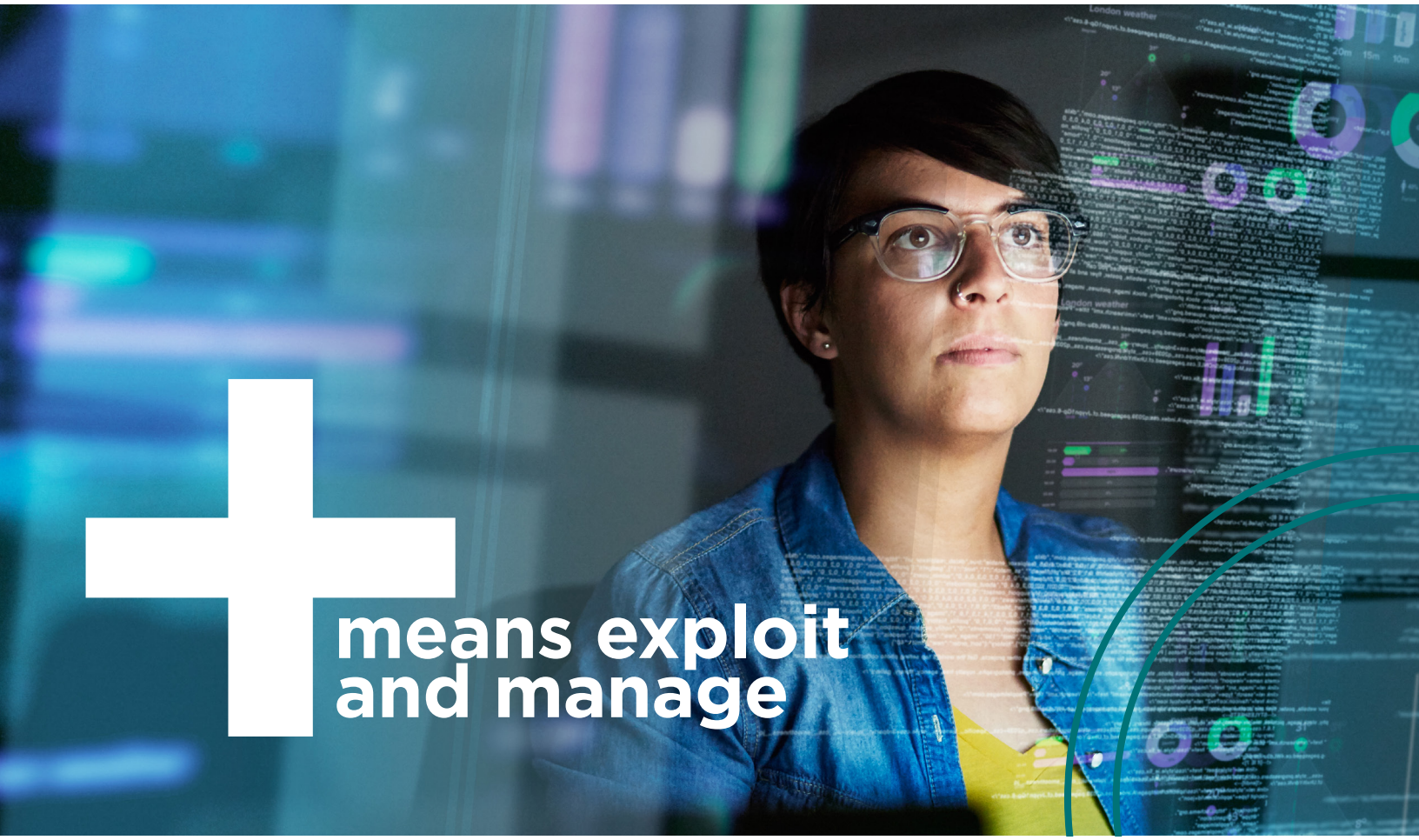
CompTIA



PT0-001 vs PT0-002 Exam Objectives Comparison

Cybercrime continues to rapidly increase year after year, as a result more IT job roles are tasked with identifying vulnerabilities and remediation techniques across broader surfaces. Additionally, as organizations continue to advance their offensive strategy to prevent sensitive data from falling into the wrong hands, the need for skilled IT Professionals to proactively test networks and security is at an all-time high. Updates to PenTest+ assess the most up-to-date penetration testing, and vulnerability assessment and management skills necessary to determine the resiliency of the network against attacks.

