CompTIA PenTest+¬ Training

Course: **00067**
Filter: **Beginner**
Duration: **4 days**
Category:: **Gouvernance, Risk and Compliance**
Price: **3000,00 €**

About Course

The CompTIA PenTest+ training course prepares IT professionals to pass the PenTest+ PT0-002 certification exam and develop the skills necessary for effective penetration testing. The course covers planning, information gathering, attacks and exploits, reporting tools and code analysis. Participants should have intermediate knowledge of information security concepts and practical experience securing various computing environments. Successful completion of this course and passing the exam will result in the CompTIA PenTest+ certification.

What you'll learn

- Planning and Scoping.
- Information Gathering and Vulnerability Scanning.
- Attacks and Exploits.
- Reporting and Communication.
- Tools and Code Analysis.

Pre-requisites

- To ensure your success in this course, you should have the following:
- Intermediate knowledge of information security concepts, including but not limited to identity and access management (IAM), cryptographic concepts and implementations, computer networking concepts and implementations, and standard security technologies.

- Practical experience securing various computing environments, including small to medium businesses and enterprise environments.
- Individuals seeking the CompTIA PenTest+ certification should also have three to four years of hands-on experience performing penetration tests, vulnerability assessments, and vulnerability management.

Curriculum

Module 1: Planning and Scoping

- Planning and Scoping Compare and contrast governance, risk, and compliance concept
- Explain the importance of scoping and organizational/customer requirements
- Given a scenario, demonstrate an ethical hacking mindset by maintaining professionalism and integrity

Module 2: Information Gathering and Vulnerability Scanning

- Given a scenario, perform passive reconnaissance
- Given a scenario, perform active reconnaissance
- Given a scenario, analyze the results of a reconnaissance exercise

Module 3: Attacks and Exploits

- Given a scenario, research attack vectors and perform network attacks
- Given a scenario, research attack vectors and perform wireless attacks
- Given a scenario, research attack vectors and perform wireless attacks
- Given a scenario, research attack vectors and perform application-based attacks
- Given a scenario, research attack vectors and perform attacks on cloud technologies
- Explain common attacks and vulnerabilities against specialized systems
- Given a scenario, perform a social engineering or physical attack
- Given a scenario, perform post-exploitation techniques

Module 4: Reporting and Communication

- Compare and contrast important components of written reports
- Given a scenario, analyze the findings and recommend the appropriate remediation within a report
- Explain the importance of communication during the penetration testing process
- Explain post-report delivery activities

Module 5: Tools and Code Analysis

- Tools and Code Analysis
- Given a scenario, analyze a script or code sample for use in a penetration test
- Explain the use cases of the following tools during the phases of a penetration test