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

Updated on 11/13/2026

Sign Up

Certified Lead Ethical Hacker (CLEH) Training Course

5 days (35 hours)

Overview

Ethical hacking allows you to assess the security of systems and networks through authorized testing. The official Certified Lead Ethical Hacker (CLEH) certification evaluates the skills required to identify vulnerabilities, conduct a controlled exploitation, and document the results of a penetration test.

Our Certified Lead Ethical Hacker (CLEH) Certification Training will help you prepare for the exam by developing a structured approach, from defining the scope to reporting findings.

You will learn how to conduct reconnaissance, identify vulnerabilities, select exploitation techniques, and master the principles of privilege escalation and pivoting in a controlled lab environment.

Upon completion of the training, you will be able to align penetration testing methodologies with regulatory frameworks and standards, collect evidence, and produce an actionable report to improve security.

This preparation combines hands-on workshops, certification scenarios, and timed simulations. The exam is administered during a dedicated session. Awarding of the certification is contingent upon passing the exam and meeting the certifying body’s experience requirements.

Like all our training courses, this one will introduce you to **the latest stable version** of the technology and its new features.

Objectives

- Master the concepts, methods, and techniques of ethical hacking and penetration testing
- Link penetration testing methodologies to regulatory frameworks and security standards
- Identify and validate vulnerabilities within an explicitly authorized scope
- Apply the principles of exploitation, privilege escalation, and pivoting in a lab environment
- Document evidence and formulate remediation recommendations
- Prepare for the practical exams and the writing of the certification report

Target Audience

- Penetration Tester
- Cybersecurity consultant
- Security analyst
- Systems and Network Security Engineer
- Information Systems Security Manager

Prerequisites

- Knowledge of information security principles and vulnerability management
- Proficiency in system administration and command-line operations on Linux and Windows
- Understanding of TCP/IP networks and DNS and HTTP services
- Basic programming or scripting skills in Python or Bash
- Ability to read technical documentation in English

Technical Requirements

- Computer with 8 GB of RAM recommended and a screen suitable for simultaneous use of the lab and course materials
- An up-to-date version of Google Chrome or Mozilla Firefox to access the remote lab and its virtual machines
- Stable internet connection allowing access to the learning platforms, with network permissions validated prior to the session
- Lab access account provided for the training and a myPECB account to be created for register for the exam
- For the remote exam: a webcam, microphone, and the PECB Exams software installed on a computer that meets the requirements provided at registration

Curriculum for our Certified Lead Ethical Hacker (CLEH) training

[Day 1 - Morning]

Fundamentals of Ethical Hacking

- Concepts of ethical hacking and the roles of stakeholders in an offensive security mission

- Differences between security audits, vulnerability assessments, and penetration testing
- The pentest lifecycle, from preparation to reporting results
- Skill areas and exam structure for the Certified Lead Ethical Hacker (CLEH) certification
- Hands-on Workshop: Analyzing a penetration testing request and mapping the proposed activities to the certification domains.

[Day 1 - Afternoon]

Scope definition and testing methodologies

- Defining the authorized scope, exclusions, and mission objectives
- Formulating rules of engagement, termination conditions, and emergency contacts
- Contributions of NIST SP 800-115 and the OWASP WSTG to test structuring
- Alignment between regulatory frameworks, standards, contractual requirements, and expected evidence
- Organization of the isolated lab and protection of collected data
- Hands-on workshop: Drafting a mission scope and a matrix linking objectives, reference frameworks, and authorized tests.

[Day 2 - Morning]

Reconnaissance and Information Gathering

- Distinction between passive and active reconnaissance
- Gathering public information and identifying the attack surface
- Discovering hosts and services with Nmap within the lab environment
- Enumeration of DNS, HTTP, and SMB services
- Consolidation of Results and Traceability of Technical Evidence
- Hands-on Workshop: Mapping a laboratory network and compiling an annotated inventory of exposed services.

