PECB BEYOND RECOGNITION

PECB Certified
Lead Ethical Hacker

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?

As the impact of security incidents in small and large organizations has increased significantly, so has the demand for ethical hacking. Ethical hacking is one of the most effective tools of safeguarding assets and protecting people and information. Ethical hacking certification is slowly becoming a standard requirement for professionals who want to work in the field of information security.
A PECB Certified Lead Ethical Hacker certification will help you demonstrate your ability to lawfully assess the security of systems and discover their vulnerabilities. The training course provides information on the latest ethical hacking methods and tools. It also provides a methodology for conducting penetration tests in accordance with standards and best practices, such as the Penetration Testing Execution Standard (PTES) and the Open Source Security Testing Methodology (OSSTMM).
Understanding hackers' strategies helps solve security issues and challenges. After attending the training course, you will be able to plan, manage, and perform information security penetration tests.

The PECB Certified Lead Ethical Hacker training course is based on the concept of practicing what you learned. It includes lab sessions and practical examples to help you apply the theory into practice.

The training course is followed by an exam. If you pass, you can apply for a "PECB Certified Lead Ethical Hacker" credential. For more information about the examination process, please refer to the Examination, Certification, and General Information section below.

Who should attend?

This training course is intended for:

- Individuals seeking to gain knowledge about the main techniques used to conduct penetration tests
- Individuals involved in information security seeking to master ethical hacking and penetration testing techniques
- Individuals responsible for the security of information systems, such as information security officers and cybersecurity professionals
- Information security team members seeking to enhance their information security knowledge
- Managers or expert advisors interested in learning how to manage ethical hacking activities
- Technical experts interested in learning how to plan and perform a penetration test

Course agenda

Duration: 5 days

Day 1 | Introduction to ethical hacking

- Training course objectives and structure
- Penetration testing standards, methodologies, and frameworks
- Lab overview
- Fundamental concepts of ethical hacking
- Network fundamentals
- Understanding cryptography
- Relevant trends and technologies
- Kali Linux fundamentals
- Initiation of the penetration test
- Analysis of the penetration testing scope
- Legal implications and contractual agreement

Day 2 | Initiating the reconnaissance phase

- Passive reconnaissance
- Active reconnaissance
- Identification of vulnerabilities

Day 3 | Initiating the exploitation phase

- Threat model and attack plan
- Evading intrusion detection systems
- Server-side attacks
- Client-side attacks
- Web application attacks
- WIFI attacks
- Privilege escalation
- Pivoting
- File Transfers
- Maintaining access

Day 4 | Post-exploitation and reporting

- Cleaning up and destroying artifacts
- Generating a findings report
- Recommendations on mitigating the identified vulnerabilities
- Closing the training course

Day 5 | Certification exam

Learning objectives

This training course allows you to:

- Master the concepts, methods, and techniques used by cybersecurity organizations and ethical hackers to conduct penetration tests
- Acknowledge the correlation between penetration testing methodologies, regulatory frameworks, and standards
- Acquire a comprehensive knowledge of the components and operations of ethical hacking

Examination

Duration: 6 hours

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

Domain 1 | Information gathering tools and techniques

Domain 2 | Threat modeling and vulnerability identification

Domain 3 | Exploitation techniques

Domain 4 | Privilege escalation

Domain 5 | Pivoting and file transfers

Domain 6 | Reporting

The PECB Certified Lead Ethical Hacker exam comprises two parts: practical exam and report writing. The practical exam requires the candidate to compromise at least two target machines through penetration testing. The process should be documented in a written report. The PECB Certified Lead Ethical Hacker exam is an open book exam. Candidates are allowed to use training course materials and personal notes during the examination process.

For specific information about the exam type, languages available, and other details, please visit the List of PECB Exams and Exam Rules and Policies.

Certification

Upon the successful completion of the exam, you can apply for the "PECB Certified Lead Ethical Hacker" credential, depending on your level of experience, as shown in the table below. You will receive the certificate once you comply with all the relevant educational and professional requirements.

For more information about ethical hacking certifications and the PECB Certification process, please refer to Certification Rules and Policies.

Credential	Exam	Professional experience	Project experience	Other requirements
PECB Certified Lead Ethical Hacker	PECB Certified Lead Ethical Hacker exam	**Two years of penetration testing and cybersecurity experience**	None	Signing the PECB Code of Ethics and the PECB CLEH Code of Conduct

General information

- Participants will be provided with training course material containing over 450 pages of information, practical examples, and exercises.
- An attestation of course completion worth 35 CPD (Continuing Professional Development) credits will be issued to the participants who have attended the training course.
- Candidates who have completed the training course but failed the exam are eligible to retake it once for free within a 12-month period from the initial date of the exam.