

Training: CompTIA CompTIA PenTest+ Prep Course



TRAINING GOALS:

CompTIA PenTest+ validates your ability to identify, mitigate, and report system vulnerabilities. Covering all stages of penetration testing across attack surfaces like cloud, web apps, APIs, and IoT, it emphasizes hands-on skills such as vulnerability management and lateral movement. This certification equips you with the expertise to advance your career as a penetration tester or security consultant.

Skills you'll learn

- Plan and scope penetration tests while ensuring compliance with legal and ethical requirements, and develop detailed reports with remediation recommendations to support engagement management.
- Perform active and passive reconnaissance, gather information, and enumerate systems to uncover vulnerabilities effectively.
- Conduct vulnerability scans, analyze results, and validate findings to identify and address security weaknesses.
- Execute network, host-based, web application, and cloud-based attacks using appropriate tools and techniques to test system defenses.
- Maintain persistence, perform lateral movement, and document findings to support remediation efforts during post-exploitation activities.

Job roles that benefit from PenTest+ skills

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

Each participant in an authorized training CompTIA PenTest+ Prep Course held in Compendium CE will receive a free PT0-003 CompTIA PenTest+ Certification Exam vouchers.

CONSPECT:

- Penetration Testing - Before You Begin
 - Professional Conduct and Penetration Testing
 - What Is Penetration Testing?
 - Ethics, Legal, and Compliance Considerations of Penetration Testing
 - Importance and Examples of Documentation
 - Scoping and Authorization
 - Overview of the PenTest Report
 - Live Lab: Exploring the Lab Environment
 - 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
 - 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
- 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
- Applying Pre-Engagement Activities
 - Define the Scope
 - Regulations, Frameworks, and Standards
 - Rules of Engagement
 - Agreement Types
 - Target Selection
 - 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
 - Utilize the Shared Responsibility Model
 - The Shared Responsibility Model Overview
 - Hosting Provider Responsibilities
 - Customer Responsibilities
 - Penetration Tester Responsibilities
 - Third-Party Responsibilities
 - Identify Legal and Ethical Considerations
 - Authorization Letters
 - Mandatory Reporting Requirements
 - Risk to the Penetration Tester
 - Documenting Pre-Engagement Activities

- Enumeration and Reconnaissance
 - 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
 - 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
 - Enumeration for Attack Planning
 - Attack Path Mapping
 - Manual Enumeration
 - Simple Network Management Protocol
 - Documenting Enumeration Activities
 - Activity: Document Enumeration Activities
 - 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
- Scanning and Identifying Vulnerabilities
 - Vulnerability Discovery Techniques
 - Tools for Vulnerability Discovery
 - Types of Scans
 - Container Scans
 - Application Scans
 - Scan for Cleartext 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
 - Analyzing Reconnaissance Scanning and Enumeration
 - Public Exploit Selection
 - Use Scripting to Validate Results
 - 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
- Conducting Pentest Attacks
 - 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
 - Scripting Automation
 - Types of Scripting Automation
 - PowerShell
 - Bash
 - Python
 - Breach and Attack Simulation (BAS)
 - Live Lab: Executing Scripts to Automate Tasks
- Web-based Attacks
 - 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
- 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
- Enterprise Attacks
 - 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
- 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
- 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
- Specialized Attacks
 - 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
 - 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
- 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
- Performing Penetration Testing Tasks
 - 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
 - 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)
- 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
- Cleanup and Restoration
 - Cleanup and Restoration Procedures
 - Activity: Implement Cleanup and Restoration Activities
 - Documenting Penetration Testing Tasks
- Reporting and Recommendations
 - 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
 - Analyze Findings and Remediation Recommendations
 - Analyzing Findings and Developing Recommendations Overview
 - Technical Controls
 - Administrative Controls
 - Operational Controls
 - Physical Controls
 - Activity: Administrative and Operational Controls

REQUIREMENTS:

Recommended experience: 3-4 years in a penetration tester job role, with Network+ and Security+ or

equivalent knowledge

Difficulty level



CERTIFICATE:

The participants will obtain certificates signed by CompTIA (course completion). This course will help prepare you for the CompTIA PenTest+ certification exam, which is available through the Pearson VUE test centers.

Each participant in an authorized training CompTIA PenTest+ Prep Course held in Compendium CE will receive a free PT0-003 CompTIA PenTest+ Certification Exam vouchers.

TRAINER:

Authorized CompTIA Trainer.