COURSE SYLLABUS

CompTIA PenTest+ Certification Training

Learn penetration testing methodologies and tools to simulate real-world cyberattacks—and prepare for the CompTIA PenTest+ certification (PT0-003).

> Group classes in Washington, DC and onsite training is available for this course.
> For more information, email onsite@graduateschool.edu or visit: https://www.graduateschool.edu/courses/comptia-pentest-certification-training

CustomerRelations@graduateschool.edu • (888) 744-4723

Course Outline

Lesson 1: Scoping Organizational/Customer Requirements

- Define Organizational PenTesting
- Acknowledge Compliance Requirements
- Compare Standards and Methodologies
- Describe Ways to Maintain Professionalism

Lesson 2: Defining the Rules of Engagement

- Assess Environmental Considerations
- Outline the Rules of Engagement
- Prepare Legal Documents

Lesson 3: Footprinting and Gathering Intelligence

- Discover the Target
- Gather Essential Data
- Compile Website Information
- Discover Open-Source Intelligence Tools

Lesson 4: Evaluating Human and Physical Vulnerabilities

- Exploit the Human Psyche
- Summarize Physical Attacks
- Use Tools to Launch a Social Engineering Attack

Lesson 5: Preparing the Vulnerability Scan

- Plan the Vulnerability Scan
- Detect Defenses
- Utilize Scanning Tools

Lesson 6: Scanning Logical Vulnerabilities

- Scan Identified Targets
- Evaluate Network Traffic
- Uncover Wireless Assets

Lesson 7: Analyzing Scanning Results

- Discover Nmap and NSE
- Enumerate Network Hosts
- Analyze Output from Scans

Lesson 8: Avoiding Detection and Covering Tracks

- Evade Detection
- Use Steganography to Hide and Conceal
- Establish a Covert Channel

Lesson 9: Exploiting the LAN and Cloud

- Enumerate Hosts
- Attack LAN Protocols
- Compare Exploit Tools
- Discover Cloud Vulnerabilities
- Explore Cloud-Based Attacks

Lesson 10: Testing Wireless Networks

- Discover Wireless Attacks
- Explore Wireless Tools

Lesson 11: Targeting Mobile Devices

- Recognize Mobile Device Vulnerabilities
- Launch Attacks on Mobile Devices
- Outline Assessment Tools for Mobile Devices

Lesson 12: Attacking Specialized Systems

- Identify Attacks on the IoT
- Recognize Other Vulnerable Systems
- Explain Virtual Machine Vulnerabilities

Lesson 13: Web Application-Based Attacks

- Recognize Web Vulnerabilities
- Launch Session Attacks
- Plan Injection Attacks
- Identify Tools

Lesson 14: Performing System Hacking

- System Hacking
- Use Remote Access Tools
- Analyze Exploit Code

Lesson 15: Scripting and Software Development

- Analyzing Scripts and Code Samples
- Create Logic Constructs

- Automate Penetration Testing

Lesson 16: Leveraging the Attack: Pivot and Penetrate

- Test Credentials
- Move Throughout the System
- Maintain Persistence

Lesson 17: Communicating During the PenTesting Process

- Define the Communication Path
- Communication Triggers
- Use Built-In Tools for Reporting

Lesson 18: Summarizing Report Components

- Identify Report Audience
- List Report Contents
- Define Best Practices for Reports

Lesson 19: Recommending Remediation

- Employ Technical Controls
- Administrative and Operational Controls
- Physical Controls

Lesson 20: Performing Post-Report Delivery Activities

- Post-Engagement Cleanup
- Follow-Up Actions