

Certified Penetration Testing Associate (CPTA) Training

Centri Authorized Training · Applied Technology Academy

Centri's Certified Penetration Testing Associate is the offensive counterpart to Blue Team Level 1: a hands-on route through the whole engagement, from scoping and discovery to exploitation, privilege escalation, lateral movement and reporting. It covers enterprise infrastructure, Active Directory, web applications and AWS across 600+ lessons and 60+ labs, and certifies on a three-part practical exam. ATA is Centri's exclusive US instructor-led partner.

LEVEL Junior to Intermediate	DURATION On-demand · approx. 100 hours	COURSE CODE CPTA	DELIVERY Instructor-led
---	---	-----------------------------------	--

Course Overview

- Twenty-four modules covering the full engagement rather than isolated techniques.
- Four environments in one course: enterprise infrastructure, Active Directory, web applications and AWS.
- 600+ lessons, activities and quizzes with more than 60 hands-on labs.
- Assessed by a three-part practical exam, with a resit included.

Course Outline

- **Module 1. Introduction to Penetration Testing**
 - What the discipline is and how engagements run.
- **Module 2. Networking Essentials**
 - The networking an attacker has to understand.
- **Module 3. Linux Essentials**
 - Linux fundamentals for offensive work.
- **Module 4. Windows Essentials**
 - Windows fundamentals for offensive work.
- **Module 5. Python Essentials**
 - Scripting and automation for testers.
- **Module 6. Introduction to Databases**
 - Database fundamentals behind data-layer attacks.
- **Module 7. The Penetration Testing Process**
 - Scoping, methodology and engagement structure.

- **Module 8. Network Discovery**
 - Enumerating hosts, services and attack surface.
- **Module 9. Vulnerability Assessment**
 - Finding and validating weaknesses.
- **Module 10. Password Attacks**
 - Credential attacks and where they succeed.
- **Module 11. Exploitation Essentials**
 - Turning a vulnerability into access.
- **Module 12. File Transfer & Data Movement**
 - Moving tooling and data during an engagement.
- **Module 13. Linux Privilege Escalation**
 - Escalating from a foothold on Linux.
- **Module 14. Windows Privilege Escalation**
 - Escalating from a foothold on Windows.
- **Module 15. Lateral Movement Essentials**
 - Moving between hosts once inside.
- **Module 16. Introduction to Active Directory**
 - How AD works, from an attacker's view.
- **Module 17. Introduction to Active Directory Attacks**
 - Common AD attack paths.
- **Module 18. Persistence Essentials**
 - Maintaining access.
- **Module 19. Web Application Essentials**
 - How web applications are built and exposed.
- **Module 20. Introduction to Web Application Attacks**
 - SQL injection, command injection, file inclusion and path traversal.
- **Module 21. AWS Essentials**
 - Cloud fundamentals for testers.
- **Module 22. Introduction to AWS Penetration Testing**
 - Testing and exploiting AWS environments.
- **Module 23. Introduction to Command & Control (C2) and Red Teaming**
 - C2 concepts and where red teaming differs from penetration testing.
- **Module 24. Practice Labs and Exam Preparation**
 - Consolidation across 60+ labs ahead of the three-part practical exam.

Prerequisites

- Centri recommends zero to three years of experience; the course is pitched junior to intermediate.
- There are no entry requirements for the exam, though Centri strongly recommends completing the labs first.
- Networking, Linux, Windows and Python fundamentals are all covered in the course.

Follow-On Courses

- Blue Team Level 1 (BTL1)
- Certified Detection Engineering Associate (CDEA)

Who Should Attend

- Aspiring penetration testers and ethical hackers starting out.
- Security consultants who need a defensible testing methodology.
- Red team operators building breadth across infrastructure, AD, web and cloud.

Blue teamers — SOC analysts, threat hunters, detection engineers and incident responders — who want to understand attacker tradecraft first-hand.

What You'll Learn

By the end of this course, participants will be able to:

- scope and run a penetration test against a defined methodology
- enumerate networks, services and attack surface
- identify and validate vulnerabilities, then exploit them to gain access
- escalate privilege on both Windows and Linux, and move laterally
- attack Active Directory along common paths and establish persistence
- test web applications for injection, file inclusion and path traversal flaws
- test and exploit AWS environments
- explain C2 and where red teaming differs from penetration testing
- report findings in terms a client can act on

Ready to enroll? Call 800.674.3550 or email Info@AppliedTechAc.com — private team cohorts, GSA MAS purchasing, military credentialing funding, VA GI Bill and VR&E and student financing available.