CompTIA: PenTest+

Course ID #: 7000-594-ZZ-Z
Hours: 35

Course Content

Course Description:

PenTest+ assesses the most up-to-date penetration testing, and vulnerability assessment and management skills necessary to determine the resiliency of the network against attacks.

At Course Completion:

Students 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

Prerequisites:

CompTIA: Security+ or equivalent knowledge and experience.

Target Student:

- Penetration Tester
- Security Consultant
- Cloud Penetration Tester
- Web App Penetration Tester
- Cloud Security Specialist
- Network & Security Specialist
- Information Security Engineer
- Security Analyst

Topics:

Lesson 1: Scoping Organizational/Customer Requirements

- Topic 1A: Define Organizational PenTesting
- Topic 1B: Acknowledge Compliance Requirements
- Topic 1C: Compare Standards and Methodologies
- Topic 1D: Describe Ways to Maintain Professionalism

Lesson 2:Defining theRules of Engagement

- Topic 2A: Assess Environmental Considerations
- Topic 2B: Outline the Rules of Engagement
- Topic 2C: Prepare Legal Documents

Lesson 3: Footprinting and Gathering Intelligence

- Topic 3A: Discover the Target
- Topic 3B: Gather Essential Data
- Topic 3C: Compile Website Information
- Topic 3D: Discover Open-Source Intelligence Tools

Lesson 4: Evaluating Human and Physical Vulnerabilities

- Topic 4A: Exploit the Human Psyche
- Topic 4B: Summarize Physical Attacks
- Topic 4C: Use Tools to Launch a Social Engineering Attack

Lesson 5: Preparing the Vulnerability Scan

- Topic 5A: Plan the Vulnerability Scan
- Topic 5B: Detect Defenses
- Topic 5C: Utilize Scanning Tools

Lesson 6: Scanning Logical Vulnerabilities

- Topic 6A: Scan Identified Targets
- Topic 6B: Evaluate Network Traffic
- Topic 6C: Uncover Wireless Assets

Lesson 7: Analyzing Scanning Results

- Topic 7A: Discover Nmap and NSE
- Topic 7B: Enumerate Network Hosts
- Topic 7C: Analyze Output from Scans

Lesson 8: Avoiding Detection and Covering Tracks

- Topic 8A: Evade Detection
- Topic 8B: Use Steganography to Hide and Conceal
- Topic 8C: Establish a Covert Channel

Lesson 9: Exploiting the LAN and Cloud

- Topic 9A: Enumerating Hosts
- Topic 9B: Attack LAN Protocols
- Topic 9C: Compare Exploit Tools
- Topic 9D: Discover Cloud Vulnerabilities
- Topic 9E: Explore Cloud-Based Attacks

Lesson 10: Testing Wireless Networks

- Topic 10A: Discover Wireless Attacks
- Topic 10B: Explore Wireless Tools

Lesson 11: Targeting Mobile Devices

- Topic 11A: Recognize Mobile Device Vulnerabilities
- Topic 11B: Launch Attacks on Mobile Devices
- Topic 11C: Outline Assessment Tools for Mobile Devices

Lesson 12: Attacking Specialized Systems

- Topic 12A: Identify Attacks on the IoT
- Topic 12B: Recognize Other Vulnerable Systems
- Topic 12C: Explain Virtual Machine Vulnerabilities

Lesson 13: Web Application-Based Attacks

- Topic 13A: Recognize Web Vulnerabilities
- Topic 13B: Launch Session Attacks
- Topic 13C: Plan Injection Attacks
- Topic 13D: Identify Tools

Lesson 14: Performing System Hacking

- Topic 14A: System Hacking
- Topic 14B: Use Remote Access Tools
- Topic 14C: Analyze Exploit Code

Lesson 15: Scripting and Software Development

- Topic 15A: Analyzing Scripts and Code Samples
- Topic 15B: Create Logic Constructs
- Topic 15C: Automate Penetration Testing

Lesson 16: Leveraging the Attack: Pivot and Penetrate

- Topic 16A: Test Credentials
- Topic 16B: Move Throughout the System
- Topic 16C: Maintain Persistence

Lesson 17: Communicating During the PenTesting Process

- Topic 17A: Define the Communication Path
- Topic 17B: Communication Triggers
- Topic 17C: Use Built-In Tools for Reporting

Lesson 18: Summarizing Report Components

- Topic 18A: Identify Report Audience
- Topic 18B: List Report Contents
- Topic 18C: Define Best Practices for Reports

Lesson 19: Recommending Remediation

- Topic 19A: Employ Technical Controls
- Topic 19B: Administrative and Operational Controls
- Topic 19C: Physical Controls

Lesson 20: Performing Post-Report Delivery Activities

- Topic 20A: Post-Engagement Cleanup
- Topic 20B: Follow-Up Actions