# PECB Certified Lead Ethical Hacker

**Master the attack techniques and countermeasures on the different structures of an information system.**

**Expand your knowledge of ethical hacking and IT security; improve your hacking skills and perfect your knowledge of the most advanced techniques in IT security.**

## Why should you attend?

The Certified Lead Ethical Hacker training course enables you to develop the necessary expertise to perform information system penetration tests by applying recognized principles, procedures and penetration testing techniques, in order to identify potential threats on a computer network. During this training course, you will gain the knowledge and skills to manage a penetration testing project or team, as well as plan and perform internal and external pentests, in accordance with various standards such as the Penetration Testing Execution Standard (PTES) and the Open Source Security Testing Methodology Manual (OSSTMM). Moreover, you will also gain a thorough understanding on how to draft reports and countermeasure proposals. Additionally, through practical exercises, you will be able to master penetration testing techniques and acquire the skills needed to manage a pentest team, as well as customer communication and conflict resolution.

The Certified Lead Ethical Hacking training course provides a technical vision of information security through ethical hacking, using common techniques such as information gathering and vulnerability detection, both inside and outside of a business network.

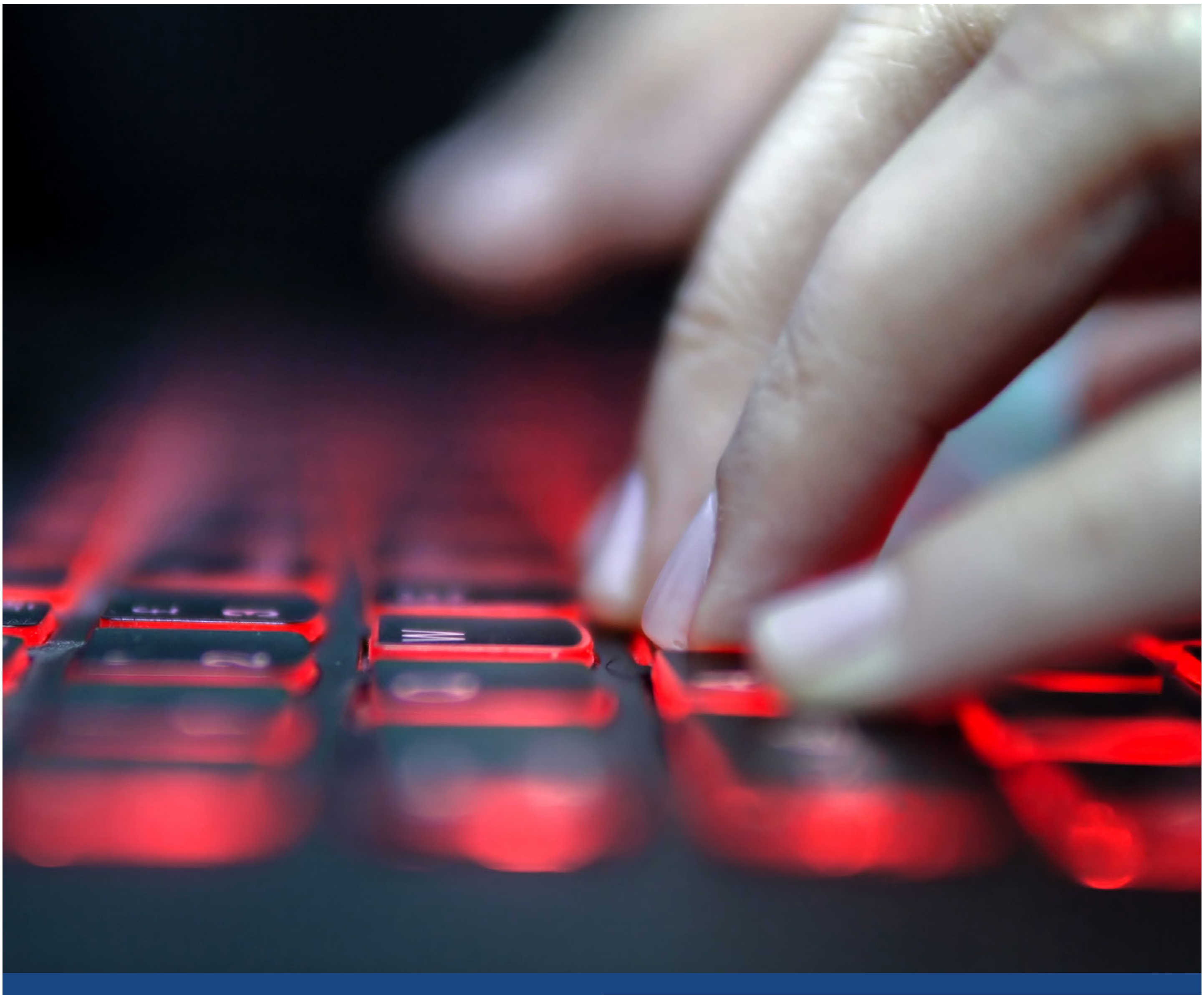
The training is also compatible with the NICE (The National Initiative for Cybersecurity Education) Protect and Defend framework. After mastering the necessary knowledge and skills in ethical hacking, you can take the exam and apply for the "PECB Certified Lead Ethical Hacker" credential. By holding a PECB Lead Ethical Hacker certificate, you will be able to demonstrate that you have acquired the practical skills for performing and managing penetration tests according to best practices.

## Who should attend?

- Individuals interested in IT Security, and particularly in Ethical Hacking, to either learn more about the topic or to start a process of professional reorientation.
- Information security officers and professionals seeking to master ethical hacking and penetration testing techniques.
- Managers or consultants wishing to learn how to control the penetration testing process.
- Auditors wishing to perform and conduct professional penetration tests.
- Persons responsible for maintaining the security of information systems in an organization.
- Technical experts who want to learn how to prepare a pentest.
- Cybersecurity professionals and information security team members.

## Learning objectives

- Understand the fundamental concepts of ethical hacking and the required technical knowledge to perform and manage penetration tests;
- Master the concepts, approaches, standards, methods, and techniques used for the operation of an effective ethical hacking process;
- Acquire the expertise to conduct a penetration test following a logical path by using a variety of tools and techniques;
- Develop the expertise to analyze the results of testing activities and produce effective reports which will help organizations to effectively address vulnerabilities;
- Strengthen the personal qualities necessary to act with due professional care when conducting penetration tests;
- Be able to define and explain the different phases of cyberattacks;
- Become acquainted with the different tools used to collect information before performing any attack;
- Learn about the different attacks that affect the security of an organization's network;
- Learn how to perform the different steps comprising a penetration test (ethical hacking) and its associated tools by obtaining information, scanning, enumeration and attack processes;
- Learn about the most important aspects of Distributed Denial of Service (DDoS) attacks and their tools;



## Examination

Duration: 3 hours

The "PECB Certified Lead Ethical Hacker" exam meets all the requirements of the PECB Examination and Certification Program (ECP). The exam covers the following competency domains:

| | |
|---|---|
| **Domain 1** | **Fundamental principles and concepts of ethical hacking** |
| **Domain 2** | **Attack mechanisms** |
| **Domain 3** | **Principles and reference frameworks on penetration tests** |
| **Domain 4** | **Planning and performing penetration tests using various tools and techniques** |
| **Domain 5** | **Drafting penetration testing reports** |

The examination consists of two parts. The first part is a paper-based exam, which consists of essay-type questions. The second part is rather technical, where the candidate will be required to conduct penetration testing exercises on a computer and draft a report of the analysis.

Participants are authorized to use their personal notes during both the paper-based exam as well as the practical part of the exam.

For more information about exam details, please visit Examination Rules and Policies.

## Certification

After successfully completing the exam, you can apply for the credentials shown on the table below.
You will receive a certificate once you comply with all the requirements related to the selected credential.

For more information about Ethical Hacking certifications and the PECB certification process, please refer to the Certification Rules and Policies.

| Credential | Exam | Professional experience | Experience in penetration testing projects | Other requirements |
|---|---|---|---|---|
| **PECB Certified Provisional Ethical Hacker** | PECB Certified Lead Ethical Hacker exam or equivalent | None | None | Signing the PECB Code of Ethics |
| **PECB Certified Ethical Hacker** | PECB Certified Lead Ethical Hacker exam or equivalent | **Two years:** One year of work experience in penetration testing | Activities: A total of 200 hours | Signing the PECB Code of Ethics |
| **PECB Certified Lead Ethical Hacker** | PECB Certified Lead Ethical Hacker exam or equivalent | **Fifteen years:** Two years of work experience in penetration testing | Activities: A total of 300 hours | Signing the PECB Code of Ethics |

## General information

- Certification fees are included on the exam price
- Training material containing over 450 pages of information and practical examples will be distributed
- A participation certificate of 31 CPD (Continuing Professional Development) credits will be issued
- In case of exam failure, you can retake the exam within 12 months for free