Course Name	CompTIA PenTest+
Course Duration	5 Days
Course Structure	Instructor-Led
Course Overview	In this course, delegates will be introduced to some general concepts and methodologies related to penetration testing. Delegates will learn how to plan, analyze, and report on penetration tests. This course can also assist delegates who pursuing the CompTIA PenTest+ certification, as tested in exam PT0-001. The course is designed to provide content and activities that correlate to the exam objectives, and therefore can be a resource as you prepare for the examination. **Audience profile** This course is designed for IT professionals who want to develop penetration testing skills to enable them to identify information-system vulnerabilities and effective remediation techniques for those vulnerabilities. Target students who also need to offer practical recommendations for action to properly protect information systems and their contents will derive those skills from this course. **Prerequisites** Before attending this course, delegates must have intermediate knowledge of information security concepts, including but not limited to: • Identity and access management (IAM) • Cryptographic concepts and implementations • Computer networking concepts and implementations • Common security technologies • Practical experience in securing various computing environments, including small to medium businesses, as well as enterprise environments Delegates can obtain this level of skills and knowledge by taking the CompTIA Security+ (IN-SE) course and obtaining the appropriate certification by completing and passing the CompTIA SY0-501 exam.
Course Outcome	After completing this course, students will be able to: • Plan and scope penetration tests • Conduct passive reconnaissance • Perform non-technical tests to gather information • Conduct active reconnaissance • Analyze vulnerabilities

	• Penetrate networks • Exploit host-based vulnerabilities • Test applications • Complete post-exploit tasks • Analyze and report pen test results
Course Details	**Topic 1:** Planning and Scoping Penetration Tests **Topic 2:** Conducting Passive Reconnaissance **Topic 3:** Performing Non-Technical Tests **Topic 4:** Conducting Active Reconnaissance **Topic 5:** Analyzing Vulnerabilities **Topic 6:** Penetrating Networks **Topic 7:** Exploiting Host-Based Vulnerabilities **Topic 8:** Testing Applications **Topic 9:** Completing Post-Exploit Tasks **Topic 10:** Analyzing and Reporting Pen Test Results