CompTIA PenTest+ PT0-001 Exam Prep

CompTIA PenTest+ PT0-001 2026. Penetration testing, vulnerability analysis, and reporting.

IT Certifications Instructor: Brian Mitchell • 5 sections • 41 lessons • 12.50h total

View this course online Browse all courses

About this course

Preparing for the CompTIA PenTest+ PT0-001 exam can feel overwhelming given the breadth of topics, from planning and scoping to reporting and communication. This course cuts through the noise to give you a focused, hands-on path to certification, using practical examples that mirror what you will face on the job and in the exam.

We will walk you through each exam domain with step-by-step guides, problem-solving sessions, and downloadable study checklists. You will learn how to apply penetration testing methodologies, analyze vulnerabilities, and report findings, with real case studies.

Course curriculum

Foundations and Planning

- Understanding Penetration Testing Methodologies (18m)
  We'll break down the key frameworks like OSSTMM and NIST, showing you how to choose the right one for your engagement.
- Scoping Your Engagement Correctly (25m)
  Learn how to define rules of engagement, set clear objectives, and avoid scope creep with a downloadable scoping template.
- Legal and Compliance Considerations (12m)
  A practical look at contracts, permission to attack, and handling sensitive data to keep you and your client safe.
- Gathering Passive Intelligence (32m)
  We'll show you how to use OSINT tools and techniques to gather information without touching the target network.
- Active Reconnaissance: Port Scanning (15m)
  A step-by-step guide to using Nmap and other scanners to identify live hosts and open services.
- Vulnerability Scanning with Nessus and OpenVAS (22m)
  Learn to set up, run, and interpret results from common vulnerability scanners to find potential entry points.
- Building Your Pentesting Lab Environment (28m)
  A real case study on setting up a safe, isolated lab using VirtualBox and vulnerable VMs for practice.

Core Attack Concepts

- Password Attacks and Cracking Techniques (20m)
  We'll cover dictionary attacks, brute force, and rainbow tables using tools like John the Ripper and Hashcat.
- Exploiting Network Vulnerabilities (24m)
  A hands-on session on exploiting common misconfigurations like SMB and FTP to gain initial access.
- Web Application Attacks: SQL Injection (29m)
  Learn to identify and exploit SQLi vulnerabilities in a vulnerable web app, with a focus on manual testing.
- Cross-Site Scripting (XSS) and CSRF (19m)
  We'll demonstrate how these client-side attacks work and how to detect them during a web app test.
- Post-Exploitation: Privilege Escalation (26m)
  A problem-solving session on moving from a low-privilege shell to root/admin using kernel exploits and misconfigurations.
- Maintaining Access: Persistence Mechanisms (14m)
  Learn about backdoors, scheduled tasks, and registry keys to understand how attackers maintain a foothold.

- Wireless Network Attacks (21m)
  We'll cover cracking WEP/WPA2 and rogue access points using Aircrack-ng suite.
- Denial of Service (DoS) Concepts (11m)
  A theoretical and practical overview of common DoS attacks and how to identify them in logs.
- Cloud Security Testing Considerations (16m)
  A practical guide to the unique challenges of testing in AWS and Azure environments.

Tools and Deep Dive

- Metasploit Framework (30m)
  We'll explore payloads, listeners, and modules to streamline your exploitation phase.
- Using Burp Suite for Web Testing (27m)
  A deep dive into the proxy, repeater, and intruder to manipulate and test web requests.
- Python Scripting for Pentesters (32m)
  Learn to write simple scripts to automate repetitive tasks like port scanning or directory brute-forcing.
- PowerShell for Post-Exploitation (17m)
  We'll show you how to use PowerShell Empire and native commands for enumeration and data exfiltration.
- Analyzing Network Traffic with Wireshark (23m)
  A practical session on capturing packets and filtering for credentials or sensitive information.
- Using Social Engineering Toolkit (SET) (9m)
  Learn to craft convincing phishing campaigns and credential harvesting attacks for your test.
- Covering Your Tracks (13m)
  We'll discuss log manipulation and timestomping, and how to detect these actions as a defender.

Advanced Reporting and Communication

- Structuring Your Penetration Test Report (18m)
  A step-by-step guide to creating executive summaries and technical findings that stakeholders understand.
- Prioritizing Vulnerabilities with CVSS (12m)
  Learn to calculate and interpret CVSS scores to rank risks for your client.
- Writing Effective Remediation Guidance (22m)
  We'll show you how to write clear, actionable steps to fix issues without causing new ones.
- Presenting Findings to Technical Teams (15m)
  A problem-solving session on handling tough questions and demonstrating proof of concept.
- Communicating Risk to Management (11m)
  Learn to translate technical jargon into business impact, focusing on ROI and risk reduction.
- Debriefing and Lessons Learned (8m)
  A real case study on conducting a post-engagement meeting to improve future tests.
- Handling Sensitive Data and Evidence (10m)
  Best practices for encrypting and storing proof of compromise securely.
- Preparing for the PT0-001 Exam Day (14m)
  We'll share tips on managing time, understanding question types, and avoiding common pitfalls.

Implementation & Next Steps

- Setting Up a Vulnerability Management Program (25m)
  A practical guide to moving from one-off tests to a continuous security assessment process.
- Integrating Pentesting into DevOps (DevSecOps) (20m)
  Learn how to automate security checks in the CI/CD pipeline with downloadable configs.
- Threat Modeling Fundamentals (16m)
  We'll show you how to use STRIDE to identify threats before you even start scanning.
- Red Team vs. Blue Team Exercises (21m)
  A problem-solving session on setting up internal simulations to test your defenses.
- Staying Current with New Attack Vectors (12m)
  We'll cover resources like Twitter, Reddit, and CVE databases to keep your skills sharp.
- Building a Personal Pentesting Toolkit (23m)
  A real case study on curating a custom Kali Linux instance with your favorite tools.
- Career Paths After PenTest+ (10m)
  Explore roles like security analyst, red teamer, and consultant, and what certs to tackle next.
- Creating a Portfolio of Your Work (13m)
  Learn to document your lab work and CTF wins to show potential employers.
- Ethical Hacking: A Code of Conduct (9m)
  A final reminder on the importance of ethics, responsibility, and continuous learning.
- Final Q&A and Community Resources (15m)
  We'll wrap up with a summary of where to find help, study groups, and practice exams.
