

PT0-003: CompTIA PenTest+

Plan, perform and report professional penetration tests — and prepare for the CompTIA PenTest+ PT0-003 exam in a hands-on lab.

DURATION

5 days · 40 hours

LEVEL

Intermediate

CURRICULUM

14 modules · 8 labs

DELIVERYLive online, Onsite,
Corporate

Course overview

Penetration testers are hired to find weaknesses before attackers do, and to explain them clearly enough that they get fixed. That requires more than running tools: a good tester plans within legal and contractual limits, works methodically, chooses techniques carefully and writes reports that business and technical readers can act on. This five-day course covers that complete life cycle.

Day one covers engagement management: scoping, rules of engagement, legal and ethical considerations, testing frameworks and collaboration with the client. Day two focuses on reconnaissance and enumeration, using open-source intelligence, active scanning and service enumeration to map an attack surface. Day three addresses vulnerability discovery and analysis across networks, applications and cloud environments, including validating findings and avoiding false positives.

Day four is about attacks and exploits: network attacks, authentication and credential attacks, web application attacks, cloud and container attacks, wireless and social engineering techniques. Day five covers post-exploitation and lateral movement — persistence, privilege escalation, pivoting and clean-up — then finishes with writing a professional report and an exam-readiness session.

All practical work takes place in an isolated lab built for the course. You will only practise against systems you are authorised to test, and ethics are discussed throughout. This course is aligned to the PT0-003 exam and prepares you for it; confirm the current version on the CompTIA website before booking.

Highlights

- 40 hours of live, lab-intensive training
- Full test life cycle from scoping to reporting
- Network, web, cloud and wireless attack labs
- Mapped to the PT0-003 exam domains
- Report writing practice for real engagements

What's included

- Isolated lab range for safe, legal practice
- Complete engagement from scoping to report
- Network, web, cloud and wireless attack exercises
- Privilege escalation and lateral movement labs
- Professional report writing workshop
- Performance-based question practice
- Course completion certificate from Ace Skills Consulting

Who this course is for

Who should attend

- Aspiring penetration testers
- Security analysts moving into offensive security
- Vulnerability assessment professionals
- Network and system administrators interested in attack techniques

Prerequisites

- Security+ or Network+ level knowledge
- Comfortable with Linux and Windows command lines
- Basic scripting knowledge (Bash or Python) helps

Detailed curriculum — 5 days, 40 hours, 14 modules, 8 hands-on labs

Day 1 Engagement Management

8 hours

1.1 Planning and scoping

- Scope, objectives and constraints
- Legal and contractual documents
- Rules of engagement
- Testing frameworks and methodologies

1.2 Professional conduct

- Ethics and responsible disclosure
- Handling sensitive data during a test
- Collaboration and communication

1.3 Lab orientation

- Kali Linux tooling overview
- Note-taking and evidence management
- Lab network and targets

LAB Prepare a scoping document and rules of engagement for a sample client · 45 min

Day 2 Reconnaissance & Enumeration

8 hours

2.1 Passive reconnaissance

- Open-source intelligence
- Public code and data leaks
- DNS and certificate transparency

LAB Gather OSINT on a fictional organisation · 40 min

2.2 Active scanning and enumeration

- Host discovery and port scanning
- SMB, LDAP and SNMP enumeration
- Service and version detection
- Scripting reconnaissance

LAB Map the lab network with Nmap and enumerate services · 60 min

Day 3 Vulnerability Discovery & Analysis

8 hours

3.1 Discovery techniques

- Vulnerability scanners
- Cloud and container misconfiguration checks
- Web application scanning

LAB Scan the lab range and validate findings · 50 min

3.2 Analysing results

- Separating true and false positives
- Choosing exploitation paths
- Prioritising targets

3.3 Physical and social vectors

- Physical security assessment
- Phishing campaign design
- Social engineering techniques

