Course duration

- 5 days

Course Benefits

- 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.

Course Outline

1. Planning and Scoping Penetration Tests
    1. Introduction to Penetration Testing Concepts
    2. Plan a Pen Test Engagement
    3. Scope and Negotiate a Pen Test Engagement
    4. Prepare for a Pen Test Engagement
2. Conducting Passive Reconnaissance
    1. Gather Background Information
    2. Prepare Background Findings for Next Steps
3. Performing Non-Technical Tests
    1. Perform Social Engineering Tests
    2. Perform Physical Security Tests on Facilities
4. Conducting Active Reconnaissance
    1. Scan Networks
    2. Enumerate Targets
    3. Scan for Vulnerabilities
    4. Analyze Basic Scripts
5. Analyzing Vulnerabilities
    1. Analyze Vulnerability Scan Results
    2. Leverage Information to Prepare for Exploitation
6. Penetrating Networks
    1. Exploit Network-Based Vulnerabilities
    2. Exploit Wireless and RF-Based Vulnerabilities
    3. Exploit Specialized Systems

7. Exploiting Host-Based Vulnerabilities
    1. Exploit Windows-Based Vulnerabilities
    2. Exploit *nix-Based Vulnerabilities
8. Testing Applications
    1. Exploit Web Application Vulnerabilities
    2. Test Source Code and Compiled Apps
9. Completing Post-Exploit Tasks
    1. Use Lateral Movement Techniques
    2. Use Persistence Techniques
    3. Use Anti-Forensics Techniques
10. Analyzing and Reporting Pen Test Results
    1. Analyze Pen Test Data
    2. Develop Recommendations for Mitigation Strategies
    3. Write and Handle Reports
    4. Conduct Post-Report-Delivery Activities

Class Materials

Each student will receive a comprehensive set of materials, including course notes and all the class examples.

Class Prerequisites

Experience in the following *is required* for this CompTIA class:

- 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.