Training: EC-Council
CEH - Certified Ethical Hacker v13

EC-Council
Building A Culture Of Security

## TRAINING GOALS:

C|EH Certified Ethical Hacker

The Certified Ethical Hacker (C|EH®) is an industry-renowned, globally recognized credential. In its 13th version, the C|EH® comes with AI capabilities.

- **AI-powered**
  - The world's first ethical hacking program to harness the power of AI.
- **Hands-on experience**
  - Cybersecurity professionals can hone their skills in real-world scenarios through hands-on labs. Here, they'll practice attack vectors and master advanced hacking tools.
- **40% more efficient**
  - Learn AI-driven techniques to boost 40% more efficiency in cyber defense while streamlining workflows.
- **Power-packed, updated curriculum**
  - Master the latest advanced attack techniques, trends and countermeasures.
- **2x productivity gains**
  - Advanced threat detection, enhanced decision making, adaptive learning, enhanced reporting and automation of repetitive tasks.
- **Real-world skills, proven mastery**
  - Participate in monthly global hacking competitions, compete with peers, and make it onto the leaderboard.

CEH's exclusive learning framework, Learn | Certify | Engage | Compete, prepares learners for



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

certification and provides in-depth, practical exercises that make it the most comprehensive cybersecurity program available.

- **Learn**
  - Develop skills in core domains of cybersecurity with over 20 modules. Learners will experience 220+ hands-on labs, 550 attack techniques and over 4,000 hacking and security tools.
- **Certify**
  - Take a 4-hour exam with 125 multiple-choice questions and a 6-hour practical exam with 20 real-life challenges to earn the CEH Master certification in CEH v13.
- **Engage**
  - Take part in a mock ethical hacking engagement. This 4-part security engagement gives learners the opportunity to engage in a real ethical hacking engagement experience from start to finish against an emulated organization.
- **Compete**
  - Compete with peers globally with year-long access to 12 CTF challenges of 4 hours each. This helps learners level up their skills and stay current on latest trends.

*Each participant in an authorized training CEH - Certified Ethical Hacker v13 held in Compendium CE will receive a free CEH (MCQ) certification exam voucher. And in the case of the Elite version, also a voucher for the CEH (Practical) exam and access to all four learning components: Learn | Certify | Engage | Compete.*

## Who CEH v13 is for:

- **Cybersecurity professionals**
  - Those looking to drive their cybersecurity career forward with the power of AI.
- **Teams and organizations**
  - Teams looking to turbocharge their AI knowledge in order to stay one step ahead of malicious actors.
- **Government and military**
  - Government departments and defense bodies looking for a trusted and highly valued global certification partner.



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

## CEH Recognition / Endorsement / Mapping:

- American Council of Education (ACE)
- ANSI National Accreditation Board (ANAB)
- DoD Cyber Workforce Qualification Program
- Army Credentialing Assistance
- National Initiative for Cybersecurity Education (NICE)

## CONSPECT:

The CEH v13 training program includes 20 modules covering various technologies, tactics, and procedures, providing prospective ethical hackers with the core knowledge needed to thrive in cybersecurity. Every tactic discussed in training is backed by step-by-step labs conducted in a virtualized environment with live targets, live tools, and vulnerable systems.

- Module 1 - Introduction to Ethical Hacking
  - Cover the fundamentals of key issues in the information security world, including the basics of ethical hacking, information security controls, relevant laws, and standard procedures.
- Module 2 - Foot Printing and Reconnaissance
  - Learn how to use the latest techniques and tools to perform foot printing and reconnaissance, a critical pre-attack phase of the ethical hacking process.
- Module 3 - Scanning Networks
  - Learn different network scanning techniques and countermeasures.
- Module 4 - Enumeration
  - Learn various enumeration techniques, such as Border Gateway Protocol (BGP) and Network File Sharing (NFS) exploits, and associated countermeasures.
- Module 5 - Vulnerability Analysis
  - Learn how to identify security loopholes in a target organization’s network, communication infrastructure, and end systems. Different types of vulnerability assessment and vulnerability assessment tools.
- Module 6 - System Hacking
  - Learn about the various system hacking methodologies—including steganography, steganalysis attacks, and covering tracks—used to discover system and network vulnerabilities.
- Module 7 - Malware Threats



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

- Learn different types of malware (Trojan, virus, worms, etc.), APT and fileless malware, malware analysis procedure, and malware countermeasures.

