PECB BEYOND RECOGNITION



PECB Certified
Lead Pen Test Professional

Master Professional Penetration Testing

Why should you attend?

Lead Pen Test Professional training enables you to develop the necessary expertise to lead a professional penetration test by using a mix of practical techniques and management skills.

This course is designed by industry experts with in-depth experience in the Penetration Testing field. Unlike other trainings, this training course is focused specifically on the knowledge and skills needed by professionals looking to lead or take part in a penetration test. It drills down into the latest technical knowledge, tools and techniques in key areas including infrastructure, Web Application security, Mobile security and Social Engineering. In addition, this course concentrates on how to practically apply what is learned on current day-to-day penetration testing and does not expand on unrelated, dated or unnecessary theoretical concepts.

Along with the in-depth hands-on practical skills, this training course equips you with the management skills you need to lead a penetration test, taking into account business risks and key business issues. The individuals who complete the course have the right blend of the real business and technical competencies needed to be a respected, understood and professional penetration tester. On the last day of the training course, you will get to use the skills learned in a comprehensive capture and flag penetration testing exercises.



Who should attend?

- IT professionals looking to enhance their technical skills and knowledge
- Auditors looking to understand the Penetration Testing processes
- IT and Risk managers seeking a more detailed understanding of the appropriate and beneficial use of Penetration Tests
- Incident handlers and Business Continuity professionals looking to use testing as part of their testing regimes
- Penetration testers
- Ethical hackers
- Cybersecurity professionals

Course agenda

Duration: 5 days

Day 1 | Introduction to Penetration Testing, ethics, planning and scoping

- Course objectives and structure
- Penetration Testing principles
- Legal and ethical issues
- Fundamental principles of information security and risk management
- Penetration Testing approaches
- Penetration Testing phases
- Management of a Penetration Test

Day 2 | Technical foundation knowledge and techniques (with practical exercises in all areas)

- Technical foundation knowledge

Day 3 | Conducting a Penetration Test (using tools and techniques) and reviewing testing areas

- Conducting a penetration test – Infrastructure testing
- Conducting a penetration test – Web application penetration testing
- Conducting a penetration test – Mobile testing
- Conducting a penetration test – Social engineering testing
- Conducting a penetration test – Physical security testing

Day 4 | Analyzing results from testing, reporting and follow up

- Documentation of the test quality review and reporting
- Action plans and follow up
- Managing a test program
- Competence and evaluation of penetration testers
- Capture the flag exercises
- Closing the training

Day 5 | Certification Exam



Learning objectives

- Learn how to interpret and illustrate the main Penetration Testing concepts and principles
- Understand the core technical knowledge needed to organize and carry out an effective set of Pen Tests
- Learn how to effectively plan a Penetration Test and identify a scope which is suitable and appropriate based on risk
- Acquire hands-on practical skills and knowledge on relevant tools and techniques used to efficiently conduct a Penetration Testing
- Learn how to effectively manage the time and resources needed to scale a specific Penetration Test

Examination

Duration: 3 hours

The "PECB Certified Lead Pen Test Professional" exam fully meets the requirements of the PECB Examination and Certification Programme (ECP). The exam covers the following competency domains:

Domain 1 | Fundamental principles and concepts in Penetration Testing

Domain 2 | Technical foundations for Penetration Testing

Domain 3 | Scoping and planning a Penetration Test

Domain 4 | Conducting a Penetration Test including test types, tools and methods

Domain 5 | Specific Penetration Testing types and techniques (infrastructure, application, mobile technology and social engineering)

Domain 6 | Analyzing results and the reporting process

Domain 7 | Penetration Test follow up

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 Pen Testing certifications and the PECB certification process, please refer to the Certification Rules and Policies.

Credential	Exam	Professional experience	Pen Testing experience	Other requirements
PECB Certified Provisional Pen Test Professional	PECB Certified Lead Pen Test Professional exam or equivalent	None	None	Signing the PECB Code of Ethics
PECB Certified Pen Test Professional	PECB Certified Lead Pen Test Professional exam or equivalent	**Two years:** One year of work experience in Pen Testing	Pen Testing activities: a total of 200 hours	Signing the PECB Code of Ethics
PECB Certified Lead Pen Test Professional	PECB Certified Lead Pen Test Professional exam or equivalent	**Five years:** Two years of work experience in Pen Testing	Pen Testing activities: a total of 300 hours	Signing the PECB Code of Ethics

General information

- Certification and examination fees are included in the price of the training course
- 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