Day 4 Attacks & Exploits

8 hours

4.1 Network and authentication attacks

- Exploiting vulnerable services
- Man-in-the-middle techniques
- Credential attacks and password cracking
- Active Directory attacks

LAB Exploit a vulnerable service and crack captured hashes · 60 min

4.2 Application attacks

- Injection attacks
- Server-side request forgery
- Authentication and session flaws
- API testing

LAB Exploit common web vulnerabilities with Burp Suite · 60 min

4.3 Cloud, wireless and specialised systems

- Cloud identity and storage attacks
- IoT and mobile considerations
- Wireless attacks

Day 5 Post-Exploitation, Reporting & Exam Readiness

8 hours

5.1 Post-exploitation and lateral movement

- Privilege escalation on Windows and Linux
- Pivoting and lateral movement
- Persistence techniques
- Clean-up and restoring systems

LAB Escalate privileges and pivot to a second network · 60 min

5.2 Reporting

- Report structure and executive summary
- Debriefing the client
- Writing findings and remediation advice

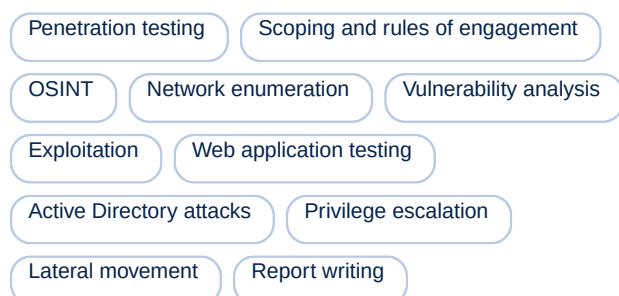
LAB Write the final report for the lab engagement · 40 min

5.3 Exam readiness

- Performance-based question strategy
- Practice test and review

Skills and tools

Skills you will build



Tools used in class



Certification exam

This course is aligned to the exam below and prepares you for it. The exam itself is booked and taken with the vendor.

Exam **CompTIA PenTest+**

Exam code	PT0-003
Questions	Maximum 90
Duration	165 minutes
Passing score	750 (on a scale of 100–900)
Format	Multiple choice, Multiple response, Performance-based / lab
Delivery	Online proctored, Test centre
Validity	3 years (renewable through CompTIA continuing education)
Official page	https://www.comptia.org/certifications/pentest

Exam skill areas covered

Penetration Testing / Social Engineering

Exam details are pending verification. Confirm the current exam code, format and fee on the official vendor page before booking.

Frequently asked questions

Is it legal to practise these techniques?

Only on systems you are authorised to test. All course practice happens in an isolated lab, and we cover the legal boundaries in detail.

How does PenTest+ compare with CEH?

Both cover offensive security. PenTest+ places more weight on the full engagement, including scoping and reporting, and uses performance-based questions.

Do I need programming skills?

Basic scripting helps, but it is not required. The course explains the scripts used in labs.

Can I practise after the course?

Yes. We share guidance on legal practice platforms and lab setups you can build at home.

Is PT0-003 the current version?

The course is mapped to PT0-003. Confirm the current exam version on the CompTIA website before booking.

Book a batch or talk to an advisor

Course page: aceskillsconsulting.com/course/pt0-003-comptia-pentest-plus · Email: info@aceskillsconsulting.com

Chennai office

Guindy, Chennai, Tamil Nadu

Delhi office

B-95, Old Post Office Street, Shakarpur
New Delhi 110092
Office: 98180 12523

CompTIA, A+, Network+, Security+, CySA+, PenTest+, SecurityX, Cloud+ and Linux+ are trademarks of CompTIA, Inc. All product names, logos, brands, trademarks and registered trademarks are the property of their respective owners. Ace Skills Consulting is an independent training provider; unless explicitly stated, it is not affiliated with, endorsed by or sponsored by any vendor mentioned on this site. Exam details are provided for guidance and may change — always confirm on the vendor's official website. Curriculum generated on 23 Oct 2026; topics and order may be adjusted by the trainer to suit each batch.