COURSE SYLLABUS

# CompTIA PenTest+ Exam Preparation Course (Self-Paced)

Master the five PenTest+ (PT0-003) exam domains, from engagement scoping through exploitation and reporting.

> Group classes in Live Online and onsite training is available for this course. For more information, email onsite@graduateschool.edu or visit: https://www.graduateschool.edu/courses/pentest-plus-exam-preparation-course-self-paced


support@graduateschool.edu •
(888) 744-4723

## Course Outline

**Module 1: Engagement Management I: Scoping, Rules of Engagement, and Legal Concepts**

- Lessons:
  - Pre-Engagement Activities and Scoping
  - Rules of Engagement and Authorization
  - Legal Concepts and Compliance Requirements
  - Contracts, Master Service Agreements, and Third-Party Considerations
- Applied activity: Given a fictional client request, learners draft a scope statement and rules of engagement that specify testing windows, excluded systems, and escalation contacts.

**Module 2: Engagement Management II: Communication, Reporting, and Post-Engagement**

- Lessons:
  - Communication and Escalation Paths
  - Report Structure and Findings Documentation
  - Risk Ratings and Remediation Recommendations
  - Post-Engagement Cleanup and Deliverables
- Applied activity: Learners convert a set of raw findings into a one-page executive summary and a prioritized remediation table.

**Module 3: Passive Reconnaissance and OSINT**

- Lessons:
  - OSINT Fundamentals and Sources
  - DNS, WHOIS, and Certificate Transparency Research
  - Social Media and Public Records Reconnaissance
  - Passive Reconnaissance Tools and Documentation
- Applied activity: Learners build a target profile for a fictional organization using only publicly available sources, without touching the

target's systems.

### Module 4: Active Reconnaissance and Scanning

- Lessons:
  - Network Discovery and Host Scanning
  - Port and Service Scanning Techniques
  - Packet Crafting and Scan Evasion
  - Scan Output Analysis
- Applied activity: Learners interpret a sample scan output and identify likely services, versions, and next-step testing priorities.

### Module 5: Enumeration Across Protocols and Services

- Lessons:
  - Enumeration Fundamentals
  - Windows and Active Directory Enumeration
  - Web, Database, and Cloud Service Enumeration
  - Documenting Enumeration Findings
- Applied activity: Learners enumerate a simulated Active Directory environment description and identify likely privilege escalation paths from the output.

### Module 6: Vulnerability Scanning and Identification

- Lessons:
  - Vulnerability Scanner Fundamentals
  - Configuring and Running Authenticated Scans
  - Interpreting CVSS and Scan Output
  - Validating and De-duplicating Findings
- Applied activity: Learners review a sample scan report, flag likely false positives, and re-rank findings by validated severity.

### Module 7: Vulnerability Analysis and Attack Surface Prioritization

- Lessons:
  - Attack Surface Mapping
  - Prioritizing Vulnerabilities by Risk and Exploitability
  - Common Vulnerability Classes: Injection, Misconfiguration, Weak Authentication
  - From Analysis to Attack Planning
- Applied activity: Learners take a list of unranked vulnerabilities and produce a prioritized attack plan with justification for the chosen order.

### Module 8: Network and Host-Based Attacks

- Lessons:
  - Exploiting Network Services and Protocols
  - Password Attacks and Credential Access
  - Host-Based Exploitation Techniques
  - On-Path and Man-in-the-Middle Attacks
- Applied activity: Learners work through a scenario selecting the least noisy, most reliable exploitation technique for a described network service weakness.

### Module 9: Application-Based Attacks: Web and API

- Lessons:
  - Web Application Attack Fundamentals
  - Injection and Input Validation Attacks
  - Authentication and Session Attacks
  - API Security Testing
- Applied activity: Learners walk through a sample web request and identify where an injection or session weakness could be tested.

### Module 10: Wireless, Cloud, and IoT Attacks

- Lessons:
  - Wireless Network Attacks
  - Cloud Service and Configuration Attacks
  - IoT and Embedded Device Attacks
  - Attack Selection by Environment
- Applied activity: Learners are given three environment descriptions, wireless, cloud, and IoT, and select the most relevant testing technique for each.

### Module 11: Social Engineering and Physical Attacks

- Lessons:
  - Social Engineering Fundamentals and Pretexting
  - Phishing and Related Attack Delivery
  - Physical Security Testing
  - Ethical and Legal Boundaries in Social Engineering
- Applied activity: Learners draft a pretext and delivery plan for an authorized phishing exercise, including required approvals.

### Module 12: Post-Exploitation Techniques

- Lessons:
  - Post-Exploitation Fundamentals
  - Privilege Escalation Techniques
  - Data Exfiltration Simulation and Impact Assessment
  - Maintaining Access and Cleanup Considerations
- Applied activity: Learners describe a privilege escalation path from a low-privileged foothold to administrative access on a described host.

### Module 13: Lateral Movement, Pivoting, and Persistence

- Lessons:
  - Lateral Movement Fundamentals
  - Pivoting Through Compromised Systems
  - Persistence Mechanisms and Detection Risk
  - Mapping the Post-Exploitation Phase to Reporting
- Applied activity: Learners trace a described lateral movement path across three systems and identify the point where detection risk was highest.

### Module 14: Tools and Scripting for Penetration Testing

- Lessons:
  - Reconnaissance and Scanning Tool Categories
  - Exploitation Framework Fundamentals

- Scripting Basics for Automation, Python and PowerShell
- Choosing the Right Tool for Each Engagement Phase

- Applied activity: Learners match a set of described testing tasks to the tool category best suited to each, and justify the choice.