

EC-Council – Certified Ethical Hacker (CEHv13 EN)

EC-Council – Certified Ethical Hacker (CEH version 13)



The World's No. 1 Ethical Hacking
Certification for 20 Years

3a Kypca:

What is C|EH® v13?

By joining the AI Revolution as a Certified Ethical Hacker, you'll gain the expertise to navigate the cutting-edge world of cybersecurity.

Certified Ethical Hackers, trained in the latest version of CEH v13, are equipped with AI-powered tools and techniques to identify, exploit, and secure vulnerabilities in systems and networks. You'll learn to leverage AI for automating threat detection, predicting security breaches, and responding swiftly to cyber incidents. Moreover, you'll also gain the

skills needed to secure AI-driven technologies against potential threats. This combination of ethical hacking and AI capabilities will place you at the forefront of cybersecurity, ready to defend organizations across industries from advanced threats and adapt to evolving challenges. Amplify Your Edge as a Certified Ethical Hacker Powered by AI Capabilities:

Advanced Knowledge: As a Certified Ethical Hacker powered by AI, you'll possess in-depth knowledge of ethical hacking methodologies, enhanced with cutting-edge AI techniques.

AI Integration: You'll effectively integrate AI across every phase of ethical hacking, from reconnaissance and scanning to gaining access, maintaining access, and covering your tracks.

Automation and Efficiency: You'll leverage AI to automate tasks, boost efficiency, and detect sophisticated threats that traditional methods might overlook.

Proactive Defense: With AI at your disposal, you'll be equipped for proactive threat hunting, anomaly detection, and predictive analysis to prevent cyber-attacks before they happen.

20 Modules That Help You Master the Foundations of Ethical Hacking and Prepare to Take the C|EH Certification Exam.

Develop a Hacker's Mindset: Master the 5 Phases of Ethical Hacking and Gain AI Skills to Automate Them

1. Reconnaissance | Learn to gather essential information about your target
2. Vulnerability Scanning | Gain the ability to identify weaknesses in the target system
3. Gaining Access | Learn how to actively exploit identified vulnerabilities
4. Maintaining Access | Develop skills to maintain continued access to the target systems
5. Clearing Tracks | Master the art of erasing any trace of

your activities

The CEH v13 is a specialized, one-of-a-kind training program that helps you gain expertise in ethical hacking, AI, and machine learning. With hands-on training labs, knowledge-based and practical exams, a mock ethical hacking engagement on live networks, and a global hacking competition, this program ensures you master the most in-demand skills needed to excel and stand out in the cybersecurity industry. This learning framework offers not only a comprehensive training program to prepare you for the certification exam but also the industry's most robust, in-depth, hands-on lab and practice range experience.

1. C|EHv13 Learn

With 20 cutting-edge modules, you'll gain the core skills needed to dominate the cybersecurity landscape.

CEH isn't just keeping pace—it's leading the charge, evolving with the latest operating systems, exploits, tools, and hacking techniques to ensure you're always ahead of the curve.

Dive deep into the future of cybersecurity with training that integrates AI into all five phases of ethical hacking, reconnaissance and scanning to gaining access, maintaining access, and covering tracks. You'll harness the power of AI to supercharge your hacking techniques and disrupt AI systems—giving you 10x efficiency in your cybersecurity role.

CEH v13 isn't just a certification; it's a fully immersive experience. CEH combines comprehensive knowledge-based training with immersive hands-on labs to ensure a well-rounded learning experience.

You'll engage with live targets, tools, and vulnerable systems

in a controlled environment, building real-world skills that empower you to confidently apply your expertise in any scenario.

Get ready to transform the way you hack and protect the digital world!

2. C|EHv13 Certify

The Certified Ethical Hacker (CEH) is globally recognized as the gold standard for assessing ethical hacking skills.

With CEH v13, you have the option to take two exams: a knowledge-based exam and a practical exam to earn the CEH Master certification.

Both exams are approved by the U.S. DoD 8140 and accredited by ANAB ISO/IEC 17024.

Industry practitioners meticulously vet certification domains to align with current industry demands.

Each exam undergoes rigorous psychometric evaluation, ensuring a fair and accurate assessment of your ethical hacking expertise.

Achieving the CEH certification and passing both the knowledge-based and practical exams earns you the prestigious CEH Master certification.

This advanced recognition demonstrates not only your theoretical understanding but also your mastery of real-world ethical hacking skills, proving you're ready to excel in any cybersecurity role.

3. C|EHv13 Engage

The CEH v13 program immerses you in real-world ethical hacking through the dynamic CEH practice environment.

With CEH Engage, you'll sharpen your skills and prove you have what it takes to thrive as an ethical hacker.