- Module 8 - Sniffing
  - Learn about packet-sniffing techniques and how to use them to discover network vulnerabilities, as well as countermeasures to defend against sniffing attacks.
- Module 9 - Social Engineering
  - Learn social engineering concepts and techniques, including how to identify theft attempts, audit human-level vulnerabilities, and suggest social engineering countermeasures.
- Module 10 - Denial-of-Service
  - Learn about different Denial of Service (DoS) and Distributed DoS (DDoS) attack techniques, as well as the tools used to audit a target and devise DoS and DDoS countermeasures and protections.
- Module 11 - Session Hijacking
  - Understand the various session hijacking techniques used to discover network-level session management, authentication, authorization, and cryptographic weaknesses and associated countermeasures.
- Module 12 - Evading IDS, Firewalls, and Honeypots
  - Get introduced to firewall, intrusion detection system (IDS), and honeypot evasion techniques; the tools used to audit a network perimeter for weaknesses; and countermeasures.
- Module 13 - Hacking Web Servers
  - Learn about web server attacks, including a comprehensive attack methodology used to audit vulnerabilities in web server infrastructures and countermeasures.
- Module 14 - Hacking Web Applications
  - Learn about web application attacks, including a comprehensive web application hacking methodology used to audit vulnerabilities in web applications and countermeasures.
- Module 15 - SQL Injection
  - Learn about SQL injection attacks, evasion techniques, and SQL injection countermeasures.
- Module 16 - Hacking Wireless Networks
  - Understand different types of wireless technologies, including encryption, threats, hacking methodologies, hacking tools, Wi-Fi security tools, and countermeasures.
- Module 17 - Hacking Mobile Platforms
  - Learn Mobile platform attack vector, android and iOS hacking, mobile device management, mobile security guidelines, and security tools.
- Module 18 - IoT and OT Hacking
  - Learn different types of Internet of Things (IoT) and Operational Technology (OT) attacks, hacking methodology, hacking tools, and countermeasures.
- Module 19 - Cloud Computing



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

- Learn different cloud computing concepts, such as container technologies and server less computing, various cloud computing threats, attacks, hacking methodology, and cloud security techniques and tools.

- Module 20 - Cryptography
  - Learn about encryption algorithms, cryptography tools, Public Key Infrastructure (PKI), email encryption, disk encryption, cryptography attacks, and cryptanalysis tools.

## REQUIREMENTS:

The training course does not require previous cybersecurity experience.

## Difficulty level

## CERTIFICATE:

The participants will obtain certificates signed by EC-Council (course completion). This course will help prepare you also for the CEH (MCQ Exam) and CEH (Practical) certification exams.

**CEH (MCQ Exam)**

The Certified Ethical Hacker (CEH) credential is trusted globally as the industry standard for evaluating one's understanding of ethical hacking and security testing. As an ANAB 17024 accredited examination, the 150-question, 4-hour proctored exam is recognized across the globe as the original and most trusted tactical cyber security certification for ethical hackers. Certification domains are carefully vetted through industry practitioners, ensuring the certification maps to current industry requirements; this exam undergoes regular psychometric evaluation and tuning to ensure a fair and accurate measure of the candidate's knowledge in the ethical hacking domain.

