

## 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
- Cyber Defense Analyst
- Vulnerability Assessment Analyst
- Warning Analyst
- Information Security Analyst 1
- Security Analyst L1
- Infosec Security Administrator
- Cybersecurity Analyst level 1, level 2, & level 3
- Network Security Engineer
- SOC Security Analyst
- Security Analyst
- Network Engineer
- Senior Security Consultant
- Information Security Manager
- Senior SOC Analyst
- Solution Architect
- Cybersecurity 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

The C|EH® v12 program helps you develop real-world experience in ethical hacking through the hands-on C|EH® practice environment. The C|EH® Engage equips you with the skills to prove that you have what it takes to be a great ethical hacker. New to C|EH® v12, students will embark on their first emulated ethical hacking engagement. This 4-phase engagement requires students to think critically and test the knowledge and skills gained by capturing a series of flags in each phase, demonstrating 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 hands-on labs, the C|EH® Engage lets you apply everything you have learned in a mock ethical hacking engagement. This 4-part security engagement gives you a real ethical hacking engagement experience from start to finish against an emulated organization. Using our capture-the-flag-style range, you will complete your engagement by answering "flag" questions as you progress.

### Your Mission

Whether this is your first engagement or you're honing your skills, get ready to test your ethical hacking knowledge like never before! Once you've practiced through the hands-on guided labs, it's time to apply your knowledge, take on the hacker persona, and find the vulnerabilities and weaknesses in ABCDorg—all built in our C|EH® Engage (practice range).

### Objectives:

Armed with your attack platform, Parrot OS, and a plethora of tools used by Ethical Hackers, you will embark on a 4-part engagement to assess ABCDorg's security posture. Follow the process, practice your TTP and experience the real thing in a controlled environment with no consequences, just the ultimate learning experience to support your career as an Ethical Hacker! Each phase builds on the last as you progress through your ABCDorg's

# EC-Council Certified Ethical Hacking (CEH)

---

engagement.

## PHASE 1 Vulnerability Assessment

- Foot Printing &
- Reconnaissance
- Scanning
- Enumeration
- Vulnerability Analysis

## PHASE 2 Gaining Access

- System Hacking
- Malware Threats
- Sniffing
- Social Engineering
- Denial-of-Service

## PHASE 3 Perimeter and Web App Exploitation

- Session Hijacking
- Evading IDS
- Firewalls
- Honey pots
- Hacking Web Servers
- Hacking Web Applications
- SQL Injection

## PHASE 4 Mobile, IoT, OT Exploitation

- Hacking Wireless Networks
- Hacking Mobile Platforms
- IoT Hacking
- OT Hacking
- Cloud Computing
- Cryptography

## Course Content

The C|EH® v12 training program includes 20 modules covering various technologies, tactics, and procedures, providing prospective ethical hackers with the core knowledge needed to thrive in cybersecurity. Delivered through a carefully curated training plan that typically spans five days, the 12th version of the C|EH® continues to evolve to keep up with the latest OS, exploits, tools, and techniques. The concepts covered in the training program are split 50/50 between knowledge-based training and hands-on application through our cyber range. 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. Through our lab technology, every participant will have comprehensive hands-on practice to learn and apply their knowledge.

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

### 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.

### 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.

### 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—including steganography, steganalysis attacks, and covering tracks—used to discover system and network vulnerabilities.

### Malware Threats

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

# EC-Council Certified Ethical Hacking (CEH)

---

## Sniffing

Learn about packet-sniffing techniques and how to use them to discover network vulnerabilities, as well as 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, as well as the tools used to audit a target and devise DoS and DDoS countermeasures and protections.

## Session Hijacking

Understand 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

Get introduced to firewall, intrusion detection system (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 web application hacking methodology used to audit vulnerabilities in web applications and countermeasures.

## SQL Injection

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

## Hacking Wireless Networks

Understand different types of wireless technologies, including encryption, threats, hacking methodologies, hacking tools, Wi-Fi security tools, and countermeasures.

## Hacking Mobile Platforms

Learn Mobile platform attack vector, android and iOS hacking, mobile device management, mobile security guidelines, and security tools.

## IoT Hacking

Learn different types of IoT and OT attacks, hacking methodology, hacking tools, and countermeasures.

## Cloud Computing

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.

## Session Hijacking

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

# EC-Council Certified Ethical Hacking (CEH)

---

## Training Centres worldwide



### Fast Lane Institute for Knowledge Transfer GmbH

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

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