



# TECH VISIONS

— CONSULTING & TRAINING —



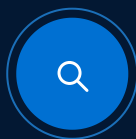
BUILDING CAPABILITY. STRENGTHENING SECURITY.

COURSE OUTLINE | EXAM PT0-003

## CompTIA PenTest+



Engagement  
Management



Reconnaissance  
& Enumeration



Vulnerability Discovery  
& Analysis



Attacks  
& Exploits



Post-exploitation &  
Lateral Movement

# CompTIA PenTest+ Certification

Exam PT0-003 | Plan, attack and report.



## COURSE OVERVIEW

CompTIA PenTest+ is an intermediate certification that validates the hands-on skills needed to plan, scope and execute penetration tests, then report findings to stakeholders. You will be assessed on your abilities in engagement management, reconnaissance and enumeration, vulnerability discovery and analysis, attacks and exploits, and post-exploitation and lateral movement. This certification prepares you for jobs such as penetration tester and security consultant.

## BENEFITS OF THE COURSE



### Engagement management

Plan and scope tests, follow legal and ethical requirements, and deliver reports that drive remediation.



### Recon & enumeration

Gather intelligence with OSINT, scanning and enumeration, and script the process to work faster.



### Vulnerability analysis

Discover, validate and prioritize vulnerabilities using scanners and standards such as CVSS.



### Attacks & exploits

Practice network, web, host, wireless, cloud and social engineering attacks in authorized lab environments.



### Post-exploitation

Understand persistence, lateral movement, exfiltration and cleanup the way real engagements demand.



### Recognized credential

Earn a vendor-neutral certification that maps to penetration tester and security consultant roles.

## TARGET AUDIENCE



**Penetration Testers**



**Security Consultants**



**Vulnerability Analysts**



**Security Analysts**



**Red Team Members**



**Security Engineers**



**Aspiring Ethical Hackers**



**IT Pros Moving into Offensive Security**

# Five domains, 26 modules

Built on the official PT0-003 exam objectives.



01

## Engagement Management

13% of exam

Where every penetration test starts and ends: scoping and rules of engagement, legal and ethical requirements, frameworks and methodologies, and reporting that drives remediation.

### MODULES

- 01 Pre-engagement activities & agreements
- 02 Collaboration & communication
- 03 Testing frameworks & methodologies
- 04 Penetration test report components
- 05 Findings analysis & remediation

**You will be able to:** scope and plan an engagement, follow legal and ethical rules, and report findings with clear remediation advice.



02

## Reconnaissance & Enumeration

21% of exam

Learning everything about the target: passive and active information gathering, enumeration of hosts and services, and the scripts and tools that speed the work up.

### MODULES

- 06 Information gathering techniques & OSINT
- 07 Enumeration techniques
- 08 Scripting for reconnaissance & enumeration
- 09 Reconnaissance & enumeration tools

**You will be able to:** gather and enumerate target information using the right techniques, tools and scripts.



03

## Vulnerability Discovery & Analysis

17% of exam

Finding and validating weaknesses: scanning techniques and tools, analyzing results, physical security concepts and prioritizing what to attack first.

### MODULES

- 10 Vulnerability discovery techniques & tools
- 11 Analyzing scan & enumeration output
- 12 Physical security concepts
- 13 Prioritizing vulnerabilities & preparing attacks

**You will be able to:** discover vulnerabilities, validate true and false positives, and prioritize targets for attack.

# Attack, then pivot

Course outline continued: domains 04 and 05.



04

## Attacks & Exploits

35% of exam

The heaviest domain: carrying out attacks across networks, hosts, applications, wireless, cloud, people and specialized systems, and automating them with scripts.

### MODULES

- 14 Network attacks
- 15 Authentication attacks
- 16 Host-based attacks
- 17 Web application attacks
- 18 Cloud-based attacks
- 19 Wireless attacks
- 20 Social engineering attacks
- 21 Specialized systems: mobile, AI & OT
- 22 Scripting to automate attacks

**You will be able to:** select and perform the right attacks against authorized targets and automate them with scripts.



05

## Post-exploitation & Lateral Movement

14% of exam

What happens after initial access: maintaining a foothold, moving through the environment, staging and exfiltrating data, and cleaning up when the test ends.

### MODULES

- 23 Persistence
- 24 Lateral movement & pivoting
- 25 Staging & exfiltration
- 26 Cleanup & restoration

**You will be able to:** explain post-exploitation activities and restore the environment after an engagement.

### HANDS-ON LAB FOCUS



#### Recon & enumeration

Map targets with Nmap, OSINT tools and enumeration scripts in lab environments.



#### Vulnerability scanning

Run and interpret scans, then validate true and false positives.



#### Exploitation labs

Practice attacks on intentionally vulnerable targets in an authorized, isolated lab.



#### PBQ-style scenarios

Solve hands-on pentest scenarios, including terminal tasks, as on the real exam.

# The PenTest+ exam

Everything you need to know before exam day.

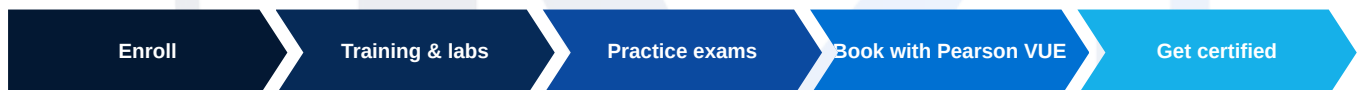


| ITEM                | DETAILS                                    |
|---------------------|--------------------------------------------|
| Certification       | CompTIA PenTest+                           |
| Exam code           | PT0-003                                    |
| Number of questions | Maximum of 90                              |
| Question types      | Multiple choice and performance-based      |
| Duration            | 165 minutes (2 hours 45 minutes)           |
| Passing score       | 750 (on a scale of 100–900)                |
| Exam delivery       | Pearson VUE: test center or online (OnVUE) |

## DOMAIN WEIGHTING



## YOUR PATH TO CERTIFICATION



Ready to build a rock-solid skills in penetration testing?

EMAIL [training@thetechvisions.com](mailto:training@thetechvisions.com)  
WEB [thetechvisions.com](https://thetechvisions.com)