PenTest+ (PT0-002) has been updated to address newer pen testing techniques for the latest attack surfaces, including the cloud, hybrid environments, web applications, and more ethical hacking concepts, vulnerability scanning, and code analysis. In addition, it covers best practices, and the latest techniques cybersecurity professionals use to plan, scope, and manage weaknesses and not simply exploit them, strengthening an organization's security and preventing the next attack.

PenTest+ is accredited by ANSI as meeting the ISO/IEC 17024 standard and is approved by U.S. Department of Defense (DoD) to fulfill Directive 8570.01-M/8140 requirements. It is compliant with government regulations under the Federal Information Security Management Act (FISMA).

CompTIA PenTest+

Exam Objectives Comparison

The following table aligns exam objectives from PT0-001 and PT0-002 for comparison. Skills are aligned by best match.

PT0-001	PT0-002	RESULTS
1.2 Explain key legal concepts	1.1 Compare and contrast governance, risk, and compliance concepts	Maps
1.4 Explain the key aspects of compliance-based assessments	1.1 Compare and contrast governance, risk, and compliance concepts	Maps
1.3 Explain the importance of scoping an engagement properly.	1.2 Explain the importance of scoping and organizational/customer requirements	Gap
n/a	1.3 Given a scenario, demonstrate an ethical hacking mindset by maintaining professionalism and integrity	New Content
2.1 Given a scenario, conduct information gathering using appropriate techniques	2.1 Given a scenario, perform passive reconnaissance	Maps
2.1 Given a scenario, conduct information gathering using appropriate techniques	2.2 Given a scenario, perform active reconnaissance	Maps
n/a	2.3 Given a scenario, analyze the results of a reconnaissance exercise	New Content
2.2 Given a scenario, perform a vulnerability scan	2.4 Given a scenario, perform vulnerability scanning	Maps
4.1 Given a scenario, use Nmap to conduct information gathering exercises	2.4 Given a scenario, perform vulnerability scanning	Maps
3.2 Given a scenario, exploit network-based vulnerabilities	3.1 Given a scenario, research attack vectors and perform network attacks	Maps
3.3 Given a scenario, exploit wireless and RF-based vulnerabilities	3.2 Given a scenario, research attack vectors and perform wireless attacks	Maps
3.4 Given a scenario, exploit application-based vulnerabilities	3.3 Given a scenario, research attack vectors and perform application-based attacks	Maps
n/a	3.4 Given a scenario, research attack vectors and perform attacks on cloud technologies	New Content
n/a	3.5 Explain common attacks and vulnerabilities against specialized systems	New Content
3.1 Compare and contrast social engineering attacks	3.6 Given a scenario, perform a social engineering or physical attack	Gap
3.6 Summarize physical security attacks related to facilities	3.6 Given a scenario, perform a social engineering or physical attack	Gap
3.7 Given a scenario, perform post-exploitation techniques	3.7 Given a scenario, perform post-exploitation techniques	Maps
2.1 Given a scenario, conduct information gathering using appropriate techniques	3.7 Given a scenario, perform post-exploitation techniques	Maps
5.1 Given a scenario, use report writing and handling best practices	4.1 Compare and contrast important components of written reports	Maps
5.3 Given a scenario, recommend mitigation strategies for discovered vulnerabilities	4.2 Given a scenario, analyze the findings and recommend the appropriate remediation within a report	Gap

PT0-001	PT0-002	RESULTS
5.4 Explain the importance of communication during the penetration testing process	4.3 Explain the importance of communication during the penetration testing process	Maps
5.2 Explain post-report delivery activities	4.4 Explain post-report delivery activities	Maps
n/a	5.1 Explain the basic concepts of scripting and software development	New Content
4.4 Given a scenario, analyze a basic script (limited to Bash, Python, Ruby, and PowerShell)	5.2 Given a scenario, analyze a script or code sample for use in a penetration test	Maps
4.2 Compare and contrast various use cases of tools	5.3 Explain use cases of the following tools during the phases of a penetration test	Maps