**CEH (Practical)**

The CEH Practical exam is an ANAB ISO/IEC 17024 accredited. The CEH Practical is a 6-hour, 100% hands-on exam delivered in our Cyber Range that requires you to demonstrate the skills and abilities of ethical hacking techniques such as:

- Port scanning tools (e.g., Nmap, Hping)
- Vulnerability detection
- Attacks on a system (e.g., DoS, DDoS, session hijacking, web server and web application attacks, SQL injection, wireless threats)
- SQL injection methodology and evasion techniques



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

- Web application security tools (e.g., Acunetix WVS)
- SQL injection detection tools (e.g., IBM Security AppScan)
- Communication protocols

This is the next step to becoming a CEH Master after you have achieved your CEH certification. Within the CEH Practical, you have limited time to complete 20 challenges to test your skills and proficiency in a performance-based cyber range. This exam is NOT a simulation and incorporates a live corporate network of VMs and applications with solutions to uncover vulnerabilities.

**CEH Master**

Upon completing the CEH (Master) program, consisting of the CEH and CEH (Practical), the CEH (Master) designation is awarded. CEH Masters have shown proficiency at a master level in the knowledge, skills, and abilities of ethical hacking with a total of 10 hours of testing to prove their competency. The top 10 performers in both CEH and CEH Practical exams are featured on the CEH Master Global Ethical Hacking Leader Board.

| Exam Details | CEH (MCQ Exam) | CEH (Practical) |
|---|---|---|
| Number of Questions/Practical Challenges | 125 | 20 |
| Test Duration | 4 Hours | 6 Hours |
| Test Format | Multiple Choice Questions | iLabs Cyber Range |
| Test Delivery | ECC EXAM, VUE | - |
| Availability | - | Aspen-iLabs |
| Exam Prefix | 312-50 (ECC EXAM), 312-50 (VUE) | - |
| Passing Score | Refer to https://cert.eccouncil.org/faq.html | |

*Each participant in an authorized training CEH - Certified Ethical Hacker v13 held in Compendium CE will receive a free CEH (MCQ) certification exam voucher. And in the case of the Elite version, also a voucher for the CEH (Practical) exam and access to all four learning components: Learn | Certify | Engage | Compete.*

## TRAINER:

Certified EC-Council Instructor (CEI)



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

## ADDITIONAL INFORMATION:

Although all available versions of the CEHv13 course materials (Lite and Elite) have full access to eCourseware and include a CEH (MCQ) exam voucher, the Elite version offers several additional features and educational materials that allow for deeper knowledge and even more practical experience.

| Package Inclusions | C\|EH- Elite v13 | C\|EH v13 |
|---|---|---|
| eCourseware* | 2 years | 2 years |
| Exam Voucher**(non-RPS) | 1 year | 1 year |
| Exam Retakes*** (non-RPS) | 1 | x |
| Ethical Hacking Videos* | 1 year | 1 year |
| EC-Council Labs* | 6 months | x |
| C\|EH Engage* | 1 year | x |
| Global C\|EH Challenge* | 1 year | x |
| C\|EH Practical**** | 1 year | x |

* Valid from the date of activation.

**Exam Voucher- Valid for 1 year from the date of evaluation submission. (non-RPS)

***Maximum 1 retake allowed per year as per exam retake policy. Exam Retake Policy https://cert.eccouncil.org/exam-retake-policy.html

****CEH Practical dashboard shall be activated upon clicking on "Ok Proceed" within the exam dashboard.

**Package- Terms & Conditions**:

1. The exam retakes shall be governed in accordance with the Exam Retake Policy. For more details, please visit Exam Retake Policy https://cert.eccouncil.org/exam-retake-policy.html
2. Exam Retakes shall be applicable on CEH (ANSI) exam only and not CEH (Practical) and cannot be exchanged.
3. A maximum of 1 exam reattempt is permitted in a period of 1 year for C|EH Elite package.
4. Package downgrade from C|EH Elite to any other title is not permitted.
5. C|EH v13 used kits will not be upgraded to C|EH Elite package.



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

6. Packages once sold are non-refundable.
7. There are 10 Ethical Hacking Video Courses available on C|EH Elite package.
8. All package components shall be activated automatically upon single code redemption.
9. Global C|EH Challenge and C|EH Engage cannot be purchased separately as standalone components.
10. No two offers can be clubbed together or exchanged in lieu of any other products/offerings.



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