Course Outline

ProTech Professional Technical Services, Inc.

CompTIA PenTest + (Exam PT0-002)

Course Summary

Description

The Official CompTIA PenTest+ Instructor and Student Guides teach the knowledge and skills to understand how to plan and scope a penetration testing engagement including vulnerability scanning, understand legal and compliance requirements, analyze results, and produce a written report with remediation techniques and prepare candidates to take the CompTIA PenTest+ certification exam.

Objectives

CompTIA PenTest+ candidates will be able to:

- Plan and scope a penetration testing engagement.
- Understand legal and compliance requirements.
- Perform vulnerability scanning and penetration testing using appropriate tools and techniques, and then analyze the results.
- Produce a written report containing proposed remediation techniques, effectively communicate results to the management team, and provide practical recommendations.

Topics

- Scoping Organizational/Customer Requirements
- Defining the Rules of Engagement
- Footprinting and Gathering Intelligence
- Evaluating Human and Physical Vulnerabilities
- Preparing the Vulnerability Scan
- Scanning Logical Vulnerabilities
- Analyzing Scanning Results
- Avoiding Detection and Covering Tracks
- Exploiting the LAN and Cloud
- Testing Wireless Networks
- Targeting Mobile Devices
- Attacking Specialized Systems
- Web Application-Based Attacks
- Performing System Hacking
- Scripting and Software Development
- Leveraging the Attack: Pivot and Penetrate
- Communicating during the PenTesting Process
- Summarizing Report Components
- Recommending Remediation
- Performing Post-Report Delivery Activities

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.

Prerequisites

There are no requirements, but it is recommended that attendees have experience in Network+, Security+, or equivalent knowledge as well as a minimum of 3-4 years of hans-on information security or related experience.

Duration

Five days

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically

CompTIA PenTest + (Exam PT0-002)

Course Outline

I. Scoping Organizational/Customer Requirements

A. Definte Organizational PenTesting
B. Acknowledge Compliance Requirements
C. Compare Standards and Methodologies
D. Describe Ways to Maintain Professionalism

II. Defining the Rules of Engagement

A. Assess Environmental Considerations
B. Outline the Rules of Engagement
C. Prepare Legal Documents

III. Footprinting and Gathering Intelligence

A. Discover the Target
B. Gather Essential Data
C. Compile Website Information
D. Discover Open-Source Intelligence Tools

IV. Evaluating Human and Physical Vulnerabilities

A. Exploit the Human Psyche
B. Summarize Physical Attacks
C. Use Tools to Launch a Social Engineering Attack

V. Preparing the Vulnerability Scan

A. Plan the Vulnerability Scan
B. Detect Defenses
C. Utilize Scanning Tools

VI. Scanning Logical Vulnerabilities

A. Scan Identified Targests
B. Evaluate Network Traffic
C. Uncover Wireless Assets

VII. Analyzing Scanning Results

A. Discover Nmap and NSE
B. Enumerate Network Hosts
C. Analyze Output from Scans

VIII. Avoiding Detection and Covering Tracks

A. Evade Detection
B. Use Steganography to Hide and Conceal
C. Establish a Covert Channel

IX. Exploiting the LAN and Cloud

A. Enumerating Hosts
B. Attack LAN Protocols
C. Compare Exploit Tools
D. Discover Cloud Vulnerabilities

X. Testing Wireless Networks

A. Discover Wireless Attacks
B. Explore Wireless Tools

XI. Targeting Mobile Devices

A. Recognize Mobile Device Vulnerabilities
B. Launch Attacks on Mobile Devices
C. Outline Assessment Tools for Mobile Devices

XII. Attaching Specialized Systems

A. Identify Attacks on the IoT
B. Recognize Other Vulnerable Systems
C. Explain Virtual Machine Vulnerabilities

XIII. Web Application-Based Attacks

A. Recognize Web Vulnerabilities
B. Launch Session Attacks
C. Plan Injection Attacks
D. Identify Tools

XIV. Performing System Hacking

A. System Hacking
B. Use Remote Access Tools
C. Analyze Exploit Code

XV. Scripting and Software Development

A. Analyzing Scripts and Code Samples
B. Create logic Constructs
C. Automate Penetration Testing

XVI. Leverating the Attack: Pivot and Penetrate

A. Test Credentials
B. Move Throughout the System
C. Maintain Persistence

XVII. Communication During the PenTesting Process

A. Define the Communication Path
B. Communication Triggers
C. Use Built-In Tools for Reporting

XVIII. Summarizing Report Components

A. Identify Report Audience
B. List Report Contents
C. Define Best Practices Reports

XIX. Recommending Remediation

A. Employ Technical Controls
B. Administrative and Operational Controls
C. Physical Controls

XX. Performing Post-Report Delivery

A. Post-Engagement cleanup
B. Follow-Up Actions

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically