CLEH – Certified Lead Ethical Hacker: Ethical Hacking and Penetration Testing

Date and duration

Training code : CLEH-EN
Duration : 4,5 days
Nombre d'heures : 31 heures

Training with certification

PECB Certified Lead Ethical Hacker

Body

With the surge in security breaches affecting SMEs and large enterprises alike, there is an increasing demand for ethical hacking expertise. This discipline remains one of the most effective tools to safeguard resources and ensure the confidentiality of data and individuals. Mastering ethical hacking techniques and penetration testing has therefore become a necessity for anyone aiming to specialize in information security and cybersecurity.
This 4.5-day training course is designed to provide you with the essential knowledge and skills required to conduct advanced ethical hacking operations. More specifically, you will be trained in penetration testing techniques targeting information systems and network infrastructures.
The Lead Ethical Hacker course includes a series of practical labs on a virtual machine as well as case studies, ensuring that you can quickly apply the theoretical knowledge acquired.
At the end of this highly relevant and in-demand training, you will be ready to take the official Lead Ethical Hacker certification exam. This online exam will allow you to earn the prestigious title of PECB Certified Lead Ethical Hacker.

Objectifs

By the end of the Lead Ethical Hacker training, you will be able to:

- Fully understand the concepts, methods, and techniques used by cybersecurity professionals and ethical hackers to conduct penetration tests.
- Comprehend the synergies between penetration testing methods, standards, and regulations.
- Develop advanced expertise in ethical hacking and its practical applications.
- Successfully pass the official exam and earn your PECB Certified Lead Ethical Hacker certification.

Points forts

- Unlike CEH, the CLEH training emphasizes hands-on practice based on real-world cases and includes a comprehensive 450-page manual.
- 35 CPD credits are awarded.
- The certification exam is included in the training price.
- In case of exam failure, you can retake it free of charge within 12 months.

Certification

At the end of the training, you will receive a voucher that allows you to schedule your PECB Lead Ethical Hacker certification exam at the date and time of your choice.

Exam Information – Lead Ethical Hacker

The exam is conducted in English and takes place online. It consists of a practical component and a written report, with a maximum duration of 6 hours. For the practical part, you must successfully compromise at least two target machines through penetration testing. For the theoretical part, you must document your hacking operations in detail. During the exam, you are allowed to consult your course materials and personal notes. The passing score is set at 70%.
Once you have passed the exam and met the eligibility requirements (2 years of experience in penetration testing and cybersecurity), you can apply for the PECB Certified Lead Ethical Hacker certification.

For more details on requirements, please refer to the PECB Exam Rules and the PECB Certification Rules.
Pour en savoir plus sur les modalités, consultez le règlement d'examen PECB ainsi que le règlement de certification PECB.

Modalités d'évaluation

Practical Work
Case study

Pré-requis

Attending the Lead Ethical Hacker training requires the following prerequisites:

- A solid understanding of concepts and principles related to information security.
- Advanced skills in operating system administration.
- Strong knowledge of networking and programming techniques is highly recommended.

Public

This training is designed for the following participants:

- Individuals who wish to become familiar with the basic techniques used to successfully carry out penetration tests.
- Cybersecurity professionals seeking to master ethical hacking methods and penetration testing techniques.
- Information Security Officers (ISOs), especially executives responsible for information security and IT security in general.
- Individuals involved in information security who want to deepen their knowledge in this field.
- Department heads or expert consultants wishing to understand how to manage ethical hacking operations.
- Technical administrators who want to learn how to plan and execute a penetration test.

Programme

Day 1: Introduction to Ethical Hacking

- Training objectives and course structure.
- Standards, methods, and penetration testing tools.
- Laboratory setup.
- Basics of ethical hacking.
- Networking fundamentals.
- Fundamentals of cryptography.

- Emerging trends and new technologies in hacking.
- Fundamentals of the Kali Linux system.
- Setting up penetration tests.
- Analyzing the scope of penetration testing.
- Legal aspects and contractual agreements.

Day 2: Reconnaissance Phase

- Passive reconnaissance.
- Active reconnaissance.
- Vulnerability identification.

Day 3: Exploitation Phase

- Threat modeling and attack strategies.
- Bypassing Intrusion Detection Systems (IDS).
- Server-side attacks.
- Client-side attacks.
- Attacks on web infrastructures.
- Wireless (Wi-Fi) attacks.
- Privilege escalation.
- Network pivoting.
- File transfers.
- Maintaining access.

Days 4 & 5: Post-Exploitation and Reporting

- Cleaning up and removing artifacts.
- Reporting findings.
- Recommendations for mitigating identified security vulnerabilities.

PECB

Training content delivered in partnership with PECB PECB