+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated 04/23/2025

Sign up

CEH™ training - Certified Ethical Hacker™

Exam included + 1 year access

5 days (35 hours)

Presentation

Our Certified Ethical Hacker training course will prepare you to pass the "Certified Ethical Hacker" certification. Assimilate the knowledge needed to secure network systems, databases and hacker attacks.

Now in its 13th version, the course has been updated to bring you the tools and techniques used by hackers and security professionals to penetrate any information system.

Thanks to CEH™ training you'll plunge into the hacker mindset to guard against any attack. CEH™ certification accredited to ANSI 17024 compliance will enable you to test, scan, and hack a targeted system.

With Ambient IT as training organization, take advantage of the CEH™ Elite pack, included with your preparation.

Training content

- 1 year access to eCourseware online courses
- 6 months' access to the Labs
- 1 Exam voucher
- 1 exam retake (in case of failure)
- CEH Engage (test and preparation)
- Global CEH Challenges (annual competition pass)
- CEH Practical Exam
- 10 videos for learning about cybersecurity

Objectives

- Understanding the fundamentals of ethical hacking
- Have the skills to secure systems, networks, databases or applications from hacking attacks
- Ready for CEH™ certification

Target audience

- Ethical hackers
- IT security expert
- Developers
- Directors
- Network administrator

Prerequisites

- Experience in using Windows and Linux operating systems
- Basic knowledge of TCP/IP network protocols and operation
- 2 years' experience in cybersecurity

Ambient IT is not an ATC of EC-Council. CEH™ is a registered trademark of EC-Council international limited. Ambient IT is neither affiliated nor accredited by EC-Council.

CEH™ Certification Preparation Program

Introduction

- Back to safety basics
- What is ethical hacking?
- What are the ethical hacker's missions?

Information gathering

- Footprinting
- TCP/IP networks
- Scanning method
- Listing

Attacking networks

- Wireless networking
- Network concepts
- Techniques and tools

- Escape techniques
- Wireless hacking

Hacking a system

- Authentication
- Elevation of privileges
- Hide files
- Covering your tracks
- Malware
- Denial of service
- Session hijacking
- Hacking a web application

Web servers

- Attack methodologies
- Web server architecture
- Server attacks
- Attacks on web applications

IoT

- Architecture
- The hacking method
- Vulnerabilities
- The attacks
- Mobile attacks and vulnerabilities

Cloud Computing

- Types of service
- The threats
- The attacks
- Cloud hacking

Cryptography

- A reminder of cryptography
- PKI
- Digital certificates
- Encrypted communications
- Cryptographic attacks

Pentest

- Security audit
- Active recognition
- The methodology
- Farms

Social Engineering

- Introduction to social engineering
- Protecting yourself against this type of attack
- Attacks on mobile devices vs. attacks on mobile devices
- Physical safety

Artificial Intelligence and CyberSecurity

- Overview of different AI tools
- Deepfake threats
- AI and machine learning in cybersecurity
- Quantum computing

Preparing for the CEH exam

- Certification overview
- Time management tips
- Memo

Companies concerned

This course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced computer technology, or to acquire specific business knowledge or modern methods.

Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire which enables us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the training to come, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical course: 60% Practical, 40% Theory. Training material distributed in digital format to all participants.

Organization

The course alternates theoretical input from the trainer, supported by examples, brainstorming sessions and group work.

Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

Sanction

A certificate will be issued to each trainee who completes the course.