[Day 2 - Afternoon]

Threats and Vulnerability Analysis

- Identification of assets, entry points, and threat scenarios
- Scanning for known vulnerabilities and analyzing misconfigurations
- Interpreting scan results and validating false positives
- Prioritization based on exposure, exploitability, and business impact
- Selection of exploitation scenarios and definition of success criteria
- Hands-on Workshop: Analyze the vulnerabilities of a fictional environment and develop a prioritized validation plan.

[Day 3 - Morning]

Controlled exploitation of services

- Exploitation Principles and Verification of Technical Prerequisites
- Selecting a proof of concept and assessing operational risk
- Getting started with the Metasploit Framework in a deliberately vulnerable environment
- Managing test access and collecting reproducible evidence
- Mitigating Impacts and Adhering to Shutdown Conditions
- Hands-on Workshop: Validating a vulnerability on a dedicated machine and documenting the conditions under which access was obtained.

[Day 3 - Afternoon]

Web Application Penetration Testing

- Analysis of HTTP traffic using an interception proxy
- Using Burp Suite Community Edition to examine requests and responses
- Verifying authentication, sessions, and access controls
- Identifying injections and input validation flaws
- Organizing tests and findings according to the OWASP WSTG
- Hands-on Workshop: Examine a deliberately vulnerable application and write a findings report with evidence and remediation steps.

[Day 4 - Morning]

Privilege Escalation and Post-Exploitation

- Local enumeration after gaining initial access
- Analysis of permissions, services, and tasks on Linux and Windows
- Identifying configurations that facilitate privilege escalation
- Assessment of obtained access and its impact on assets
- Management of sensitive data, preservation of evidence, and cleanup of test artifacts
- Hands-on workshop: Identify a local misconfiguration, validate its impact in the lab, and propose a fix.

[Day 4 - Afternoon]

Pivoting and pentest reporting

- Principles of pivoting between segments of a lab network
- Selecting file transfer mechanisms and verifying their integrity
- Traceability of the access path and demonstration of cumulative impacts
- Structure of the technical report, executive summary, and evidence appendices
- Prioritizing Remedies and Preparing Verification Tests
- Hands-on Workshop: Perform an authorized pivot between two segments and produce a summary report of the tested scenario.

[Day 5 - Morning]

Certification simulation

- Review of areas for information gathering and vulnerability identification
- Consolidation of exploitation, privilege escalation, and pivoting techniques
- Organizing notes and resources for an open-book exam
- Time management, prioritizing leads, and preparing the evidence log
- Hands-on Workshop: Conducting the first part of a timed white-hat penetration test on a lab environment with multiple target machines.

[Day 5 - Afternoon]

Debriefing and final exam preparation

- Finalizing the penetration test scenario and verifying evidence of compromise
- Drafting a clear, reproducible audit report organized by target
- Reviewing findings, impacts, and corrective recommendations
- Analysis of common errors and development of a personalized review plan
- Procedures for the official exam during a dedicated session and distinction between passing the exam and awarding the certification
- Hands-on workshop: Finalizing the white-hat penetration test report and conducting a peer review using a
  educational preparation checklist.

Target Audience

This training is intended for both individuals and companies—large or small—seeking to train their teams in new, advanced IT technologies or to acquire specific professional knowledge or modern methods.

Entry-Level Assessment

The pre-training assessment complies with Qualiopi quality standards. Upon final registration, the learner receives a self-assessment questionnaire that allows us to evaluate their estimated proficiency level across various types of technologies, as well as their expectations and personal goals for the upcoming training, within the limits imposed by the selected format. This questionnaire also allows us to anticipate certain connection or internal security issues within the company (intra-company or virtual classroom) that could pose challenges for monitoring and ensuring the smooth operation of the training session.

Teaching Methods

Hands-On Training: 60% Hands-On, 40% Theory. Training materials distributed in digital format to all participants.

Organization

The course alternates between theoretical instruction from the trainer—supported by examples and reflection sessions—and group work.

Assessment

At the end of the session, a multiple-choice quiz is administered to verify that participants have successfully acquired the skills.

Certification

A certificate will be issued to each trainee who has completed the entire training program.

Training organization registered under number 11 75 54743 75. This registration does not constitute state accreditation.
© Ambient IT 2015-2026. All rights reserved. Paris, France - Switzerland - Belgium - Luxembourg