CERTIFICATION GUIDE

CompTIA PenTest+

What is it?

CompTIA PenTest+ is a certification for intermediate skills level cybersecurity professionals who are tasked with hands-on penetration testing to identify, exploit, report, and manage vulnerabilities on a network.

Why is it different?

- CompTIA PenTest+ is the only exam taken at a Pearson VUE testing center with both hands-on, performance-based questions and multiple-choice, to ensure each candidate possesses the skills, knowledge, and ability to perform tasks on systems.
- PenTest+ exam not only covers hands-on penetration testing and vulnerability assessment, but includes management skills used to plan, scope, and manage weaknesses, not just exploit them.
- PenTest+ is unique because our certification requires a candidate to demonstrate the hands-on ability and knowledge to test devices in new environments such as the cloud and mobile, in addition to traditional desktops and servers.

About the exam

PenTest+ assesses the most up-to-date penetration testing, and vulnerability assessment and management skills necessary to determine the resiliency of the network against attacks. Successful candidates will also have the intermediate skills and best practices required to customize assessment frameworks to effectively collaborate on and report findings and communicate recommended strategies to improve the overall state of IT security.

CompTIA PenTest+ is compliant with ISO 17024 standards and approved by the US DoD to meet directive 8140/8570.01-M requirements. Regulators and government rely on ANSI accreditation, because it provides confidence and trust in the outputs of an accredited program. Over 2.3 million CompTIA ISO/ANSI-accredited exams have been delivered since January 1, 2011.

Exam #
PT0-001

Release Date
July 2018

Languages
English

CE Required?
Yes

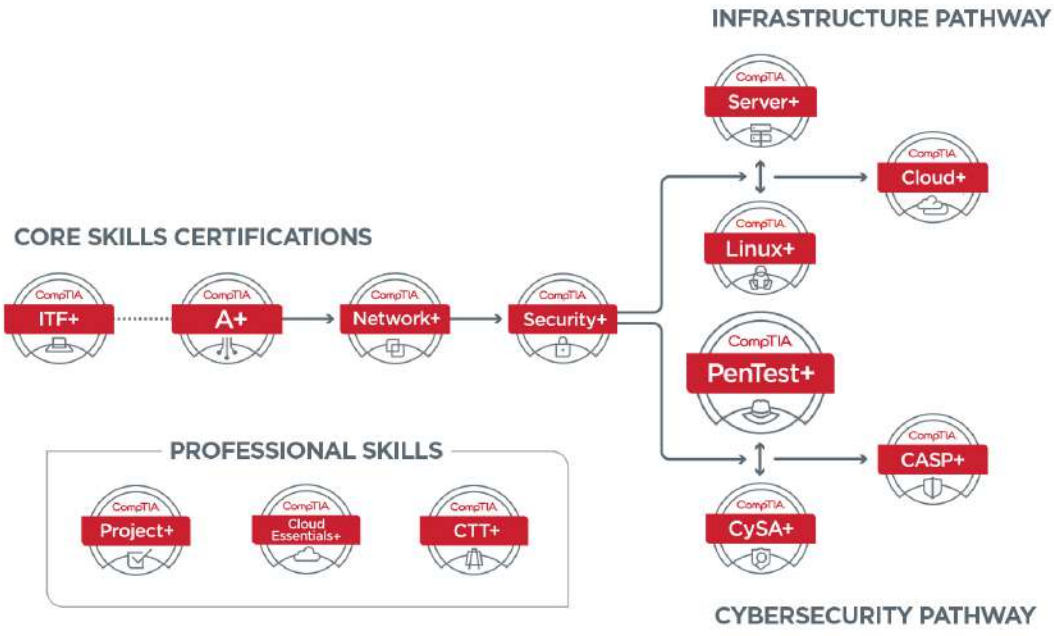
Accreditation
Accredited by ANSI to show compliance with the ISO 17024 Standard. It is also approved by the DoD for Directive 8140/8570.01-M.

How does PenTest+ Compare to Alternatives?

	PenTest+	CEH	GPEN	OSCP
Certification	**PenTest+**	**EC-Council Certified Ethical Hacker (CEH)**	**GIAC Penetration Tester (GPEN)**	**Offensive Security Certified Professional (OSCP)**
Performance-based Questions	Yes	No A second exam, CEH (Practical) offers performance-based questions	No	Yes
Exam Length	1 exam, 90 questions, 165 minutes	1 exam, 4 hours	1 exam, 3 hours	1 exam, 24 hours
Experience Level	Intermediate	Intermediate	Intermediate	Intermediate / Advanced
Exam Focus	Penetration testing and vulnerability assessment	Penetration testing	Penetration Testing from a Business-value	Real World-based with a Lab and submitted report
Prerequisites	Network+, Security+ or equivalent knowledge. Minimum of 3-4 years of hands-on information security or related experience. While there is no required prerequisite, PenTest+ is intended to follow CompTIA Security+ or equivalent experience and has a technical, hands-on focus.	CEH Training, 2 years information security experience, Endorsement	None	Must first complete the Penetration Testing with Kali Linux training course (self-paced)

CompTIA Certification Pathway

CompTIA certifications align with the skillsets needed to support and manage cybersecurity. Enter where appropriate for you. Consider your experience and existing certifications or course of study.



