CompTIA PenTest+ (PT0-002) Exam Prep: Practical Guide

CompTIA PenTest+ PT0-002. Nmap, Metasploit, vulnerability identification, and reporting.

IT Certifications Instructor: Brian Taylor • 5 sections • 44 lessons • 13.25h total

View this course online Browse all courses

About this course

Preparing for the CompTIA PenTest+ certification can feel overwhelming, with many domains to cover from planning and scoping to reporting and communication. This course breaks down the PT0-002 exam objectives into manageable lessons, focusing on the practical skills you need.

You will learn how to plan and scope engagements, use Nmap and Metasploit, identify vulnerabilities, and report your findings clearly. We will walk through real case studies, practice attacks, and share downloadable checklists.

Course curriculum

Foundations and Planning

- Understanding PT0-002 Exam Domains (12m)
  Break down the five exam domains and learn how to prioritize your study plan with a downloadable checklist.
- Scoping an Engagement Correctly (18m)
  Define rules of engagement, set boundaries, and avoid common scoping mistakes with real-world examples.
- Legal and Compliance Considerations (10m)
  Learn the key legal frameworks and consent requirements to keep your tests compliant.
- Gathering Passive Reconnaissance Data (22m)
  Use OSINT tools and techniques to collect target information without touching the network.
- Building Your Pen Testing Lab (15m)
  Step-by-step guide to setting up a safe lab with Kali Linux, Metasploitable, and VirtualBox.
- Choosing the Right Testing Strategy (14m)
  Compare black box, white box, and gray box approaches and when to use each.
- Creating a Statement of Work (20m)
  Write a clear SOW with deliverables, timelines, and assumptions using a downloadable template.

Core Scanning and Enumeration

- Nmap Scans (25m)
  Run stealthy, accurate scans with Nmap and interpret results like a pro.
- Enumeration Techniques for Windows (16m)
  Find shares, users, and services on Windows targets using built-in tools.
- Enumeration Techniques for Linux (19m)
  Explore Samba, NFS, and SSH enumeration methods on Linux systems.
- Vulnerability Scanning with Nessus (28m)
  Set up Nessus, run scans, and analyze reports to identify potential weaknesses.
- Mapping Attack Surfaces (12m)
  Learn how to identify exposed services and entry points in complex networks.
- Password Attacks and Cracking (24m)
  Use Hydra, John the Ripper, and hashcat to test password strength responsibly.
- Wireless Network Enumeration (17m)
  Scan for wireless networks and assess security with airodump-ng and aireplay-ng.
- Web Application Reconnaissance (21m)
  Map web app structures and identify hidden endpoints with Burp Suite and OWASP ZAP.

Exploitation and Post-Exploitation

- Metasploit Basics and Payloads (30m)
  Launch exploits, generate payloads, and understand Meterpreter sessions.

- Manual Exploitation Techniques (22m)
  Practice buffer overflows and privilege escalation without automated tools.
- Post-Exploitation: Lateral Movement (18m)
  Pivot through networks and access other systems from a compromised host.
- Web App Exploits: SQL Injection (26m)
  Manually test for SQLi using error-based and union-based methods.
- Cross-Site Scripting (XSS) Attacks (14m)
  Identify and exploit stored, reflected, and DOM-based XSS vulnerabilities.
- Local Privilege Escalation on Linux (20m)
  Exploit misconfigurations and kernel vulnerabilities to gain root access.
- Local Privilege Escalation on Windows (23m)
  Use token impersonation and service misconfigurations to escalate privileges.
- Maintaining Access: Persistence (15m)
  Set up backdoors and scheduled tasks to retain access ethically.

Advanced Techniques and Tools

- Scripting Attacks with Python (32m)
  Write custom scripts for brute-forcing and automating repetitive tasks.
- Using PowerShell for Red Teaming (19m)
  Leverage PowerShell for enumeration, exploitation, and evasion.
- Bypassing Antivirus and EDR (27m)
  Techniques for obfuscating payloads and avoiding detection.
- Cloud Penetration Testing Basics (24m)
  Assess AWS and Azure environments with tools like Pacu and ScoutSuite.
- Container Security Testing (16m)
  Identify Docker and Kubernetes misconfigurations and escape containers.
- Social Engineering Simulations (12m)
  Plan phishing campaigns and pretexting scenarios responsibly.
- Custom Exploit Development (35m)
  Build and test simple exploits for known CVEs in a lab setting.
- Using Custom Wordlists and Tools (11m)
  Generate targeted wordlists with CeWL and enhance your toolkit.
- Troubleshooting Failed Exploits (13m)
  Debug common issues and refine your approach with error analysis.

Reporting and Next Steps

- Organizing Findings Effectively (14m)
  Categorize vulnerabilities by risk and impact for clear reporting.
- Writing a Professional Pen Test Report (25m)
  Structure executive summaries, technical details, and remediation steps.
- Creating Remediation Recommendations (18m)
  Provide actionable fixes for common vulnerabilities with examples.

- Presenting Results to Stakeholders (20m)
  Communicate findings clearly to technical and non-technical teams.
- Handling Sensitive Data (9m)
  Best practices for encrypting and storing engagement data securely.
- Post-Engagement Cleanup (8m)
  Remove artifacts, revoke access, and document lessons learned.
- PT0-002 Practice Exam Strategy (16m)
  Simulate exam conditions and focus on weak areas with targeted practice.
- Career Paths in Pen Testing (12m)
  Explore red team, blue team, and consultant roles after certification.
- Staying Updated with CVEs (10m)
  Use resources like CVE Details and NVD to keep skills current.
- Building a Portfolio (11m)
  Document your lab work and write blog posts to showcase expertise.
- Final Review and Exam Day Tips (15m)
  Quick recap of key topics and mental prep for test day.
- Resources for Continued Learning (7m)
  Recommended books, forums, and labs to advance your skills post-cert.