CompTIA PenTest+ (Exam PT0-003), Videos & Skill Labs Set

Course Specifications

Course Number: ACI77-007VL_rev1.0
Video and Lab Length: Approximately 16 hours, 36 minutes

Course Introduction

CompTIA PenTest+ certified professionals are skilled cybersecurity specialists who assess and strengthen the security posture of organizations. They perform hands-on penetration testing and vulnerability assessments across a variety of environments, including traditional networks, cloud, hybrid systems, and web applications. As cyber threats grow more complex, PenTest+ stands out as the industry's most comprehensive intermediate-level certification for offensive security professionals. This course is designed to prepare you for the CompTIA PenTest+ (PT0-003) certification exam. Aligned with the latest exam objectives, it delivers a practical and scenario-based learning experience to help you demonstrate the skills employers demand.

Video Enhanced Learning

(5h 36m * 6 Modules * 51 Episodes)

We've enhanced select lab sets with targeted video content to strengthen student readiness and improve lab success. With focused video learning, students get reinforcement of core concepts before they enter the lab, giving them the confidence and context needed to apply skills effectively. Support diverse learning styles, improve lab readiness, and drive stronger outcomes across today's most in-demand skills.

Video Topics

1. Course Overview
2. Examining Security Control Categories
3. Examining Security Control Types
4. Examining the Principles of Security
5. Examining Authentication Factors
6. Examining Authorization and Access Control Models
7. Examining Authentication, Authorization, and Accounting (AAA)
8. Examining the Principles of Zero Trust
9. Examining Physical Security

10. Overview
11. Regulation and Compliance
12. Professionalism and Ethical Conduct
13. Common Pentest Restrictions
14. Scoping an Engagement
15. Legal Concepts and Documents
16. Professionalism and Integrity
17. Standards and Methodologies
18. Communication During a Pentest
19. Components of Written Reports
20. Recommended Remediations
21. Post Report Delivery Activities
22. Network Segmentation Testing
23. Target Recon
24. DNS Recon
25. Web and Cloud Discovery and Enumeration
26. Nmap
27. Business Logic Flaws
28. Vulnerability Scanning
29. Physical Attacks
30. Data Storage System Vulnerabilities
31. Host Discovery and Enumeration
32. Exploit Resources
33. IoT and Data Storage System Vulnerabilities
34. Network Poisoning Attacks
35. VLAN Hopping
36. Denial of Service
37. Password Attacks
38. MAC Spoofing
39. Wireless Attacks
40. Social Engineering Attacks
41. OWASP Top 10 Web App Security Risks
42. Session Management Attacks
43. SQL Injection Attacks

44. XSS Attacks
45. Other Injection Attacks
46. SSRF Attacks
47. Web Application Firewalls (WAFs) Detection and Bypass
48. Cloud Attacks
49. Virtual Environment Vulnerabilities
50. Container Vulnerabilities
51. ICS SCADA and IIoT Vulnerabilities
52. Programming Fundamentals for Penetration Testing
53. Analyze Scripts Or Code For Use In A Pentest
54. Automation in Penetration Testing
55. API Attacks
56. Mobile Attacks
57. Post Exploitation Enumeration and Tools
58. Privilege Escalation
59. Persistence Techniques
60. Detection Avoidance

Skill Labs

(11h * 11 Labs)

A **skills lab** is a guided, hands-on learning environment that allows students to practice real-world tasks in a safe, virtual setting. Instead of simply reading or watching videos, learners actively do the work—navigating realistic scenarios, applying concepts, troubleshooting issues, and building confidence through practical experience. This ensures that theory becomes usable skill. Skill labs are essential for developing true workplace readiness because they mirror real systems, tools, and challenges, helping learners bridge the gap between knowledge and performance. By completing a skills lab, students gain the hands-on competence employers expect and are better prepared for both assessments and real job responsibilities.

Skill Labs Topics

1. Penetration Testing Information Gathering Techniques (PT0-003)
2. Enumeration Tools and Techniques (PT0-003)
3. Vulnerability Scanning Techniques (PT0-003)
4. Conducting Network Attacks (PT0-003)
5. Conducting Authentication Attacks (PT0-003)

6. Conducting Host-Based Attacks (PT0-003)
7. Conducting Web Application Attacks (PT0-003)
8. Performing a Social Engineering Attack (PT0-003)
9. Automating Attacks Using Scripts (PT0-003)
10. Compromising a System and Maintaining Persistence (PT0-003)
11. Penetration Testing Management Engagement (PT0-003)