CompTIA: PenTest+ On-Demand

Course ID #: 7000-1151-ZZ-Z
Hours: 35
Delivery Method: Group Internet Based

Course Content

Description:

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 can also assist you if you are pursuing the CompTIA PenTest+ certification, as tested in PT0-001. The course is designed to provide content and activities that correlate to the exam objectives, and therefore can be a resource as you prepare for the examination.

Objectives:

Upon successful completion of this course, students will:

- Plan, scope, and perform information gathering as part of a penetration test.
- Perform attacks that are aligned to and fulfill legal and compliance requirements.
- Perform each phase of a penetration test using and modifying appropriate tools and use the appropriate tactics, techniques, and procedures.
- Analyze the results of each phase of a penetration test to develop a written report, effectively communicate findings to stakeholders and provide practical recommendations.

Prerequisites:

10+ years of general hands-on IT experience, with at least five of those years being broad hands-on IT security experience, and 3 - 4 years in a penetration tester job role.

Target Audience:

IT Security Professionals

CompTIA: PenTest+ On-Demand

Course ID #: 7000-1151-ZZ-Z
Hours: 35
Delivery Method: Group Internet Based

Topics:

1.0 Penetration Testing: Before You Begin

1.1 Professional Conduct and Penetration Testing

- What Is Penetration Testing?
- Ethics, Legal, and Compliance Considerations of Penetration Testing
- Importance and ples of Documentation
- Scoping and Authorization
- Overview of the PenTest Report
- Live Lab: Exploring the Lab Environment
- Lesson Review

1.2 Collaboration and Communication

- Collaboration and Communication Overview
- PenTest Team Roles and Responsibilities
- Communicating with Clients and Team Members
- Peer Review
- Stakeholder Alignment
- Root Cause Analysis
- Escalation Path
- Secure Distribution
- Articulation of Risk, Severity, and Impact
- Goal Reprioritization
- Business Impact Analysis
- Client Acceptance
- Lesson Review

1.3 Testing Frameworks and Methodologies

- Testing Frameworks and Methodologies Overview
- Open Source Security Testing Methodology Manual (OSSTMM)
- Council of Registered Ethical Security Testers (CREST)
- Penetration Testing Execution Standard (PTES)
- MITRE ATT&CK
- Open Web Application Security Project (OWASP) Top 10
- OWASP Mobile Application Security Verification Standard (MASVS)
- Purdue Model
- Threat Modeling Frameworks
- Lesson Review

1.4 Introduction to Scripting for Penetration Testing

- Scripting Languages
- Bash Shell and Bash Script
- Python
- PowerShell
- Use of Libraries, Functions, and Classes
- Logic Constructs
- Create Logic Constructs
- Lesson Review

1.5 Module Quiz

2.0 Applying Pre-Engagement Activities

2.1 Define the Scope

- Regulations, Frameworks, and Standards
- Rules of Engagement
- Agreement Types
- Target Selection
- Lesson Review

2.2 Compare Types of Assessments

- Types of Assessments Overview
- Web and Application Assessments
- Network Assessments
- Activity: Assess Environmental Considerations
- Mobile Assessments
- Cloud Assessments
- Wireless Assessments
- IoT Devices and Penetration Testing
- Information Technology Versus Operational Technology
- Lesson Review

2.3 Utilize the Shared Responsibility Model

- The Shared Responsibility Model Overview
- Hosting Provider Responsibilities
- Customer Responsibilities
- Penetration Tester Responsibilities
- Third-Party Responsibilities
- Lesson Review

2.4 Identify Legal and Ethical Considerations

- Authorization Letters
- Mandatory Reporting Requirements
- Risk to the Penetration Tester
- Documenting Pre-Engagement Activities
- Lesson Review