New to CEH v13, learners will embark on their first emulated ethical hacking engagement.

This four-phase engagement requires students to think critically and test the knowledge and skills gained by capturing a series of flags in each phase.

It demonstrates the live application of skills and abilities in a consequence-free environment through EC-Council's new "Cyber Range." As you complete your training and labs, CEH Engage empowers you to put theory into practice through a mock hacking engagement.

You'll navigate a real-world, four-part engagement, targeting an emulated organization.

Using a capture-the-flag format, you'll progress by answering critical "flag" questions, gaining hands-on experience in a full-scale ethical hacking operation.

4. C|EHv13 Compete

The CEH global challenges takes place monthly, providing capture-the-flag style competitions that give learners exposure to various new technologies and platforms, from web applications, OT, IoT, SCADA, and ICS systems to cloud and hybrid environments.

You will compete against other ethical hackers in a fast-paced, four-hour event as you climb the leaderboard in curated

CTFs designed around the ethical hacking process.

Each objective-based flag sharpens your current skills, tests your critical thinking, and covers the latest vulnerabilities and exploits.

Hosted entirely online in EC-Council's advanced Cyber Range, these scenario-based engagements are set in fully developed network and application environments with real operating systems, networks, tools, and vulnerabilities.

You'll have the opportunity to practice, engage, compete, build and hone your hacking techniques as you engage with new target organizations, all while racing against the clock to prove your mastery.

New Focus Areas and Trends in CEH v13:

Trained to think outside the box with a hacker's mindset, individuals who pursue the Certified Ethical Hacker (CEH) v13 thoroughly explore top OWASP attacks, active directory breaches, the vulnerability of traditional encryption to quantum computing, the growing ransomware threat, and other emerging risks, equipping learners with strategies to implement zero trust architecture and other cybersecurity measures. CEH v13 is comprehensive with the latest knowledge, providing cybersecurity professionals with the skills, tools, techniques, and strategies to defend against trending, modern, and complex cyber threats effectively and efficiently.

- Active Directory Attacks
- Ransomware Attacks and Mitigation
- AI and Machine Learning in Cybersecurity
- Critical Infrastructure Vulnerabilities
- Extended Detection and Response (XDR)
- Quantum Computing Risks and Attacks

- Post-Quantum Cryptography
 - Deepfake Threats
 - Zero Trust Architecture
 - Cloud Security
 - IoT Security Challenges
 - Critical Infrastructure Vulnerabilities
-

Цели – Какво ще научите:

What You Will Learn ?

Introduction to Ethical Hacking

Learn the fundamentals and key issues in information security, including the basics of ethical hacking, information security controls, relevant laws, and standard procedures

Foot Printing and Reconnaissance

Learn how to use the latest techniques and tools for footprinting and reconnaissance, a critical pre-attack phase of ethical hacking

Scanning Networks

Learn different network scanning techniques and countermeasures.

Enumeration

Learn various enumeration techniques, such as Border Gateway Protocol (BGP) and Network File Sharing (NFS) exploits, and associated countermeasures.

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.

System Hacking

Learn about the various system hacking methodologies used to discover system and network vulnerabilities, including steganography, steganalysis attacks, and how to cover tracks.

Malware Threats

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

Sniffing

Learn about packet sniffing techniques and their uses for discovering network vulnerabilities, plus countermeasures to defend against sniffing attacks.

Social Engineering

Learn social engineering concepts and techniques, including how to identify theft attempts, audit human-level vulnerabilities, and suggest social engineering countermeasures.

Denial-of-Service

Learn about different Denial of Service (DoS) and Distributed DoS (DDoS) attack techniques, plus the tools used to audit a target and devise DoS and DDoS countermeasures and protections.

Session Hijacking

Learn the various session-hijacking techniques used to discover network-level session management, authentication, authorization, and cryptographic weaknesses and associated countermeasures.

Evading IDS, Firewalls, and Honeypots

Learn about firewalls, intrusion detection systems (IDS), and honeypot evasion techniques; the tools used to audit a network perimeter for weaknesses; and countermeasures

Hacking Web Servers

Learn about web server attacks, including a comprehensive attack methodology used to audit vulnerabilities in web server infrastructures and countermeasures.

Hacking Web Applications

Learn about web application attacks, including a comprehensive hacking methodology for auditing vulnerabilities in web applications and countermeasures.

SQL Injection

Learn about SQL injection attack techniques, evasion techniques, and SQL injection countermeasures.

Hacking Wireless Networks

Learn about different types of encryption, threats, hacking methodologies, hacking tools, security tools, and countermeasures for wireless networks.

