

COMPTIA

PenTest+ PT0-003 — CompTIA

PenTest+

Preparation Training

Delivered from Hacky Security's own curriculum, by instructors who also work our security operations centre. Classroom, online live, or at your office.

INTERMEDIATE

40 HOURS

5 DAYS

At a glance

COURSE	PenTest+ PT0-003 — CompTIA PenTest+
TRACK	CompTIA
DOMAIN	Cyber Security
LEVEL	Intermediate
DURATION	40 hours (about 5 days)
DELIVERY	Classroom · Online live · On-site at your office
LANGUAGE	English
CLASS SIZE	Small cohorts — everyone gets lab time

WHAT IS INCLUDED

- ✓ Instructor-led delivery by practitioners who also work our SOC
- ✓ Hands-on lab access for the duration of the course
- ✓ Course materials and lab guides
- ✓ Hacky Security certificate of completion
- ✓ Post-course support by email

Who this is for

This is an intermediate course. It suits people already working in or moving into Cyber Security who want structured, hands-on preparation rather than a video library. If you are unsure whether the level fits your team, send us the job titles and we will tell you honestly — including if a different course would serve you better.

Course outline

About this course map

Five domains, mapped one-for-one to the CompTIA PenTest+ PTO-003 exam objectives and taught in the same order, so nothing on the exam is left uncovered.

PTO-003 is the current version of PenTest+. What separates it from its predecessor is structural: engagement management is now its own domain rather than scaffolding around the technical work, reconnaissance and vulnerability analysis have been pulled apart into separate domains, and post-exploitation and lateral movement stand alone at the end. The attack surface has moved with it — cloud and container exploitation and attacks against AI systems now sit inside the objectives rather than outside them.

Each domain below carries its published weighting, and we give it classroom time in proportion. Better than half the course is hands-on, run against a target estate we have built to be broken, so you are finding genuine weaknesses rather than walking a script to a known answer.

Domain 01 — Engagement Management

The part that separates a penetration test from an unauthorised intrusion. 13% of the exam.

- Pre-engagement activities: scoping, target selection, testing windows and the rules of engagement
- Getting written authorisation, and why a signed scope protects you more than it protects the client
- Legal and regulatory constraints on testing, including third-party and hosted assets you do not own
- Mandatory reporting obligations, and what to do when you find evidence of an existing compromise
- Professional and ethical conduct, confidentiality, and handling client data during and after the test
- Stakeholder alignment: agreed points of contact, escalation paths and communication triggers
- Peer review, quality assurance and goal reprioritisation mid-engagement
- Articulating risk in business terms rather than technical severity alone
- Report structure: executive summary, methodology, findings, evidence and remediation guidance
- Common report deficiencies, secure report handling and delivery, and post-report activities including retesting and client acceptance

Domain 02 — Reconnaissance and Enumeration

Building a complete picture of the target before you touch anything that matters. 21% of the exam.

- Passive reconnaissance and open-source intelligence: domains, certificates, public records, code repositories and social sources
- Active reconnaissance, and controlling how much noise you make while doing it
- Network sniffing, protocol scanning, host discovery and service identification
- DNS enumeration, subdomain discovery and zone information gathering
- Service, share, user and directory enumeration across common protocols
- Web and application enumeration: technology fingerprinting, content discovery and API surface mapping
- Cloud and external asset enumeration, including storage, identity endpoints and exposed management interfaces
- Wireless and physical reconnaissance where the engagement includes them
- Reconnaissance tooling in practice, including Nmap, packet analysers and internet-wide scan services
- Reading, modifying and writing scripts in Python, PowerShell and Bash to automate collection and normalise the output

Domain 03 — Vulnerability Discovery and Analysis

Turning an attack surface into a prioritised list of things that will actually work. 17% of the exam.

- Scanning approaches: authenticated and unauthenticated, credentialed and uncredentialed, agent-based and agentless
- Static and dynamic application security testing, and where each finds things the other misses
- Scanning considerations for fragile targets, including operational technology and legacy systems
- Vulnerability scanning tools and their output, including general-purpose scanners and web application scanners
- Validating findings and separating exploitable weaknesses from scanner noise
- Identifying false positives and false negatives, and troubleshooting scanner configuration
- Manual analysis: source review, configuration review and reasoning about a flaw the tooling did not name
- Vulnerability research, exploit selection and assessing the risk of running it in a live environment
- Prioritising targets by likely impact and likelihood of success within the agreed scope

Domain 04 — Attacks and Exploits

The largest domain, and the one where everything before it is put to use. 35% of the exam.

