Training: EC-Council
# CPENT - Certified Penetration Testing Professional v2

EC-Council
Building A Culture Of Security

## TRAINING GOALS:

Gain unmatched pentesting skills with the CPENT - Certified Penetration Testing Professional v2 - CPENT$^{AI}$. The Certified Penetration Testing Professional (CPENT$^{AI}$) program is the world's most comprehensive guided penetration testing program. CPENT$^{AI}$ enables you to master pen-testing from small, medium, and up to enterprise network environments, evaluating intrusion risks and compiling actionable, structured reports. Master scoping engagements, understanding design, estimating effort, and presenting findings. CPENT$^{AI}$ also 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.

Skills you will gain with CPENT$^{AI}$:

- 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.



Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- 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.

AI Skills you learn from the CPENT$^{AI}$ 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.

Who is CPENT$^{AI}$ for?

- Any cybersecurity professional looking to expand their knowledge in the field of defensive security.
- Penetration Tester
- Penetration Testing Consultant
- Penetration Testing Engineer
- Security Penetration Testing Consultant / Architect
- Vulnerability Assessment and Penetration Testing (VAPT) Analyst / Engineer
- QA Security Tester
- Web Application Penetration Tester
- Vulnerability Assessment Specialist
- Red Team - VAPT Security Consultant
- Penetration Test Lead



Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Network Penetration Testing Engineer
- Director of Technical Advisor
- Senior Manual Ethical Hacker
- Senior API Security Vulnerability Analyst
- Application Security Engineer (Penetration Tester)
- Senior Web Application Security Specialist
- Senior Red Team Operator
- Cyber Threat Operator
- Computer Exploitation Test Engineer (Penetration Tester)
- Security Vulnerability Management Lead
- Security Lit - AI/ML Security Engineer
- AI Cyber Security Advisory Engineer
- Cyber Security Engineer (Generative AI)

*Each participant in an authorized training CPENT - Certified Penetration Testing Professional v2 held in Compendium CE will receive a free CPENT v2 certification exam voucher.*

## CONSPECT:

- Module 1 - Introduction to Penetration Testing and Methodologies
  - Principles and objectives of penetration testing
  - Penetration testing methodologies and frameworks
  - Best practices and guidelines for conducting penetration tests
  - The role of Artificial Intelligence in penetration testing
  - Penetration testing for compliance with laws, regulations, and standards
  - Key topics covered
    - Penetration testing fundamentals, penetration testing process, methodologies and frameworks (including MITRE ATT&CK), characteristics of an effective penetration test, AI-driven penetration testing, AI-powered tools for penetration testing, compliance-focused penetration testing, and the role of AI and machine learning in compliance-driven testing.
- Module 2 - Penetration Testing Scoping and Engagement
  - Pre-engagement activities for penetration testing
  - Key elements for responding to penetration testing RFPs



Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Drafting effective Rules of Engagement (ROE)
- Legal and regulatory considerations critical to penetration testing
- Resources and tools for successful penetration testing
- Strategies to effectively manage scope creep
- Key topics covered
  - Proposal preparation, Rules of Engagement, drafting ROE, creating penetration testing contracts, rules of behavior, nondisclosure agreements, liability considerations, engagement letters, kickoff meetings, statements of work, test plan preparation, data use agreements, mission briefings, and managing scope creep.

- Module 3 - Open-Source Intelligence (OSINT)
  - Collect OSINT on the target's domain name
  - Gather OSINT about the target organization from the web
  - Perform OSINT on the target's employees
  - Utilize automation tools for OSINT
  - Map the attack surface
  - Labs
    - Collect OSINT on the target's domain name, web presence, and employees
    - Use automation tools for OSINT collection
    - Identify and map the attack surface
  - Key topics covered
    - Finding domains and subdomains, WHOIS lookups, DNS records, reverse lookups, DNS zone transfers, advanced web searches using operators, Google Dorking, footprinting with Shodan, email harvesting, people search services, automating OSINT processes with tools and frameworks, attack surface mapping, traceroute analysis, scanning target networks, discovering live hosts, port scanning, OS banner grabbing, and service fingerprinting.

- Module 4 - Social Engineering Penetration Testing
  - Core concepts of social engineering penetration testing
  - Off-site social engineering penetration testing
  - On-site social engineering penetration testing
  - Document findings and provide countermeasure recommendations
  - Labs
    - Capture credentials using the Social-Engineer Toolkit (SET)
  - Key topics covered
    - Social engineering penetration testing process, off-site social engineering testing, phishing attacks, social engineering via phone, social engineering using AI and machine learning, on-site social engineering penetration testing, and social engineering countermeasures.



Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Module 5 - Web Application Penetration Testing
  - Web application footprinting and enumeration techniques
  - Methods for web vulnerability scanning
  - Testing for vulnerabilities in application deployment and configuration
  - Techniques to assess identity management, authentication, and authorization mechanisms
  - Evaluate session management security
  - Assess input validation mechanisms
  - Detect and exploit SQL injection vulnerabilities
  - Techniques for identifying and testing injection vulnerabilities
  - Exploit improper error handling vulnerabilities
  - Identify weak cryptographic implementations
  - Test for business logic flaws in web applications
  - Evaluate applications for client-side vulnerabilities
  - Labs
    - Perform website footprinting
    - Conduct web vulnerability scanning using AI
    - Execute various attacks on target web applications
  - Key topics covered
    - OWASP Penetration Testing Framework, website footprinting, web spidering, website mirroring, HTTP service discovery, web server banner grabbing, testing for default credentials, enumerating web server directories, web vulnerability assessment, web application fuzz testing, directory brute forcing, web vulnerability scanning, test handling of file extensions, test backup and unreferenced files, username enumeration, authorization attacks, insecure access control methods, session token sniffing, session hijacking, cross-site request forgery (XSRF), URL parameter tampering, SQL injection, LDAP injection, improper error handling, logic flaws, and frame injection.
- Module 6 - API and JSON Web Token Penetration Testing
  - Techniques and tools for performing API reconnaissance
  - Test APIs for authentication and authorization vulnerabilities
  - Assess the security of JSON Web Tokens (JWT)
  - Test APIs for input validation and injection vulnerabilities
  - Identify and exploit security misconfiguration vulnerabilities in APIs
  - Test APIs for rate limiting and denial-of-service (DoS) weaknesses
  - Evaluate the security of GraphQL implementations
  - Test APIs for business logic flaws and session management issues
  - Labs
    - Perform API reconnaissance using AI



Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

        - Scan and identify vulnerabilities in APIs
        - Exploit various API vulnerabilities to gather information about the target application
    - Key topics covered
        - API reconnaissance, testing APIs for broken authentication, object-level permission flaws (BOLA), JWT security issues, SQL injection in APIs, cross-site scripting (XSS) in APIs, fuzzing API inputs, API vulnerability scanning, abuse of API resource consumption, throttling and rate-limiting attacks, GraphQL security issues, workflow circumvention in APIs, and API session hijacking.
- Module 7 - Perimeter Defense Evasion Techniques
    - Techniques to evaluate firewall security implementations
    - Techniques to assess IDS (Intrusion Detection System) security implementations
    - Methods to evaluate the security of routers
    - Methods to evaluate the security of switches
    - Labs
        - Identify and bypass a firewall
        - Evade perimeter defenses using the Social-Engineer Toolkit (SET)
        - Perform WAF (Web Application Firewall) fingerprinting
    - Key topics covered
        - Testing firewalls, locating firewalls, enumerating firewall access control lists, scanning firewalls for vulnerabilities, bypassing firewalls, IDS penetration testing, techniques for evading IDS systems, testing IDS using different methods, bypassing IDS, router testing issues, port scanning routers, testing for router misconfigurations, identifying security misconfigurations in switches, testing OSPF performance, and auditing router and switch security.
- Module 8 - Windows Exploitation and Privilege Escalation
    - Windows penetration testing methodology
    - Techniques for performing reconnaissance on Windows targets
    - Methods for vulnerability assessment and exploit verification
    - Approaches to gain initial access to Windows systems
    - Techniques for enumeration with user-level privileges
    - Methods for privilege escalation
    - Post-exploitation activities
    - Labs
        - Exploit Windows OS vulnerabilities
        - Exploit and escalate privileges on a Windows operating system
        - Gain access to a remote system
        - Exploit buffer overflow vulnerabilities on a Windows machine
    - Key topics covered
        - Reconnaissance on Windows, Windows vulnerability scanning, gaining access to



Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

Windows systems, vulnerability scanning and exploit suggestions using AI, password cracking, remote shell access, exploiting buffer overflow vulnerabilities on Windows, Meterpreter post-exploitation techniques, privilege escalation, UAC bypass, antivirus evasion, disabling Windows Defender, setting up backdoors at boot, and evading antivirus detection.

