PT0-003 Exam Preparation

CompTIA PT0-003 PenTest+. Broad exam scope broken into manageable steps with case studies.

IT Certifications Instructor: Brian Taylor • 5 sections • 52 lessons • 16.00h total

View this course online Browse all courses

About this course

This course tackles the common challenges of preparing for the PT0-003 exam, which can feel overwhelming with its broad scope. We break down the key domains into manageable parts so you can focus your study time.

You will get a step-by-step guide to each exam objective, with practical examples and problem-solving sessions. The course includes video lessons, real case study analysis, and downloadable study templates.

Course curriculum

Section 1: Foundations and Exam Overview

- Understanding the PT0-003 Exam Structure (12m)
  Learn the exam format, question types, and scoring so you know exactly what to expect on test day.
- Mapping Your Study Plan to the Exam Domains (18m)
  Get a step-by-step guide to creating a personalized study schedule that covers all key areas.
- Setting Up Your Pen Testing Lab Environment (25m)
  We'll show you how to set up a practical lab using virtual machines for hands-on practice.
- Key Tools You Need for the Exam (15m)
  A real case study analysis of essential tools like Nmap and Metasploit that you'll use during the test.
- Time Management for the 165-Minute Exam (10m)
  Learn practical strategies to pace yourself and avoid running out of time on the performance-based questions.
- Common Pitfalls and How to Avoid Them (14m)
  Problem-solving session on the biggest mistakes candidates make and how to sidestep them.
- Creating Your First Study Tracker (8m)
  Downloadable template to organize your progress and identify weak areas early.
- Setting Realistic Goals for Your Preparation (11m)
  How to set achievable milestones that keep you motivated without burnout.

Section 2: Planning and Scoping

- Defining Engagement Rules of Engagement (RoE) (22m)
  Learn how to draft a clear RoE document with real-world examples from client engagements.
- Identifying and Classifying Assets (19m)
  Step-by-step guide to mapping assets and prioritizing them based on risk.
- Setting Clear Scoping Boundaries (16m)
  Problem-solving session on avoiding scope creep and managing client expectations.
- Legal Considerations and Compliance (24m)
  Real case study analysis of legal frameworks like GDPR and how they impact pen testing.
- Creating a Detailed Project Plan (20m)
  Downloadable template for a pen testing project plan that covers timelines and resources.
- Risk Assessment Fundamentals (17m)
  Learn how to conduct a basic risk assessment using industry-standard methodologies.
- Communicating Scope to Stakeholders (13m)
  Practical tips for presenting your scope document to technical and non-technical stakeholders.
- Adjusting Scope Based on Findings (15m)
  How to handle unexpected discoveries and adjust the plan without derailing the project.
- Budgeting and Resource Allocation (18m)
  Step-by-step guide to estimating costs and allocating team members effectively.

- Pre-Engagement Checklist (9m)
  A downloadable checklist to ensure you're fully prepared before starting any test.

Section 3: Information Gathering and Vulnerability Identification

- Active vs. Passive Reconnaissance Techniques (21m)
  Real case study analysis comparing methods like OSINT and network scanning.
- Using Nmap for Effective Network Discovery (28m)
  Hands-on session with Nmap commands and scripts to identify live hosts and services.
- Web Application Reconnaissance (23m)
  Learn how to map web apps, identify technologies, and find hidden directories.
- Vulnerability Scanning with Nessus and OpenVAS (26m)
  Step-by-step guide to configuring scans and interpreting results for the exam.
- Identifying Common Vulnerabilities (OWASP Top 10) (19m)
  Problem-solving session on recognizing and prioritizing web app vulnerabilities.
- Social Engineering Reconnaissance (14m)
  Practical techniques for gathering info through LinkedIn, company websites, and more.
- Analyzing Network Traffic for Clues (17m)
  Using Wireshark to spot potential attack vectors in captured packets.
- Documenting Your Findings (12m)
  Downloadable template for a structured vulnerability report that exam graders will love.
- Prioritizing Vulnerabilities for Exploitation (16m)
  How to use CVSS scores and business impact to decide what to tackle first.

Section 4: Attacks and Exploitation

- Password Attacks: From Brute Force to Credential Stuffing (25m)
  Real case study analysis of tools like Hydra and John the Ripper in action.
- Exploiting Web Application Flaws (30m)
  Hands-on session with SQL injection and XSS attacks using DVWA or similar labs.
- Post-Exploitation Techniques on Windows (27m)
  Step-by-step guide to privilege escalation and maintaining access on Windows systems.
- Linux Privilege Escalation Methods (29m)
  Learn common techniques like kernel exploits and misconfigured services.
- Wireless Network Attacks (22m)
  Problem-solving session on cracking WPA2 and exploiting rogue access points.
- Social Engineering Attacks and Payloads (20m)
  How to craft phishing emails and deploy payloads using tools like GoPhish.
- Metasploit Framework Deep Dive (32m)
  Practical guide to using Metasploit for exploitation and pivoting.
- Bypassing Antivirus and Defenses (18m)
  Techniques for obfuscating payloads and avoiding detection.
- Exploiting IoT and Embedded Devices (15m)
  Real-world examples of attacking smart devices and industrial control systems.

- Maintaining Access and Covering Tracks (23m)
  Step-by-step guide to backdoors, rootkits, and log manipulation.
- Hands-On Exploitation Lab Walkthrough (35m)
  A complete, step-by-step exploitation scenario that ties together multiple techniques.

Section 5: Reporting and Next Steps

- Structuring a Professional Pen Test Report (24m)
  Downloadable template for an executive summary, technical details, and recommendations.
- Writing Clear and Actionable Recommendations (19m)
  Learn how to prioritize fixes and communicate them effectively to clients.
- Presenting Findings to Stakeholders (17m)
  Practical tips for delivering your report in a meeting without overwhelming the audience.
- Remediation Verification Techniques (16m)
  How to retest and confirm that vulnerabilities have been properly addressed.
- Handling Legal and Ethical Issues Post-Test (14m)
  Real case study analysis of ethical dilemmas and how to navigate them.
- Building Your Portfolio with Real Projects (21m)
  Step-by-step guide to creating case studies that showcase your skills to employers.
- Preparing for the Performance-Based Questions (26m)
  Problem-solving session with sample PBQs and strategies to tackle them under time pressure.
- Final Review and Mock Exam Strategy (22m)
  How to use practice tests and create a last-minute review plan.
- Exam Day Checklist and Mindset (10m)
  A downloadable checklist for the day of the test to stay calm and focused.
- What to Do After Passing the Exam (12m)
  Next steps for career advancement, continuing education, and maintaining your certification.
- Community Resources and Ongoing Support (9m)
  Where to find study groups, forums, and mentors to help you beyond the exam.
- Course Wrap-Up and Your Action Plan (11m)
  A final problem-solving session to create your personalized plan for exam success.
- Bonus: PT0-003 Exam Tips from Certified Professionals (15m)
  Real-world advice and common exam questions to watch out for.
- Downloadable Resources and Templates (8m)
  Access all the templates, checklists, and study guides mentioned throughout the course.
