CompTIA PenTest+ Course Outline

EXAM NUMBER: PT0-002

Planning and Scoping

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

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.

Attacks and Exploit

- 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.

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.

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.