PECB Certified Lead Ethical Hacker

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;

Educational approach

- This training is based on both theory and practical exercises. The percentage ratio for the theoretical and practical part of the training is 40% and 60% respectively. Practical exercises are combined with tutorials to help the candidates acquire the required skills.
- The laboratory environment is intensive, providing in-depth knowledge and practical experience regarding current security systems to each candidate.
- Learning by doing: The participant will engage in scenarios, situations and decision-making that he or she will most probably face during his or her professional life.
- Practical tests are similar to the Certification Exam.

Course Agenda

Day 1: Overview of cybersecurity, ethical hacking and contemporary architecture

Day 2: Active recognition

Day 3: System operation

Day 4: Exploitation and post-exploitation, and report drafting

Day 5: Certification Exam

Prerequisites

A fundamental knowledge of Information Security, and advanced skills in operating systems (e.g., Microsoft, Linux, etc.) is required. Furthermore, it is desirable for the candidate to have knowledge on computer networks, the use of operating systems and the notions of programming.

Examination

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.

Price: 7.950 Kn + VAT

Contact

ZIH d.o.o., tel: 01/4855-271, 4855-273, fax: 01/4855-272, e-mail: zih@zih.hr

Application:

DOC Download