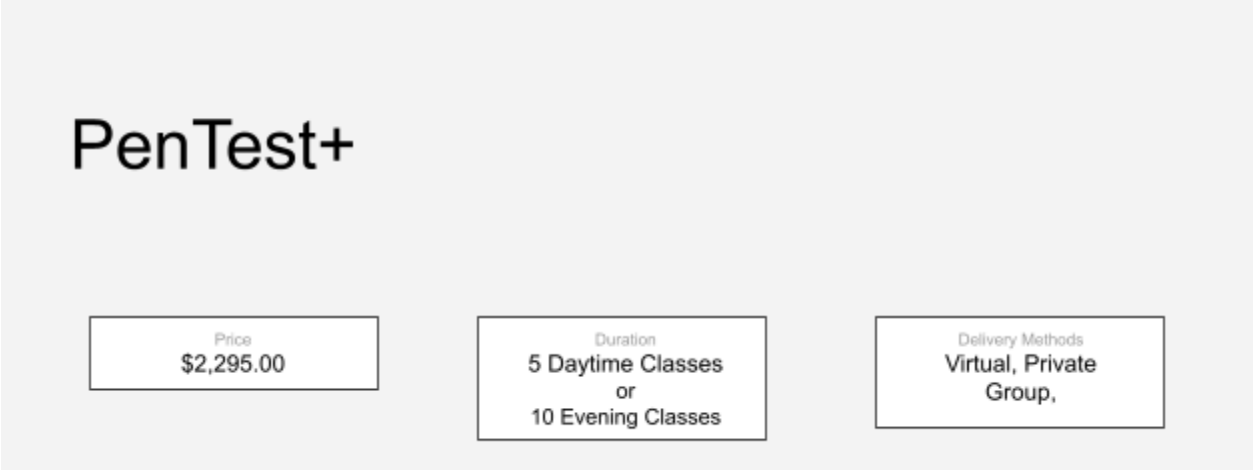

CAREER SKILLS+™

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 will also prepare you for the CompTIA PenTest+ certification exam PT0-002.

Who Should Attend

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 PT0-002, 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 Prerequisites

There are no prerequisites for this course.

Course Objectives

On course completion, participants will be able 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.

Agenda

1 - Scoping Organizational/Customer Requirements
Define Organizational PenTesting
Acknowledge Compliance Requirements
Compare Standards and Methodologies
Describe Ways to Maintain Professionalism
2 - Defining the Rules of Engagement
Assess Environmental Considerations
Outline the Rules of Engagement
Prepare Legal Documents
3 - Footprinting and Gathering Intelligence
Discover the Target
Gather Essential Data
Compile Website Information
Discover Open-Source Intelligence Tool
4 - Evaluating Human and Physical Vulnerabilities
Exploit the Human Psyche

Summarize Physical Attacks
Use Tools to Launch a Social Engineering Attack
5 - Preparing the Vulnerability Scan
Plan the Vulnerability Scan
Detect Defenses
Utilize Scanning Tools
6 - Scanning Logical Vulnerabilities
Scan Identified Targets
Evaluate Network Traffic
Uncover Wireless Assets
7 - Analyzing Scanning Results
Discover Nmap and NSE
Enumerate Network Hosts
Analyze Output from Scans
8 - Avoiding Detection and Covering Tracks
Evade Detection
Use Steganography to Hide and Conceal
Establish a Covert Channel
9 - Exploiting the LAN and Cloud
Enumerating Hosts
Attack LAN Protocols
Compare Exploit Tools
Discover Cloud Vulnerabilities
Explore Cloud-Based Attacks
10 - Testing Wireless Networks
Discover Wireless Attacks
Explore Wireless Tools
11 - Targeting Mobile Devices
Recognize Mobile Device Vulnerabilities
Launch Attacks on Mobile Devices
Outline Assessment Tools for Mobile Devices
12 - Attacking Specialized Systems
Identify Attacks on the IoT
Recognize Other Vulnerable Systems
Explain Virtual Machine Vulnerabilities
13 - Web Application-Based Attacks
Recognize Web Vulnerabilities
Launch Session Attacks
Plan Injection Attacks
Identify Tools
14 - Performing System Hacking
System Hacking
Use Remote Access Tools
Analyze Exploit Code
15 - Scripting and Software Development
Analyzing Scripts and Code Samples
Create Logic Constructs
Automate Penetration Testing
16 - Leveraging the Attack: Pivot and Penetrate

Test Credentials
Move Throughout the System
Maintain Persistence
17 - Communicating During the PenTesting Process
Define the Communication Path
Communication Triggers
Use Built-In Tools for Reporting
18 - Summarizing Report Components
Identify Report Audience
List Report Contents
Define Best Practices for Reports
19 - Recommending Remediationc
Employ Technical Controls
Administrative and Operational Controls
Physical Controls
20 - Performing Post-Report Delivery Activities
Post-Engagement Cleanup
Follow-Up Actions