CompTIA Penetration Testing (PenTest+) Certification (Exam PT0-001)

Overview

"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.

Prerequisite Comments

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+ Certification course or by obtaining the appropriate industry certification.

Target 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.

Course Objectives

After completing this course, you will be able to plan, conduct, analyze, and report on penetration tests, including the ability to…
Plan and scope penetration tests
Conduct passive reconnaissance
Perform non-technical tests to gather information
Conductive active reconnaissance
Analyze vulnerabilities
Penetrate networks
Exploit host-based vulnerabilities
Test applications Complete post-exploit tasks
Analyze and report pen test results

Course Outline

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

2 - Conducting Passive Reconnaissance

Gather Background Information
Prepare Background Findings for Next Steps

3 - Performing Non-Technical Tests

Perform Social Engineering Tests
Perform Physical Security Tests on Facilities

4 - Conducting Active Reconnaissance

Scan Networks
Enumerate Targets
Scan for Vulnerabilities
Analyze Basic Scripts

5 - Analyzing Vulnerabilities

Analyze Vulnerability Scan Results
Leverage Information to Prepare for Exploitation

6 - Penetrating Networks

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

7 - Exploiting Host-Based Vulnerabilities

Exploit Windows-Based Vulnerabilities
Exploit *nix-Based Vulnerabilities

8 - Testing Applications

Exploit Web Application Vulnerabilities
Test Source Code and Compiled Apps

9 - Completing Post-Exploit Tasks

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

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