EC-Council Certified Ethical Hacking (CEH)

ID CEH **Price** CHF 5,500.—(excl. VAT) **Duration** 5 days

Who should attend

- Mid-Level Information Security Auditor
- Cybersecurity Auditor
- Security Administrator
- IT Security Administrator
- Information Security Analyst 1
- Infosec Security Administrator
- Cybersecurity Analyst (Level 1, Level 2, & Level 3)
- Network Security Engineer
- SOC Security Analyst
- Network Engineer
- Senior Security Consultant
- Information Security Manager
- Senior SOC Analyst
- Solution Architect
- Cybersecurity Consultant
- Cyber Defense Analyst
- Vulnerability Assessment Analyst
- Warning Analyst
- All-Source Analyst
- Cyber Defense Incident Responder
- Research & Development Specialist
- Senior Cloud Security Analyst
- Third Party Risk Management:
- Threat Hunting Analyst
- Penetration Ttester
- Cybersecurity Instructor
- Red Team Specialist
- Data Protection & Privacy Officer
- SOAR Engineer
- AI Security Engineer
- Sr. IAM Engineer
- PCI Security Advisor
- Exploitation Analyst (EA)
- Zero Trust Solutions Engineer / Analyst
- Cryptographic Engineer
- AI/ML Security Engineer
- Machine Learning Security Specialist
- AI Penetration Tester
- AI/ ML Security Consultant
- Crypto Security Consultant

Prerequisites

To be eligible to challenge the EC-Council CEH certification examination, the candidate has two options:

Attend Official Network Security Training by EC-Council:

If a candidate has completed an official EC-Council training either at an Accredited Training Center, via the iClass platform, or at an approved academic institution, the candidate is eligible to challenge the relevant EC-Council exam without going through the application process.

Attempt the Exam without Official EC-Council Training:

In order to be considered for the EC-Council CEH exam without attending official network security training, the candidate must have at least 2 years of work experience in the Information Security domain. If the candidate has the required work experience, they can submit an eligibility application form along with US?$?100.—, a non-refundable fee

Course Objectives

Amplify Your Edge as a Certified Ethical Hacker Powered by AI Capabilities:

Advanced Knowledge: As an AI-powered Certified Ethical Hacker, 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.

How C|EH v13 Powered by AI Redefines Your Cybersecurity Career

- Experience the world's first ethical hacking program powered by AI
- Master the five phases of ethical hacking integrated with AI
- Achieve 40% efficiency and double your productivity with AI-driven skills
- Learn how to hack AI systems
- Become an AI expert with hands-on labs for practicing AI skills
- Master the latest advanced attack techniques, trends, and countermeasures
- Gain practical experience with 221 labs, attack vectors, and hacking tools
- Experience with over 550 attack techniques
- Explore 4,000+ commercial-grade hacking and security tools
- Follow a unique four-phase learning framework: Learn, Certify, Engage, Compete
- Practice hacking a real organization in a live cyber range
- Validate your skills in a 6-hour practical exam or 4-hour knowledge-based exam
- Compete with hackers in global CTF competitions on the latest issues
- Earn the globally recognized No.1 Ethical Hacking Certification
- Gain a certification that is approved and accredited by U.S. DoD 8140, ANAB 17024, and NCSC
- Meet the rigorous standards of NICE 2.0 and the NIST Framework
- Get the opportunity to be employed by top organizations including Fortune 500 companies, government, and private sector firms

Course Content

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

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.

Footprinting 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, including 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 are also included.

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 about different types of malware (Trojan, viruses, worms, etc.), APT and fileless malware, malware analysis procedures, 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

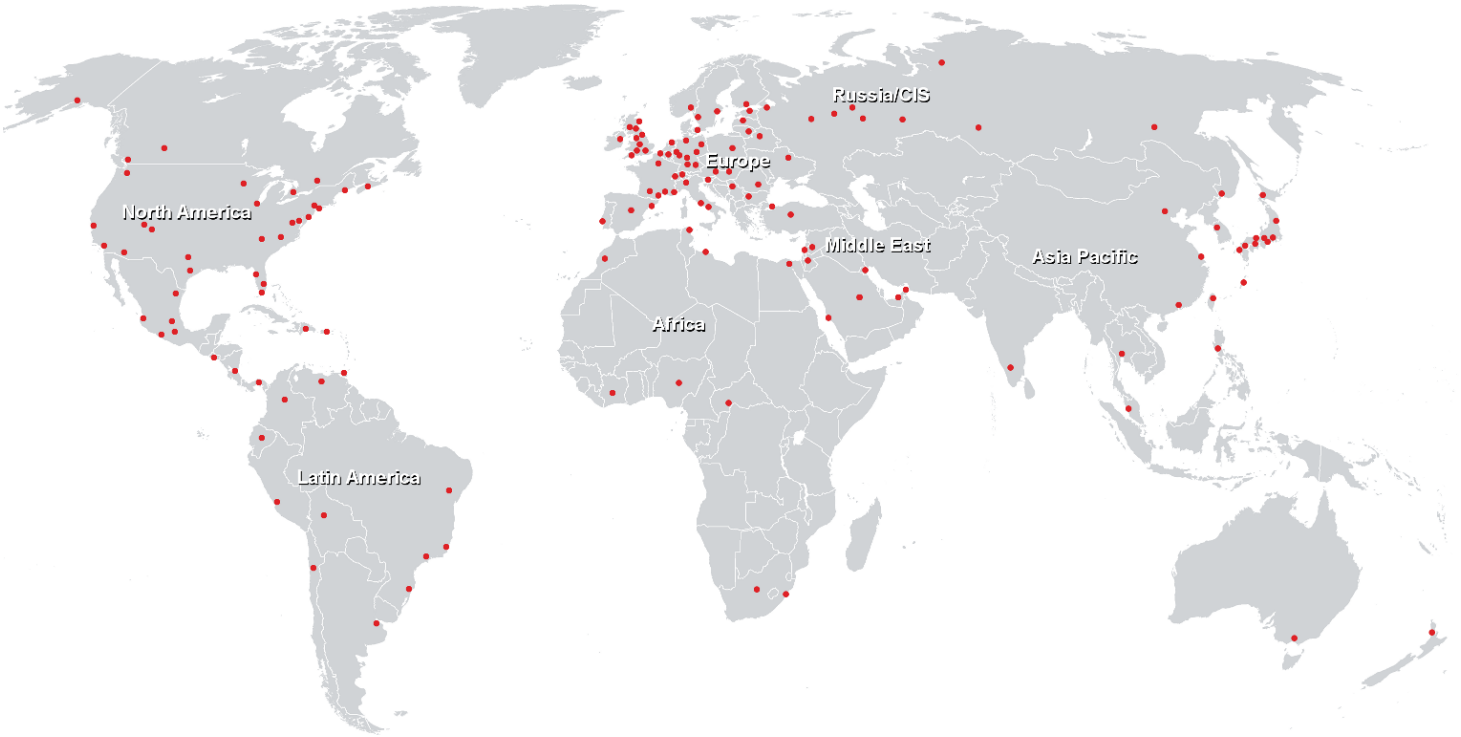
Learn different cloud computing concepts, such as container technologies and serverless computing, various cloud computing threats, attacks, hacking methodologies, and cloud security techniques and tools.

Cryptography

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

EC-Council Certified Ethical Hacking (CEH)

Training Centres worldwide



Fast Lane Institute for Knowledge Transfer (Switzerland) AG

Husacherstrasse 3
CH-8304 Wallisellen
Tel. +41 44 832 50 80

info@flane.ch, https://www.flane.ch