CompTIA PenTest+

OUR LEARNING EXCLUSIVE

- Custom exam prep software and materials
- Exam delivery in the classroom, with a **98% success rate**
- Course-specific thinQtank® Learning publications to keep the learning engaging
- Extended hours of training, including immersive hands-on exercises
- **We do not teach the test.** We always deliver valuable hands-on experience
- All reading material and study guides sent to you when you register
- Every course taught by working penetration testers

TRAINING CAMP FORMAT

thinQtank® Learning delivers this course as an **instructor-led training camp**, with the exam sat in the classroom as part of the camp. Camps are scheduled by cohort rather than to a fixed calendar, and the balance of lecture and lab work is set to suit the group and the delivery method. Contact us for the schedule covering your dates.

PREREQUISITES

- CompTIA Network+ and Security+, or equivalent knowledge
- Working familiarity with TCP/IP networking, and with administering both Linux and Windows
- Some exposure to a scripting language — Bash, Python or PowerShell
- CompTIA recommends three to four years in a penetration testing role — a recommendation, not a bar to entry

TARGET AUDIENCE

- Penetration testers, red team operators and vulnerability analysts
- Security analysts and engineers moving from defensive work into offensive testing
- Security consultants who need a recognized, hands-on credential
- Anyone whose role requires a DoD 8140 approved offensive-security certification

EXAM

PT0-003 — CompTIA PenTest+ (V3)

Maximum of 90 questions, multiple choice and performance-based. 165 minutes. Passing score 750 on a scale of 100 to 900.

CompTIA PenTest+ is accredited to **ISO 17024** and is approved by the US Department of Defense to meet **directive 8140 / 8570.01-M** requirements.

COURSE OVERVIEW

thinQtank® Learning offers an industry-unique training camp in which students earn the **CompTIA PenTest+** certification. As with all our CompTIA training experiences, the exam is delivered in the classroom.

PenTest+ is the credential for people whose job is to break in on purpose. It covers the whole engagement — scoping and the legal agreements that authorize the work, reconnaissance and enumeration, finding and validating vulnerabilities, exploitation across networks, hosts, web applications, cloud services and wireless, then persistence, lateral movement and clean restoration of the target.

It is one of very few offensive-security certifications that tests **both** the hands-on attack skills and the management of an engagement: the scope, the communication, the findings and the report that turns a test into work the client will actually do. It maps to exam **PT0-003**, with objective coverage marked throughout, and the **exam voucher is available** at $404 USD.

COURSE OBJECTIVES

Primary course objectives:

- Scope and plan an engagement: rules of engagement, legal agreements and the ethical limits of the work
- Apply the recognized testing frameworks — OSSTMM, PTES, CREST, MITRE ATT&CK and the OWASP testing guides
- Gather intelligence on a target using passive and active OSINT
- Enumerate hosts, services, DNS records and users, and fingerprint operating systems
- Run and tune vulnerability scans, then validate the output by hand
- Assess physical security controls, and the exposure of industrial control and embedded systems
- Execute network, authentication and host-based attacks
- Execute web application, cloud, wireless and social engineering attacks
- Establish persistence, escalate privilege, move laterally and exfiltrate data
- Write and modify scripts in Bash, Python and PowerShell to automate the repetitive work
- Clean up and restore a target environment when the engagement ends
- Analyze findings, rank them by business risk, and recommend remediation
- Write and defend the report for a technical and a non-technical audience

DELIVERY METHODS

- Instructor-led training
- Immersive live-online training
- On-site and custom delivery

WHAT YOU WILL BE ABLE TO DO

- Plan and scope an authorized engagement, and stay inside it
- Find, validate and exploit vulnerabilities across an estate rather than a single host
- Move laterally, hold access, and leave the environment exactly as you found it
- Rank findings by business risk and write the report a client will act on

EXCLUSIVE LEARNING PACKAGE

- Penetration testing kit
- Custom Linux build for penetration testing
- Kali Linux video course
- PenTest+ video course
- PenTest+ reading plan and review guide
- PenTest+ certification practice exam
- Scripting primer — Bash, Python and PowerShell for testers

COURSE MODULES

01 Engagement Management — 13%
- Topic A: Pre-engagement activities, scope and shared responsibility
- Topic B: Legal agreements, authorization and the ethical limits of the work
- Topic C: Collaboration and communication during an engagement
- Topic D: Testing frameworks: OSSTMM, PTES, CREST, MITRE ATT&CK, OWASP
- Topic E: Report structure, findings analysis and remediation recommendations

02 Reconnaissance and Enumeration — 21%
- Topic A: Passive information gathering and open-source intelligence
- Topic B: Active reconnaissance and its footprint
- Topic C: Host, service and DNS enumeration; operating system fingerprinting
- Topic D: Tooling: Maltego, Shodan, the Wayback Machine, nslookup and dig
- Topic E: Modifying scripts to gather and shape the data you need

03 Vulnerability Discovery and Analysis — 17%
- Topic A: Vulnerability scanning techniques and scan tuning
- Topic B: Analyzing output and validating results by hand
- Topic C: Industrial control and embedded system considerations
- Topic D: Physical security assessment: tailgating, badge cloning, locks

04 Attacks and Exploits — 35%
- Topic A: Network attacks
- Topic B: Authentication attacks
- Topic C: Host-based attacks and privilege escalation
- Topic D: Web application attacks
- Topic E: Cloud-based attacks
- Topic F: Wireless attacks
- Topic G: Social engineering and physical attacks
- Topic H: Attacks on specialized and legacy systems
- Topic I: Automating attacks with scripting

05 Post-Exploitation and Lateral Movement — 14%
- Topic A: Establishing and maintaining persistence
- Topic B: Lateral movement across the estate
- Topic C: Staging and exfiltrating data
- Topic D: Detection avoidance and covering the engagement's tracks
- Topic E: Cleanup and restoration of the target environment

A Appendices
- Appendix A: Taking the exam
- Appendix B: Mapping course content to the CompTIA® PenTest+® exam
- Appendix C: Linux essentials for testers
- Appendix D: Scripting essentials — Bash, Python, PowerShell
- Appendix E: Reporting templates and worked examples