Hacking Mobile Platforms

Learn mobile platform attack vectors, Android and iOS hacking, mobile device management, mobile security guidelines, and

security tools.

IoT Hacking

Learn different types of Internet of Things (IoT) and operational technology (OT) attacks, hacking methodologies, hacking tools, and countermeasures.

Cloud Computing

Learn different cloud computing concepts, such as container technologies and serverless computing, various cloud computing threats, attacks, hacking methodologies, and cloud security techniques and tools

Cryptography

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

Формат на курса:

<input type="checkbox"/>	<input type="checkbox"/>
Присъствен (Classroom) Курс в Учебната ни зала или В Офис на Клиент	Онлайн (Online/Virtual) Курс във виртуална зала с инструктор

Език на курса:

<input type="checkbox"/>	<input type="checkbox"/>
Български (Bulgarian)	Английски (English)

Учебни Материали:



Учебните материали са достъпни в електронен формат. Могат да се ползват online/offline на всяко устройство. Неограничен достъп.

Лабораторна среда:



Dedicated Lab Environment

With 221 hands-on labs in our cutting-edge Cyber Range cyber range, you'll practice every skill on live machines and real-world vulnerabilities. Armed with over 4,000 powerful hacking tools and a range of operating systems, you'll gain unrivaled, practical expertise with the most widely used security tools, current vulnerabilities, and industry-standard operating systems.

This revolutionary environment brings the industry's top security tools and the latest vulnerabilities to your fingertips, all in a web-accessible platform. No matter where you are, you can dive into the real[1]world experience and emerge as a force to be reckoned with in cybersecurity.

100% virtualization for a complete learning experience Full access to pre-configured targets, networks, and the attack tools necessary to exploit them:

Pre-configured vulnerable websites

Vulnerable, unpatched operating systems

Fully networked environments

4000+ hacking tools and so much more!



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

След завършване получавате:

	
Lifetime Access - Video Archive 24/7	Certificate of Course Completion

Продължителност:



- 5 working days (09:00 – 17:00 / 9:00 am – 5:00 pm) UTC +2 (contact us for another Time Zone)

or

- **40 learning hours after hours (2 weeks, classes are held 2 times a week in one of the following**

options):

- Sat. and Sun. 10:00 – 14:00 or 14:00 – 18:00 or 18:00 – 22:00
 - Mon. and Wed. 19:00 – 23:00
 - Tue. or Thu. 19:00 – 23:00
-

Плащане:



Предстоящи Курсове:

юни 8

8 юни 2026 @ 09:00 - 12 юни 2026 @ 17:00 EEST 📅

[**EC-Council – Certified Ethical Hacker \(CEHv13 EN\)**](#)

юни 15

15 юни 2026 @ 09:00 - 19 юни 2026 @ 17:00 EEST 📅

[**EC-Council – Certified Ethical Hacker \(CEHv13 EN\)**](#)

юни 22

22 юни 2026 @ 09:00 - 26 юни 2026 @ 17:00 EEST 📅

[**EC-Council – Certified Ethical Hacker**](#)

[\(CEHv13 EN\)](#)

юни 29

29 юни 2026 @ 09:00 - 3 юли 2026 @ 17:00 EEST 

[EC-Council – Certified Ethical Hacker \(CEHv13 EN\)](#)

юли 6

6 юли 2026 @ 09:00 - 10 юли 2026 @ 17:00 EEST 

[EC-Council – Certified Ethical Hacker \(CEHv13 EN\)](#)

[Към календара](#)

За повече информация използвайте формата за контакт.

Ще се свържем с Вас за потвърждаване на датите.

All EC-Council Course Schedules

юни 8

8 юни 2026 @ 09:00 - 12 юни 2026 @ 17:00 EEST 

[EC-Council – Certified Ethical Hacker \(CEHv13 EN\)](#)

юни 15

15 юни 2026 @ 09:00 - 19 юни 2026 @ 17:00 EEST 


[EC-Council – Certified Ethical Hacker \(CEHv13 EN\)](#)

юни 22

22 юни 2026 @ 09:00 - 26 юни 2026 @ 17:00 EEST 


[EC-Council – Certified Ethical Hacker \(CEHv13 EN\)](#)

юни 29

29 юни 2026 @ 09:00 - 3 юли 2026 @ 17:00 EEST 

[EC-Council – Certified Ethical Hacker \(CEHv13 EN\)](#)

юли 6

6 юли 2026 @ 09:00 - 10 юли 2026 @ 17:00 EEST 

[EC-Council – Certified Ethical Hacker \(CEHv13 EN\)](#)

[Към календара](#)

[CEHv12 Brochure.cleaned](#)