Publication date : 02/04/2026

Course : Certified Lead Ethical Hacker, PECB certification

Practical course - 4d - 28h00 - Ref. CEY
Price : 3460 € E.T.

★★★★☆ 4,5 / 5

You will acquire the knowledge and skills needed to plan and carry out internal and external pentests, in compliance with various standards (PTES, OSSTMM), as well as writing reports and proposing countermeasures. The course is compatible with the NICE Protect and Defend rubric.

Teaching objectives

At the end of the training, the participant will be able to:

- ✓ Understand the mechanism of the main attacks
- ✓ Detect system weaknesses through knowledge of the different targets of a hacking attack
- ✓ Apply basic measures and rules to combat hacking
- ✓ Writing a pentest report

Intended audience

Security managers and architects. System and network technicians and administrators.

Prerequisites

Good knowledge of networks and systems (Microsoft and Linux).

Certification

Once you've acquired the necessary expertise with this course, you'll take the "PECB Certified Lead Ethical Hacker" exam. The 6-hour remote exam consists of two parts: the practical exam and the report. The practical exam requires the candidate to compromise at least two target machines using penetration tests. The process must be documented in a written report. The PECB Certified Lead Ethical Hacker exam is an open-book exam. Candidates are allowed to use course materials and personal notes during the exam. The PECB certificate certifies that you have acquired the necessary skills for penetration testing according to the best standards.

Remote certifications

See the certifier's official documentation for the list of prerequisites for completing the online certification exam.

PARTICIPANTS

Security managers and architects. System and network technicians and administrators.

PREREQUISITES

Good knowledge of networks and systems (Microsoft and Linux).

TRAINER QUALIFICATIONS

The experts leading the training are specialists in the covered subjects. They have been approved by our instructional teams for both their professional knowledge and their teaching ability, for each course they teach. They have at least five to ten years of experience in their field and hold (or have held) decision-making positions in companies.

ASSESSMENT TERMS

The trainer evaluates each participant's academic progress throughout the training using multiple choice, scenarios, hands-on work and more.
Participants also complete a placement test before and after the course to measure the skills they've developed.

Course schedule

1 Cybersecurity and architecture

- Panorama of cybersecurity and contemporary architecture.
- Performing an intrusion test, a pentest, the different types of pentest.
- Architectures, operating systems, known vulnerabilities.

2 Active recognition

- Active and passive forms of recognition.
- Recognition, scanning and enumeration.
- Gather information on vulnerabilities.
- Port scanning.
- Exploit known security flaws in port-related services, etc.

Hands-on work

Review of automatic vulnerabilities: Nessus, OpenVAS.

3 System operation

- Operating frameworks.
- Understanding CVEs: types (Remote, Local, Web).
- Process exploits: Buffer Overflow, ROP, Dangling Pointers.
- Shellcodes and rootkits.
- Microsoft authentication attack, PassTheHash.
- Windows: Buffer Overflow by hand, exploits.

Hands-on work

Exploit system vulnerabilities (Microsoft and Linux).

4 Operation and post-operation

- Document preparation and report writing.
- Describe the vulnerabilities found.
- Formulate safety recommendations.

Hands-on work

Report writing and formatting.

Dates and locations

REMOTE CLASS
2026 : 2 June, 15 Sep., 1 Dec.

PARIS LA DÉFENSE
2026 : 2 June, 15 Sep., 1 Dec.

TEACHING AIDS AND TECHNICAL RESOURCES

• The main teaching aids and instructional methods used in the training are audiovisual aids, documentation and course material, hands-on application exercises and corrected exercises for practical training courses, case studies and coverage of real cases for training seminars.

• At the end of each course or seminar, ORSYS provides participants with a course evaluation questionnaire that is analysed by our instructional teams.

• A check-in sheet for each half-day of attendance is provided at the end of the training, along with a course completion certificate if the trainee attended the entire session.

TERMS AND DEADLINES

Registration must be completed 24 hours before the start of the training.

ACCESSIBILITY FOR PEOPLE WITH DISABILITIES

Do you need special accessibility accommodations? Contact Mrs. Fosse, Disability Manager, at psh-accueil@orsys.fr to review your request and its feasibility.