2.5 Module Quiz

3.0 Enumeration and Reconnaissance

3.1 Information Gathering Techniques

- Active and Passive Reconnaissance
- Tools for Reconnaissance
- Open-Source Intelligence (OSINT)
- Using Shodan
- Previously Breached Password Lists
- Network Reconnaissance
- Basics of Scanning
- Perform Recon with Nmap
- Certificate Transparency Logs
- Information Disclosure
- Search Engine Analysis/Enumeration
- Network Sniffing
- Data Manipulation
- Lesson Review

3.2 Host and Service Discovery Techniques

- What Is Enumeration?
- Host Discovery
- Scripting with Nmap
- Activity: Scripting with Nmap
- Banner Grabbing
- Protocol Enumeration
- Service Discovery
- DNS Enumeration
- Operating System (OS) Fingerprinting
- Perform Enumeration with Nmap
- Live Lab: DNS Enumeration and Reconnaissance
- Lesson Review

3.3 Enumeration for Attack Planning

- Attack Path Mapping
- Manual Enumeration
- Simple Network Management Protocol
- Documenting Enumeration Activities
- Activity: Document Enumeration Activities
- Lesson Review

3.4 Enumeration for Specific Assets

- Directory Enumeration
- User Enumeration
- Wireless Enumeration
- Permission Enumeration
- Secrets Enumeration
- Share Enumeration
- Web Application Firewall (WAF) Enumeration
- Perform a Decoy Scan
- Industrial Control Systems (ICS) Vulnerability Assessment
- Web Crawling/HTML Scraping
- Lesson Review

3.5 Module Quiz

4.0 Scanning and Identifying Vulnerabilities

4.1 Vulnerability Discovery Techniques

- Tools for Vulnerability Discovery
- Types of Scans
- Container Scans
- Application Scans
- Scan for Clear Vulnerabilities
- Network Scans
- Activity: Scan Identified Targets
- Host-Based Scans
- Live Lab: Using Metasploit
- Secrets Scanning
- Wireless Scans
- Use aircrack-ng to Discover Hidden Networks
- Locate a Rogue Wireless Access Point
- Validate Scan, Reconnaissance, and Enumeration Results
- Applied Live Lab: Network Reconnaissance
- Scan for Linux Vulnerabilities
- Lesson Review

4.2 Analyzing Reconnaissance Scanning and Enumeration

- Public Exploit Selection
- Use Scripting to Validate Results
- Lesson Review

4.3 Physical Security Concepts

- Tailgating
- Site Surveys
- Universal Serial Bus (USB) Drops
- Badge Cloning
- Lock Picking
- Documenting Scanning and Identifying Vulnerabilities Activities
- Activity: Identify Physical Security Concepts
- Lesson Review

4.4 Module Quiz

4.5 Checkpoint Review

5.0 Conducting Pentest Attacks

5.1 Prepare and Prioritize Attacks

- Target Prioritization
- High-Value Asset Identification
- Descriptors and Metrics
- End-of-Life Software and Systems
- Default Configurations
- Running Services
- Vulnerable Encryption Methods
- Defensive Capabilities
- Capability Selection
- Exploit Selection and Customization
- Documentation Procedures for Attacks
- Dependencies
- Consideration of Scope Limitations
- Activity: Customize Exploits
- Live Lab: Evaluate EOL Software & Systems
- Applied Live Lab: Exploiting Default Configurations with Responder
- Lesson Review

5.2 Scripting Automation
- Types of Scripting Automation
- PowerShell
- Bash
- Python
- Breach and Attack (BAS)
- Live Lab: Executing Scripts to Automate Tasks
- Lesson Review

5.3 Module Quiz

6.0 Web-based Attacks

6.1 Web-based Attacks
- Web Application Attacks Overview
- Types of Web Application Attacks
- Tools for Performing Web Application Attacks
- Brute-Force Attack
- Collision Attack
- Directory Traversal
- Request Forgery Attacks
- Deserialization Attack
- Injection Attacks
- Activity: Injection Attacks
- Insecure Direct Object Reference
- Session Hijacking
- Arbitrary Code Execution
- File Inclusions
- API Abuse
- JSON Web Token (JWT) Manipulation
- Live Lab: Evaluating a Database Using SQLMap
- Live Lab: Exploiting Directory Traversal
- Live Lab: Performing XSS
- Live Lab: Abusing Insecure Direct Object References
- Live Lab: Performing Lateral Movement
- Live Lab: Performing RFI and LFI Exploitation
- Lesson Review

