Module Title : CompTIA PenTest+ Certification Training

Duration : 5 days

Overview

As organizations scramble to protect themselves and their customers against privacy or security breaches, 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 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 will assist you if you are pursuing the CompTIA PenTest+ certification, as tested in exam PT0-001.

Job Roles

- Penetration Tester
- Vulnerability Tester
- Security Analyst (II)
- Vulnerability Assessment Analyst
- Network Security Operations
- Application Security Vulnerability

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 CompTIA® Security+® (Exam SY0-501) course or by obtaining the appropriate industry certification.

Course Content

Lesson 1: Planning and Scoping Penetration Tests

Topic A: Introduction to Penetration Testing Concepts

Topic B: Plan a Pen Test Engagement

Topic C: Scope and Negotiate a Pen Test Engagement

Topic D: Prepare for a Pen Test Engagement

Lesson 2: Conducting Passive Reconnaissance

Topic A: Gather Background Information

Topic B: Prepare Background Findings for Next Steps

Lesson 3: Performing Non-Technical Tests

Topic A: Perform Social Engineering Tests

Topic B: Perform Physical Security Tests on Facilities

Lesson 4: Conducting Active Reconnaissance

Topic A: Scan Networks

Topic B: Enumerate Targets

Topic C: Scan for Vulnerabilities

Topic D: Analyze Basic Scripts

Lesson 5: Analyzing Vulnerabilities

Topic A: Analyze Vulnerability Scan Results

Topic B: Leverage Information to Prepare for Exploitation

Lesson 6: Penetrating Networks

Topic A: Exploit Network-Based Vulnerabilities

Topic B: Exploit Wireless and RF-Based Vulnerabilities

Topic C: Exploit Specialized Systems

Lesson 7: Exploiting Host-Based Vulnerabilities

Topic A: Exploit Windows-Based Vulnerabilities

Topic B: Exploit *Nix-Based Vulnerabilities

Lesson 8: Testing Applications

Topic A: Exploit Web Application Vulnerabilities

Topic B: Test Source Code and Compiled Apps

Lesson 9: Completing Post-Exploit Tasks

Topic A: Use Lateral Movement Techniques

Topic B: Use Persistence Techniques

Topic C: Use Anti-Forensics Techniques

Lesson 10: Analyzing and Reporting Pen Test Results

Topic A: Analyze Pen Test Data

Topic B: Develop Recommendations for Mitigation Strategies

Topic C: Write and Handle Reports

Topic D: Conduct Post-Report-Delivery Activities

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