CompTIA® PenTest+®

Course Code: PenTes; Duration: 5 days; Instructor-led

WHAT YOU WILL LEARN

Security remains one of the hottest topics in IT and other industries. It seems that each week brings news of some new breach of privacy or security. As organizations scramble to protect themselves and their customers, the ability to conduct penetration testing is an emerging skill set that is becoming ever more valuable to the organizations seeking protection, and ever more lucrative for those who possess these skills. In this course, you will be introduced to some general concepts and methodologies related to pen testing, and you will work your way through a simulated pen test for a fictitious company.

This course can also assist you if you are pursuing the CompTIA PenTest+ certification, as tested in exam PT0-001. The course is designed to provide content and activities that correlate to the exam objectives, and therefore can be a resource as you prepare for the examination.

AUDIENCE

This course is designed for IT professionals who want to develop penetration testing skills to enable them to identify information-system vulnerabilities and effective remediation techniques for those vulnerabilities. Target students who also need to offer practical recommendations for action to properly protect information systems and their contents will derive those skills from this course.

This course is also designed for individuals who are preparing to take the CompTIA PenTest+ certification exam PT0-001, or who plan to use PenTest+ as the foundation for more advanced security certifications or career roles. Individuals seeking this certification should have three to four years of hands-on experience performing penetration tests, vulnerability assessments, and vulnerability management.

PREREQUISITES

To ensure your success in this course, you should have:

- 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 common security technologies.
- Practical experience in securing various computing environments, including small to medium businesses, as well as enterprise environments.

You can obtain this level of skills and knowledge by taking the CompTIA® Security+® (Exam SY0-501) course or by obtaining the appropriate industry certification.

METHODOLOGY

This program will be conducted with interactive lectures, PowerPoint presentation, discussion and practical exercise.

COURSE OBJECTIVES

After you complete this course, you will be able to plan, conduct, analyze, and report on penetration tests.

You will:

- Plan and scope penetration tests.
- Conduct passive reconnaissance.
- Perform non-technical tests to gather information.
- Conduct active reconnaissance.
- Analyze vulnerabilities.
- Penetrate networks.
- Exploit host-based vulnerabilities.
- Test applications.
- Complete post-exploit tasks.
- Analyze and report pen test results.

OUTLINES

Module 1: Planning and Scoping Penetration Tests

- Introduction to Penetration Testing Concepts
- Plan a Pen Test Engagement
- Scope and Negotiate a Pen Test Engagement
- Prepare for a Pen Test Engagement

Module 2: Conducting Passive Reconnaissance

- Gather Background Information
- Prepare Background Findings for Next Steps

Module 3: Performing Non-Technical Tests

- Perform Social Engineering Tests
- Perform Physical Security Tests on Facilities

Module 4: Conducting Active Reconnaissance

- Scan Networks
- Enumerate Targets
- Scan for Vulnerabilities
- Analyze Basic Scripts

Module 5: Analyzing Vulnerabilities

- Analyze Vulnerability Scan Results
- Leverage Information to Prepare for Exploitation

Module 6: Penetrating Networks

- Exploit Network-Based Vulnerabilities
- Exploit Wireless and RF-Based Vulnerabilities
- Exploit Specialized Systems

Module 7: Exploiting Host-Based Vulnerabilities

- Exploit Windows-Based Vulnerabilities
- Exploit *nix-Based Vulnerabilities

Module 8: Testing Applications

- Exploit Web Application Vulnerabilities
- Test Source Code and Compiled Apps

Module 9: Completing Post-Exploit Tasks

- Use Lateral Movement Techniques
- Use Persistence Techniques
- Use Anti-Forensics Techniques

Module 10: Analyzing and Reporting Pen Test Results

- Analyze Pen Test Data
- Develop Recommendations for Mitigation Strategies
- Write and Handle Reports
- Conduct Post-Report-Delivery Activities

Appendix A: Taking the Exams

Appendix B: Mapping Course Content to CompTIA® PenTest+® (Exam PT0-001)