6.2 Cloud-based Attacks
- Cloud-based Attacks Overview
- Types of Cloud-based Attacks
- Tools for Performing Cloud-based Attacks
- Metadata Service Attacks
- Access Management Misconfigurations
- Third-party Integrations
- Resource Misconfiguration
- Activity: Conduct Resource Misconfiguration Attacks
- Logging Information Exposure
- Image and Artifact Tampering
- Supply Chain Attacks
- Workload Runtime Attacks
- Container Escape
- Trust Relationship Abuse
- Perform and Analyze a SYN Flood Attack
- Lesson Review

6.3 Module Quiz

7.0 Enterprise Attacks

7.1 Perform Network Attacks
- Network Attack Types
- Tools for Performing Network Attacks
- Default Credentials
- On-Path Attack
- Certificate Services
- Misconfigured Services Exploitation
- Virtual Local Area Network (VLAN) Hopping
- Multihomed Hosts
- Relay Attack
- IDS Evasion
- Live Lab: Sniffing Network Traffic
- Applied Live Lab: Exploring the Power of Nmap NSE
- Live Lab: Discovering Vulnerabilities with Netcat
- Applied Live Lab: Performing a Relay Attack
- Lesson Review

7.2 Perform Authentication Attacks

- Authentication Attack Types
- Tools for Performing Authentication Attacks
- Multifactor Authentication (MFA) Fatigue
- Pass-the-Hash Attacks
- Pass-the-Ticket Attacks
- Pass-the-Token Attacks
- Kerberos Attacks
- Lightweight Directory Access Protocol (LDAP) Injection
- Dictionary Attacks
- Crack a Password with John the Ripper
- Brute-Force Attacks
- Mask Attacks
- Password Spraying
- Credential Stuffing
- OpenID Connect (OIDC) Attacks
- Security Assertion Markup Language (SAML) Attacks
- Live Lab: Cracking Passwords
- Lesson Review

7.3 Perform Host-Based Attacks

- Types of Host-Based Attacks
- Tools for Performing Host-Based Attacks
- Privilege Escalation
- Credential Dumping
- Circumventing Security Tools
- Clear Audit Policies
- Misconfigured Endpoints
- Payload Obfuscation
- User-Controlled Access Bypass
- Shell Escape
- Kiosk Escape
- Library Injection
- Process Hollowing and Injection
- Log Tampering
- Unquoted Service Path Injection
- Documenting Enterprise Attacks
- Applied Live Lab: Performing an On-Path (AiTM) Attack
- Live Lab: Performing Privilege Escalation
- Live Lab: Implementing Payload Obfuscation
- Live Lab: Performing SQL Injection
- Live Lab: Investigating with Evil-WinRM
- Live Lab: Exploiting LOLBins
- Live Lab: Implementing Credential Dumping
- Lesson Review

7.4 Module Quiz

7.5 Checkpoint Review

8.0 Specialized Attacks

8.1 Wireless Attacks

- Types of Wireless Attacks
- Tools for Performing Wireless Attacks
- Activity: Explore Wireless Tools
- Wardriving
- Bluetooth
- Evil Twin Attack
- Signal Jamming
- Protocol Fuzzing
- Packet Crafting
- Deauthentication
- Captive Portal
- Wi-Fi Protected Setup (WPS) and Personal Identification (PIN) Attack
- Lesson Review

8.2 Social Engineering Attacks

- Types of Social Engineering Attacks
- Tools for Performing Social Engineering Attacks
- Phishing, Whaling, Spear phishing, and Smishing
- Social Engineering Techniques for Gathering Information
- Watering Hole
- Credential Harvesting
- Live Lab: Performing Social Engineering using SET
- Lesson Review

