CompTIA PenTest+

The CompTIA PenTest+ will certify the successful candidate has the knowledge and skills required to plan and scope a penetration testing engagement within compliance requirements, conduct enumeration and reconnaissance activities, analyze vulnerabilities, launch attacks, exfiltrate data and produce a written report with remediation techniques.

The certification validates that successful candidates have the knowledge and skills to:

- Plan, scope, and perform information gathering as part of a penetration test.
- Perform attacks that are aligned to and fulfill legal and compliance requirements.
- Perform each phase of a penetration test using and modifying appropriate tools and use the appropriate tactics, techniques, and procedures.
- Analyze the results of each phase of a penetration test to develop a written report, effectively communicate findings to stakeholders and provide practical recommendations.

Exam Objectives Comparison

The following table aligns exam objectives from PT0-003 and PT0-002 for comparison. Skills are aligned by best match.

PT0-003		PT0-002		Gap Indicator
1.1	Summarize pre-engagement activities.	1.1	Compare and contrast governance, risk, and compliance concepts.	Maps
1.1	Summarize pre-engagement activities.	1.2	Explain the importance of scoping and organizational/customer requirements.	Maps
1.2	Explain collaboration and communication activities.	4.3	Explain the importance of communication during the penetration testing process.	Maps
1.3	Compare and contrast testing frameworks and methodologies.	1.2	Explain the importance of scoping and organizational/customer requirements.	Maps
1.4	Explain the components of a penetration test report.	4.1	Compare and contrast important components of written reports.	Gap
1.5	Given a scenario, analyze the findings and recommend the appropriate remediation within a report.	4.2	Given a scenario, analyze the findings and recommend the appropriate remediation within a report.	Maps
2.1	Given a scenario, apply information gathering techniques.	2.1	Given a scenario, perform passive reconnaissance.	Maps
2.1	Given a scenario, apply information gathering techniques.	2.2	Given a scenario, perform active reconnaissance.	Maps
2.1	Given a scenario, apply information gathering techniques.	2.3	Given a scenario, analyze the results of a reconnaissance exercise.	Maps
2.2	Given a scenario, apply enumeration techniques.	n/a		New content
2.3	Given a scenario, modify scripts for reconnaissance and enumeration.	n/a		New content
2.4	Given a scenario, use the appropriate tools for reconnaissance and enumeration.	n/a		New content
3.1	Given a scenario, conduct vulnerability discovery using various techniques.	2.4	Given a scenario, perform vulnerability scanning.	Maps
3.2	Given a scenario, analyze output from reconnaissance, scanning, and enumeration phases.	n/a		New content
3.3	Explain physical security concepts.	3.6	Given a scenario, perform a social engineering or physical attack.	Maps
4.1	Given a scenario, analyze output to prioritize and prepare attacks.	n/a		New content

PT0-003		PT0-002		Gap Indicator
4.2	Given a scenario, perform network attacks using the appropriate tools.	3.1	Given a scenario, research attack vectors and perform network attacks.	Maps
4.3	Given a scenario, perform authentication attacks using the appropriate tools.	n/a		New content
4.4	Given a scenario, perform host-based attacks using the appropriate tools.	n/a		New content
4.5	Given a scenario, perform web application attacks using the appropriate tools.	3.3	Given a scenario, research attack vectors and perform application-based attacks.	Maps
4.6	Given a scenario, perform cloud-based attacks using the appropriate tools.	3.4	Given a scenario, research attack vectors and perform attacks on cloud technologies.	Maps
4.7	Given a scenario, perform wireless attacks using the appropriate tools.	3.2	Given a scenario, research attack vectors and perform wireless attacks.	Maps
4.8	Given a scenario, perform social engineering attacks using the appropriate tools.	3.6	Given a scenario, perform a social engineering or physical attack.	Maps
4.9	Explain common attacks against specialized systems.	3.5	Explain common attacks and vulnerabilities against specialized systems.	Maps
4.10	Given a scenario, use scripting to automate attacks.	5.1	Explain the basic concepts of scripting and software development.	Gap
4.10	Given a scenario, use scripting to automate attacks.	5.2	Given a scenario, analyze a script or code sample for use in a penetration test.	Maps
5.1	Given a scenario, perform tasks to establish and maintain persistence.	3.7	Given a scenario, perform post-exploitation techniques.	Maps
5.2	Given a scenario, perform tasks to move laterally throughout the environment.	n/a		New content
5.3	Summarize concepts related to staging and exfiltration.	n/a		New content
5.4	Explain cleanup and restoration activities.	4.4	Explain post-report delivery activities.	Maps

CompTIA