- Network attacks: on-path positioning, relay and coercion techniques, VLAN hopping and service exploitation
- Authentication attacks: password spraying, brute force, credential stuffing, pass-the-hash and Kerberos abuse
- Host-based attacks: privilege escalation on Windows and Linux, credential dumping, process injection and abusing scheduled execution
- Web application attacks: injection flaws, cross-site scripting, directory traversal, insecure deserialisation, file upload abuse and server-side request forgery
- API and web service attacks, including broken authorisation and business logic flaws
- Cloud attacks: identity and access misconfiguration, metadata service abuse, over-permissive roles and exposed storage
- Container and orchestration attacks, including escape techniques and insecure registries
- Wireless and mobile attacks where in scope
- Social engineering and physical attacks run under agreed authorisation
- Supply chain and dependency attacks
- Attacks against artificial intelligence systems, including prompt injection and model manipulation
- Exploit selection, modification and delivery, and the tooling used to stage and control it

Domain 05 — Post-exploitation and Lateral Movement

What you do once you are in, and how you leave the estate as you found it. 14% of the exam.

- Establishing a foothold: persistence mechanisms and command-and-control channels
- Enumerating from the inside, where the picture is far richer than it was externally
- Credential harvesting and reuse to reach the next system
- Lateral movement techniques across Windows and Linux estates
- Pivoting, tunnelling and port forwarding into segmented networks
- Privilege escalation towards domain or tenant-level control
- Data exfiltration techniques, demonstrated safely and proportionately
- Detection avoidance, and understanding what a defender would have seen at each step
- Cleanup: removing tooling, accounts, persistence and artefacts, and documenting everything you changed

- Building the attack narrative — the chain of steps that turns individual findings into a demonstrated business risk
- Remediation recommendations that address the chain, not just the last link

Who should take this

Penetration testers, red team operators, security consultants, vulnerability analysts, and application or cloud security engineers who need to test their own systems credibly. It also suits experienced defenders who want to understand offensive work well enough to judge a report rather than take it on trust.

CompTIA recommends Network+ and Security+ or equivalent knowledge, along with three to four years of hands-on experience in a penetration testing role. These are recommendations, not requirements — nothing prevents you from sitting the exam without them, and we regularly teach strong candidates earlier in their careers.

You will need working knowledge of networking, Windows and Linux, and to be genuinely comfortable at a command line. Some scripting ability is a real advantage, because the scripting objectives are examined rather than assumed.

The exam

PenTest+ is set and awarded by CompTIA.

- A maximum of 90 questions, 165 minutes
- A mix of multiple-choice and performance-based questions
- A scaled score of 750 on a scale of 100 to 900 is required to pass
- Available in English, French, Japanese and Portuguese

CompTIA does not publish how much of the paper is performance-based, so plan to meet those questions anywhere in it. The exam voucher is purchased separately from CompTIA; we arrange it on your behalf and send you the code, and you book your own exam date.

How we deliver it

Five days, classroom or online live, or at your office for a private group. The majority of the time is hands-on in our lab estate, and the course ends with a scoped engagement run end to end — reconnaissance through to a written report that is marked as a report, not as a list of findings. Domain checkpoints each day, and a full-length mock under exam conditions on the final afternoon.

Mapped to the CompTIA PenTest+ PT0-003 exam objectives. Taught from Hacky Security's own curriculum and lab estate by instructors who test client estates for a living.

Sitting the official exam

Exam voucher sold separately. We buy it from the certification body on your behalf and send you the code — you book your own exam date. This course is Hacky Security's own preparation training. The certification itself is awarded by the certification body, not by us.

Investment

Priced per cohort. Tell us how many people and which delivery mode and we will send a quote the same working day.

Book this course

Tell us how many people, where, and when — we will come back with dates and a quote within one working day.

+91-8091900310 • info@hackysecurity.com

<https://hackysecurity.com/courses/pentest-plus/>

CHANDIGARH • SHIMLA • DELHI • DUBAI • LONDON

Independent preparation training delivered from Hacky Security's own curriculum. Hacky Security Private Limited is not affiliated with or endorsed by the certification body named in this document. Certification names and codes are the trademarks of their respective owners and are used only to describe what this course prepares you for. Prices, durations and outlines are indicative and may change; the quotation we send you is the binding one. Issued 11 September 2026.