CompTIA PenTest+

Duration 5 Days

COURSE DESCRIPTION

CompTIA PenTest+ is one of the most comprehensive courses that cover all the PenTesting stages. PenTest+ is the only exam that incorporates all aspects of vulnerability management. This course also includes all the latest techniques used against the expanded attack surfaces.

CompTIA has designed a CompTIA PenTest+ PT0-002 course where you will learn to plan and scope a penetration testing engagement, perform pen-testing using correct techniques, tools, and then analyze the outcomes, you will also learn how to understand the compliance and legal requirements, you will also be able to produce a written report containing proposed remediation techniques.

From the CompTIA PT0-002 course designed by CompTIA, you will also learn about Regulatory compliance considerations, location restrictions, rules of engagement, background checks of penetration testing teams, DNS lookups, open-source intelligence, enumeration, fingerprinting, scanning methods, attack methods, injection attacks, report audience, data structures and many more..

COURSE OBJECTIVES

After completing this course, you will accomplish following:

- Knowledge on performing penetration testing and vulnerability scanning.
- Analyzing the results and data and communicate results through effective reporting.
- Analyze the importance of planning and key aspects of compliance
- Learn to explore the network, wireless and RF vulnerabilities and physical security attacks and perform post-exploitation techniques.
- Understand penetration testing through various coding scripts such as Python, Ruby, Bash and PowerShell to gather information from the tool.
- Understand the pliability of the network to vulnerable attacks and how to mitigate them.
- Knowledge on overall state of improving the IT security across an organisation

COURSE OUTLINE

Lesson 1: Planning and Scoping

- Compare and contrast governance, risk, ad compliance concepts
- Explain the importance of scoping organizations/customer requirements
- Given a scenario, demonstrate an ethical hacking mindset by maintaining professionalism and integrity.

Lesson 2: Information gathering and vulnerability scanning

- Given a scenario, perform passive reconnaissance
- Given a scenario, perform active reconnaissance
- Given a scenario, analyze the results of a reconnaissance exercise
- Given a scenario, perform vulnerability scanning

Lesson 3: Attacks and Exploits

- Given a scenario, research attack vectors and perform network attacks
- Given a scenario, research attack vectors and perform wireless attacks
- Given a scenario, research attack vectors and perform application-based attacks
- Given a scenario, research attack vectors and perform attacks on cloud technologies
- Explain common attacks and vulnerabilities against specialized systems
- Given a scenario, perform a social engineering or physical attack
- Given a scenario, perform post-exploitation techniques

Lesson 4: Reporting and Communication

- Compare and contrast important components of written reports
- Given a scenario, analyze the findings and recommend the appropriate remediation within a report
- Explain the importance of communication during the penetration testing process
- Explain post-report delivery activities

Lesson 5: Tools and Code Analysis

- Explain the basic concepts of scripting and software development
- Given a scenario, analyze a script or code sample for use in a penetration test
- Explain use cases of the following tools during the phases of a penetration test

WHO SHOULD ATTEND

- IT Security Analyst
- Penetration and Vulnerability tester
- Network Security operational
- Application security vulnerability analyst

PREREQUISITES

- Minimum 3 to 4 years of experience in the field of IT security or related field.
- Network and security knowledge.

NETWORK TRAINING CENTER CO.,LTD. (NTC) | www.trainingcenter.co.th
Call us today 0-2634-7993-4
177/1 BUI Bldg., 14th Fl., Unit 1, 3 & 4, Surawongse Rd., Suriyawongse, Bangrak, Bangkok, THAILAND | Email: sales@trainingcenter.co.th