- Module 9 - Active Directory Penetration Testing
  - Architecture and key components of Active Directory
  - Techniques for Active Directory reconnaissance
  - Methods for Active Directory enumeration
  - Exploiting identified Active Directory vulnerabilities
  - Role of Artificial Intelligence in Active Directory penetration testing strategies
  - Labs
    - Explore and analyze the Active Directory environment
    - Perform Active Directory enumeration
    - Execute horizontal privilege escalation and lateral movement
    - Retrieve cached Active Directory credentials
  - Key topics covered
    - Active Directory fundamentals, AD components, reconnaissance techniques, enumeration of Active Directory, Active Directory Service Interfaces (ADSI), enumeration tools, password spraying attacks, Active Directory Certificate Services (AD CS), Exchange Server user enumeration, exploiting Exchange Server, extracting password hashes, cracking NTLM hashes, Active Directory exploitation, and AI-driven Active Directory enumeration.
- Module 10 - Linux Exploitation and Privilege Escalation
  - Linux exploitation and penetration testing methodologies
  - Techniques for Linux reconnaissance and vulnerability scanning
  - Methods to gain initial access to Linux systems
  - Linux privilege escalation techniques
  - Labs
    - Perform reconnaissance and vulnerability assessment on Linux
    - Gain access and perform enumeration
    - Identify misconfigurations for privilege escalation
  - Key topics covered
    - Linux penetration testing, Linux vulnerability scanning, privilege escalation techniques, reconnaissance on Linux systems, enumeration methods, exploiting misconfigurations, password cracking, remote shell access, buffer overflow exploitation on Linux, post-exploitation strategies, and persistence mechanisms.
- Module 11 - Reverse Engineering, Fuzzing, and Binary Exploitation
  - Concepts and methodologies for analyzing Linux binaries



Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Techniques for examining Windows binaries
- Buffer overflow attacks and exploitation methods
- Principles, methodologies, and tools for application fuzzing
- Labs
  - Perform binary analysis
  - Explore binary analysis methodologies
  - Write exploit code
  - Reverse engineer a binary
  - Identify and debug stack buffer overflows
  - Fuzz an application
- Key topics covered
  - Machine instructions, 32-bit assembly, ELF binaries, IA-32 instructions for penetration testing, binary analysis methodologies, Capstone framework, static analysis, dynamic analysis, x86 C programs, buffer overflow, heap overflow, memory corruption exploits, cross-compiling binaries, fuzzing techniques, fuzzing steps, types of fuzzers, debugging, fuzzing tools, and building custom fuzzers.

- Module 12 - Lateral Movement and Pivoting
  - Advanced techniques for lateral movement within networks
  - Advanced pivoting and tunneling methods to maintain access
  - Labs
    - Perform pivoting
    - Execute DNS tunneling and HTTP tunneling
  - Key topics covered
    - Lateral movement strategies, Pass-the-Hash (PtH) attacks, Pass-the-Ticket (PtT) attacks, Kerberos attacks, Silver Ticket and Golden Ticket attacks, Kerberoasting, PsExec and Metasploit Framework for lateral movement, Windows Remote Management (WinRM) for lateral movement, cracking RDP, pivoting techniques and tools, HTTP tunneling, DNS tunneling, ICMP tunneling, SSH tunneling, and port forwarding.

- Module 13 - IoT Penetration Testing
  - Fundamental concepts of IoT penetration testing
  - Information gathering and attack surface mapping
  - Analyze IoT device firmware
  - In-depth analysis of IoT software
  - Assess the security of IoT networks and protocols
  - Post-exploitation strategies and persistence techniques
  - Comprehensive penetration testing reports
  - Labs
    - Perform IoT firmware acquisition, extraction, analysis, and emulation



Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

        - Probe IoT devices
    - Key topics covered
        - IoT penetration testing, OWASP Top 10 IoT threats, OWASP IoT attack surface areas, IoT penetration testing methodology, identifying IoT devices, firmware analysis, extracting firmware images, firmware extraction, reverse engineering firmware, static and dynamic binary analysis, IoT software analysis, IoT network and protocol security testing, network traffic analysis between devices, gateways, and servers, privilege escalation techniques in IoT, lateral movement techniques within IoT networks, and IoT penetration testing report preparation.
- Module 14 - Report Writing and Post-Testing Actions
    - Purpose and structure of a penetration testing report
    - Essential components of a penetration testing report
    - Phases of penetration test report writing
    - Skills to deliver a penetration testing report effectively
    - Post-testing actions for organizations
    - Labs
        - Generate penetration testing reports
    - Key topics covered
        - Characteristics of a good penetration testing report, report components, phases of report development, writing a draft report, report writing tools, delivering the penetration testing report, report retention, destroying the report, sign-off documentation, developing and implementing a data backup plan, conducting training, retesting, and validation.

## REQUIREMENTS:

Recommended:

- A minimum of 2 years of experience in IT or cybersecurity
- Knowledge of fundamental concepts in networking, operating systems (Windows/Linux), and security
- Holding a **CEH (Certified Ethical Hacker)** certification or equivalent practical knowledge

## Difficulty level

## CERTIFICATE:

The participants will obtain certificates signed by EC-Council (course completion). This course will help prepare you also for the CPENT v2 (CPENT$^{AI}$) certification exam.



Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

CPENT v2 exam details:

- 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

*Each participant in an authorized training CPENT - Certified Penetration Testing Professional v2 held in Compendium CE will receive a free CPENT v2 certification exam voucher.*

## TRAINER:

Certified EC-Council Instructor (CEI)

## ADDITIONAL INFORMATION:

The training materials include official EC-Council electronic courseware, CPENT Cyber Range for 90 Days and iLabs for 180 Days, and an exam voucher.



Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007