"CompTIA PenTest+ exam is different because it is not only technical, but also demonstrates that a candidate has the ability to understand and deliver results. A manager could hire a PenTest+ certified individual and fully trust that he or she would alleviate day to day operations."

Josh Skorich
Managing Principal

Technical Areas Covered in the Certification

Planning and Scoping
15%

- Explain the importance of planning for an engagement
- Explain legal concepts
- Explain the key aspects of compliance-based assessments

Information Gathering and Vulnerability Identification
22%

- Conduct information gathering using appropriate techniques
- Perform a vulnerability scan
- Analyze vulnerability scan results
- Explain the process of leveraging information to prepare for exploitation
- Explain weakness related to specialized systems

Attacks and Exploits
30%

- Compare and contrast social engineering attacks
- Exploit network-based vulnerabilities
- Exploit wireless and RF-based vulnerabilities
- Exploit application-based vulnerabilities
- Exploit local host vulnerabilities
- Summarize physical security attacks related to facilities
- Perform post-exploitation techniques

Penetration Testing Tools
17%

- Use NMAP to conduct information gathering exercises
- Compare and contrast various use cases of tools
- Analyze tool output or data related to a penetration test
- Analyze a basic script (limited to: Bash, Python, Ruby, PowerShell)

Reporting and Communication
16%

- Use report writing and handling best practices
- Explain post-report delivery activities
- Recommend mitigation strategies for discovered vulnerabilities
- Explain the importance of communication during thepenetration testing process

"PenTest+ demonstrates knowledge beyond entry-level and that the individual is competent to add value within a pentester team immediately; this person can hit the ground running."

Gavin Dennis
Senior IT Security Consultant

Organizations that contributed to the development of PenTest+

- Brotherhood Mutual
- Global Cyber Security
- SecureWorks
- North State Technology Solutions
- BlackFire Consulting
- TransUnion
- Las Vegas Sands Corporation
- Integra LifeSciences
- Enterprise Holdings
- Paylocity
- Johns Hopkins University Applied Physics Laboratory
- ASICS Corporation

Top PenTest+ job roles

- Penetration/Vulnerability Tester
- Security Analyst (II)
- Vulnerability Assessment Analyst
- Network Security Operations

Research and Statistics

Fastest-Growing Job Category The U.S. Bureau of Labor Statistics predicts that roles requiring penetration testing will be within the fastest-growing job category, with **31 percent overall growth by 2029.**.[1]

Growing Priority The overall penetration testing market is estimated to **grow 21.8 percent from 2020 to 2025**.[2]

Learn with CompTIA

Official CompTIA Content is the only study material exclusively developed by CompTIA for the CompTIA certification candidate; no other content library covers all exam objectives for all certifications. CompTIA eBooks and CertMaster Products have been developed with our Official CompTIA Content to help you prepare for your CompTIA certification exams with confidence. Learners now have everything they need to learn the material and ensure they are prepared for the exam and their career.

Whether you are just starting to prepare and need comprehensive training with CertMaster Learn, need a final review with CertMaster Practice, or need to renew your certification upon expiration with CertMaster CE, CertMaster's online training tools have you covered.

What does it mean to be a "high stakes" exam?

An extraordinarily high level of rigor is employed in developing CompTIA certifications. Each question created for a CompTIA exam undergoes multiple layers of quality assurance and thorough psychometric statistical validation, ensuring CompTIA exams are highly representative of knowledge, skills and abilities required of real job roles. This is why CompTIA certifications are a requirement for many professionals working in technology. Hiring managers and candidates alike can be confident that passing a CompTIA certification exam means competence on the job. This is also how CompTIA certifications earn the ANSI/ISO 17024 accreditation, the standard for personnel certification programs. Over 2.3 million CompTIA ISO/ANSI-accredited exams have been delivered since January 1, 2011.

What does it mean to be a "vendor-neutral" exam?

All CompTIA certification exams are vendor-neutral. This means each exam covers multiple technologies, without confining the candidate to any one platform. Vendor-neutrality is important because it ensures IT professionals can perform important job tasks in any technology environment. IT professionals with vendor-neutral certifications can consider multiple solutions in their approach to problem-solving, making them more flexible and adaptable than those with training in just one technology.

What is a Performance Certification?

CompTIA performance certifications validate the skills associated with a particular job or responsibility. They include simulations that require the test taker to demonstrate multi-step knowledge to complete a task. CompTIA has a higher ratio of these types of questions than any other IT certifying body.

1. Occupational Outlook Handbook, BLS, 2019
2. Penetration Testing Market Report, Markets and Markets, 2019