8.3 Specialized System Attacks

- Types of Specialized System Attacks
- Tools for Performing Specialized System Attacks
- Mobile Attacks
- AI Attacks
- Operational Technology (OT)
- Radio-Frequency Identification (RFID) and Near-Field Communication (NFC)
- Bluejacking
- Conducting Specialized Penetration Testing Attacks
- Lesson Review

8.4 Module Quiz

9.0 Performing Penetration Testing Tasks

9.1 Establish and Maintain Persistence

- Principles of Establishing and Maintaining Persistence
- Scheduled Tasks/cron Jobs
- Service Creation
- Reverse and Bind Shells
- Add New Accounts
- Obtain Valid Account Credentials
- Registry Keys
- Command and Control (C2) Frameworks
- Backdoor
- Activity: Maintain Persistence
- Create a Backdoor with Metasploit
- Rootkit
- Browser Extensions
- Tampering Security Controls
- Live Lab: Configuring Reverse and Bind Shells
- Live Lab: Establishing Persistence and Other Post-Exploitation Activities
- Lesson Review

9.2 Move Laterally through Environments

- Lateral and Horizontal Movement
- Scan for Open Ports from a Remote Computer
- Techniques for Moving Laterally through Environments
- Tools for Moving Laterally through Environments
- Pivoting
- Relay Creation
- Enumeration
- Perform Enumeration of MSSQL with Metasploit
- Service Discovery
- Perform a Scan Using Zenmap
- Bypass Windows Firewall
- Windows Management Instrumentation (WMI)
- Window Remote Management (WinRM)
- Lesson Review

9.3 Staging and Exfiltration

- Fundamentals of Staging and Exfiltration
- Getting Data from a Target
- Hide Files with OpenStego
- Alternate Data Streams
- Applied Live Lab: Staging and Exfiltration Using ADS
- Lesson Review

9.4 Cleanup and Restoration

- Cleanup and Restoration Procedures
- Activity: Implement Cleanup and Restoration Activities
- Documenting Penetration Testing Tasks
- Lesson Review

9.5 Module Quiz

10.0 Reporting and Recommendations

10.1 Penetration Test Report Components

- Creating the Penetration Test Report
- Reporting Considerations
- Report Components and Definitions
- Documentation Specifications and Format Alignment
- Risk Scoring
- Test Limitations and Assumptions
- Lesson Review

10.2 Analyze Findings and Remediation Recommendations

- Analyzing Findings and Developing Recommendations Overview
- Technical Controls
- Administrative Controls
- Operational Controls
- Physical Controls
- Activity: Administrative and Operational Controls
- Lesson Review

10.3 Module Quiz

Register for this class by visiting us at:
www.tcworkshop.com or by calling us at 800-639-3535

NASBA CPE details are provided on the following pages.

CompTIA: PenTest+ On-Demand

Course ID #: 7000-1151-ZZ-Z
Hours: 35
Delivery Method: Group Internet Based

NASBA Information

Level: Intermediate/ Advanced
Advanced Preparation:
Attendance Requirement: To be awarded the full credit hours, you must sign in and attend the entire course.
Recommended Field(s) of Study: Computer Software & Applications
Recommended CPEs: 39.00

Policies: Course Registration, Cancellation, Refund, and Complaint Resolution
For more information regarding administrative policies such as complaint and program cancellation policies, please contact our offices at 800-639-3535 or visit us at: **www.tcworkshop.com**

Official National Registry Statement:
The Computer Workshop is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors. State boards of accountancy have final authority on the acceptance of individual courses for CPE credits. Complaints regarding registered sponsors may be submitted to the National Registry of CPE Sponsors through its website: www.nasbaregistry.org

NOTE: Since our information is in multiple places on our website or in PDF format that is sent to clients, we have provided our normal course content with the NASBA Information added along with links to our policy page on the web. We will add our name to the Official National Registry Statement after we are approved.