
Customization and scalability	Up to 40% more efficiency in cyber defense
90% accuracy in detecting various cybersecurity threats	2X productivity gains

Course outline

Advanced pentesting skills

Practice ranges

Who is it for?

Cybersecurity professionals

Drive your cybersecurity career forward with CPENT ^{AI}, enhanced by the power of AI

Teams and Organizations

Turbocharge you team's knowledge with certified expertise

Government and military

Trusted and highly valued globally by government departments and defense organizations

Educators

Create and grow your cybersecurity courses and programs

Trusted worldwide

Earn world-class certifications trusted and highly valued globally by government bodies, private organizations, and the defense.

Advance your career with our expert guidance.

"

"CPENT 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 CPENT"

Hesham Mohamadin

Cybersecurity Specialist

"

"

"I regard CPENT 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

"

"

"CPENT is a big plus in proper scaling methodology and its processes, which a penetration tester needs. So, this is how CPENT adds special value to a portfolio."

Malav Parikh

Cyber Crime Advisor

"

Get advice

Schedule your consultation today and start achieving your goals

Inquire now

FAQs

CPENT ^{AI} Program

CPENT ^{AI} Certification

CPENT ^{AI} Training

VAPT / Penetration Testing

*For more details on Certification Policies & FAQ's please refer to our
Certification Website

Top Courses

Discover our most popular certifications and see for yourself why participants rate them so highly.

Certified Ethical Hacker
Master the core domains of cybersecurity with the world's No.1 ethical hacking program, now with the power of AI.

View Course

Certified Chief Information Security Officer
The industry-leading certification to train professionals to succeed at the highest executive levels of the security industry.
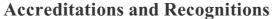
View Course

Computer Hacking Forensic Investigator
Gain the knowledge to perform effective digital forensics investigations and bring your organization into a state of forensic readiness.

View Course

Looking for something else?
EC-Council has many high-profile certifications, all recommended by leading organizations in the cybersecurity industry.

Accreditations and Recognitions

EC-Council is recommended and endorsed by leading organisations and government bodies in the cybersecurity industry.

American Council on Education

A membership organization that leads higher education.

ANSI National Accreditation board

Providing accreditation services in over 75 countries and is the largest accreditation body in North America

Army Credentialing Assistance

Helps Army Soldiers with full tuition and exam cost coverage for certifications.

National Initiative for Cybersecurity Education

A partnership between government, academia, and the private sector focused on cybersecurity education, training, and workforce development.

EC-Council was formed in 2001 after very disheartening research following the 9/11 attack on the World Trade Center. Founder and CEO of the EC-Council Group, Jay Bavisi, after watching the attacks unfold, raised the question, what if a similar attack were to be carried out on the cyber battlefield? Read More…

CAREER TRACKS

TRENDING CERTIFICATIONS

CUSTOMER SERVICE

COMPANY

Partner With Us

Legal