

PenTest+

In this course, you'll learn valuable pen testing skills for a variety of platforms and applications, including vulnerability assessment and analysis, and planning, scoping, and managing infrastructure weaknesses.

course outline

IS THIS COURSE FOR YOU?

This course is designed for IT professionals seeking to learn vulnerability assessment from a broad, comprehensive perspective.

ABOUT THE COURSE

In this course, you'll learn valuable pen testing skills for the cloud, hybrid environments, web applications, and traditional on-premise systems. You'll cover hands-on vulnerability assessment, scanning, and analysis, as well as planning, scoping, and managing infrastructure weaknesses.

You'll learn how to perform vulnerability scanning and passive / active reconnaissance. You'll also learn about vulnerability management, as well as how to analyse the results of reconnaissance exercises.

You'll learn how to prepare for network attacks, wireless attacks, application-based attacks, and attacks on cloud technologies. You'll also develop the skills needed to perform post-exploitation analysis.

The course will also help prepare you for the CompTIA PenTest+ (PT0-002) certification exam.

AIMS AND OBJECTIVES

This course will prepare you for roles of greater responsibility in IT security, as well as for CompTIA's PenTest+ certification exam.

PRE-REQUISITES

Network+ or Security+ or equivalent background with 3-4 years in information security or related experience.

COURSE CONTENT

- Module 1 - Scoping & Engagement
- Module 2 - Professionalism & Integrity
- Module 3 - Passive Reconnaissance
- Module 4 - Active Reconnaissance
- Module 5 - Vulnerability Scanning
- Module 6 - Network Attacks & Exploits
- Module 7 - Wireless Attacks
- Module 8 - Application-based Attacks
- Module 9 - Attacks on Cloud Technologies
- Module 10 - Attacks on Specialised Systems
- Module 11 - Social Engineering Attacks
- Module 12 - Post-exploitation Techniques
- Module 13 - Written Reports
- Module 14 - Communication & Post-Report Activities
- Module 15 - Analysing Tool & Script Output
- Module 16 - Penetration Testing Tools

CAREER PATH

This course and associated certification will stand you in good stead in roles that involve analysing, monitoring, and protecting an organisation's infrastructure.

COURSE DURATION

40 hours. This will vary from individual to individual based on prior knowledge and ability.



CPD POINTS: 40

CPD points awarded upon successful completion.



Building careers
for 180 years.

