training code: CEHv13 Lite / ENG DL 5d / EN

Certified Ethical Hacker CEH v.13 AI

As per the latest ongoing trends in IT Industries and to meet the growing demand for new skills and knowledge about cybersecurity, EC-Council has developed the Certified Ethical Hacker training. An unconventional approach to thinking about the companies infrastructure from an intruders perspective is an extremely effective learning mechanism that opens the eyes to many often neglected areas of our work. Although it is an "entry-level" course, CEH contains a lot of material and practical exercises which also touches upon very technically advanced aspects of IT.

From the creators of Certified Ethical Hacker (CEH) comes the new and evolved version 13 with added AI capabilities. Structured across 20 learning modules covering over 550 attack techniques, CEH provides cybersecurity professionals with the core knowledge they need to detect and defend against emerging threats.

CEH offers a balanced blend of knowledge-based training and hands-on labs. This all takes place in a virtual environment with live targets as well as the latest in AI tools, techniques and systems.

- 100% visualization with full access to pre-configured targets,networks, and attack tools
- Pre-configured vulnerable websites
- Vulnerable, unpatched operating systems
- Fully networked environments
- 4000+ hacking tools
- Wide range of target platforms to hone your skills
- 550 attack techniques covered
- Objective-oriented flags for critical thinking and applied knowledge assessment
- Cloud-based cyber range

Training recipients

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.

Benefits

The ethical hacker's goal is to identify the weaknesses of their organization and help find an effective method of defence against such attacks on corporate systems. Course participants make controlled intrusions into the "target" system and gain practical skills on how to effectively protect the network. While conventional security measures are essential, it is important to gain the perspective of the cybercriminals who could potentially compromise the systems. During exercises, everyone will get acquainted with many tools used by security specialists.
Students will learn how to :

- define and characterize the most important techniques of attacks used by hackers
- carry out a reconnaissance about your own company or competition
- scan, test and break system security
- identify and analyse vulnerabilities in the organization
- recognize and prevent authority escalation methods in systems
- create better intrusion detection policies on IDS / IPS devices
- recognize social engineering used by criminals
- create viruses, hack mobile devices, smartphones
- analyse malware
- identify the potential of threats from the "Internet of Things" (IoT) and how to protect against them
- identify challenges for industrial networks and the impact of cybersecurity on OT (Operational Technology) concepts
- characterize the most important elements of container systems (Docker, Kubernetes)
- verify the security of cloud solutions such as AWS
- recognize subtle differences between backdoors, Trojans, and other threats
- ultimately, they will be able to make company employees more aware of information security issues

CEH v13 will equip individuals and teams with:

- In-depth knowledge of ethical hacking methodologies and practices, augmented with AI techniques

- The skills to integrate AI across ethical hacking phases: reconnaissance, scanning, gaining access, maintaining access, and covering tracks
- AI techniques to automate tasks, boost efficiency, and detect sophisticated threats beyond traditional methods
- Tools that will utilize AI for proactive threat hunting, anomaly detection, and predictive analysis to prevent cyber-attacks

Training program

1. Introduction to Ethical Hacking
2. Foot Printing and Reconnaissance
3. Scanning Networks
4. Enumeration
5. Vulnerability Analysis
6. System Hacking
7. Malware Threats
8. Sniffing
9. Social Engineering
10. Denial-of-Service
11. Session Hijacking
12. Evading IDS, Firewalls, and Honeypots
13. Hacking Web Servers
14. Hacking Web Applications
15. SQL Injection
16. Hacking Wireless Networks
17. Hacking Mobile Platforms
18. IoT Hacking
19. Cloud Computing
20. Session Hijacking

Expected preparation of the participant

Basic knowledge of Windows and Linux is required. Basic understanding of network essentials, core concepts including server and network components (basic knowledge of TCP/IP communication, services such as DNS/DHCP, the understanding concept of IP addressing). We recommend at least 2 years of experience in the IT industry.

Training Includes

- 5 days with instructor training
- Trainer’s supervision

The table below lists the components that participants receive based on the version of the training they purchased.

Language

- Training: English
- Materials: English

Duration

5 days / 40 hours

Examination method

Knowledge-Based Exam 312-50 (ECC Exam) can be taken at authorized EC-Council exam centers.
Title: Certified Ethical Hacker
Test Format: Multiple-choice questions
Number of Questions: 125
Duration: 4 hours
Note: When taking the CEH exam online with remote proctoring, there is an additional fee of $100 USD net. This cost covers hiring a proctor for the exam, and the purchase is made individually on the vendor's website: https://store.eccouncil.org/product/voucher-upgrade-rps-to-vue/

——

Additionally, when purchasing the Elite training package:
Practical Exam
Test Format: Scenario-based questions
Number of Questions: 20 scenarios
Duration: 6 hours.