PECB Where Excellence Meets Recognition



PECB Certified Advanced Penetration Tester

Master advanced, hands-on penetration testing to identify vulnerabilities and validate security controls across complex environments.

Why should you attend?

As cyber threats become more sophisticated, organizations need professionals who can realistically assess and challenge modern defenses. The Certified Advanced Penetration Tester course is designed for experienced cybersecurity practitioners seeking to build advanced, hands-on skills for testing and strengthening complex enterprise environments.

The course focuses on real-world attack techniques through structured instruction and practical labs, covering advanced exploitation, modern Active Directory attacks, lateral movement, evasion, post-exploitation, and vulnerability chaining within monitored networks. Participants learn to evaluate security controls from an attacker's perspective and conduct effective penetration testing and adversarial assessments.

Earning the PECB Certified Advanced Penetration Tester credential validates your ability to perform in-depth technical assessments, simulate advanced attack scenarios, and deliver actionable findings that support organizational risk management. Ideal for penetration testers, red team members, and senior cybersecurity professionals, this course equips you to execute advanced testing, bypass modern defenses in a controlled manner, support red and purple team exercises, and strengthen detection and response capabilities.



Who should attend?

This training course is intended for:

- Experienced penetration testers seeking to further develop advanced technical capabilities
- Red team members and adversary simulation analysts aiming to enhance their assessment techniques
- Security consultants responsible for conducting complex and high-impact technical assessments
- Threat hunters and incident responders seeking deeper insight into advanced attacker techniques
- Security architects and engineers involved in designing, testing, and validating security controls
- Cybersecurity professionals preparing for senior technical roles or advanced certifications that require hands-on experience in complex attack scenarios

Course agenda

Duration: 5 days

Day 1 | Advanced reconnaissance and threat modeling

- Training course objectives and structure
- Advanced Open Source Intelligence (OSINT)
- Network mapping and service enumeration
- Web application architecture analysis

Day 2 | Advanced web exploitation and initial access

- Fuzzing and input validation attacks
- Client-side attacks and injection
- Remote code execution (RCE)
- Shell stabilization and persistence

Day 3 | Post-exploitation, privilege escalation, and credential attacks

- Advanced authentication attacks
- Linux post-exploitation
- Evasion and defense avoidance

Day 4 | Active Directory, windows escalation, and pivoting

- Active Directory (AD) reconnaissance
- Compromising Active Directory and lateral movement
- Windows local privilege escalation
- Network pivoting and tunneling
- Closing of the training course

Day 5 | Certification exam



Learning objectives

By the end of this training course, participants will be able to:

- Execute advanced exploitation to assess hardened targets and complex attack surfaces
- Establish and maintain footholds using persistence and covert communication channels
- Apply privilege escalation and lateral movement across systems and Active Directory domains
- Employ evasion strategies to reduce detection by modern security controls and monitoring
- Plan and conduct realistic red team operations with professional reporting and remediation guidance

Examination

Duration: 3 hours

The "PECB Certified Advanced Penetration Tester" exam fully meets the PECB Examination and Certification Program (ECP) requirements. It covers the following competency domains:

Domain 1 | Passive and active reconnaissance

Domain 2 | Threat modeling and vulnerability identification

Domain 3 | Exploitation and initial access techniques

Domain 4 | Post-exploitation techniques and data exfiltration

Domain 5 | Documentation and reporting

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

After passing the exam, you can apply for one of the credentials in the table below. You will receive a certificate once you fulfill all the requirements of the selected credential.

Credential	Exam	Professional experience	Project experience	Other requirements
PECB Certified Advanced Penetration Tester (CAPT)	PECB Certified Advanced Penetration Tester exam or equivalent	Five years: two years of work experience in penetration testing and cybersecurity	300 hours	Signing the PECB Code of Ethics

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

General information

- Certificate and examination fees are included in the price of the training course.
- Participants will receive more than 300 pages of comprehensive training materials, including practical examples, exercises, and quizzes.
- Participants who have attended the training course will receive an attestation of course completion worth 31 Continuing Professional Development (CDP) credits.
- Candidates who have completed the training course with one of our partners and failed the first exam attempt are eligible to retake the exam for free within a 12-month period from the course completion date, because the fee paid for the training course includes a first exam attempt and one retake. Otherwise, retake fees apply.