What is it?

CompTIA PenTest+ is for cybersecurity professionals tasked with penetration testing and vulnerability management.

Why is it different?

- **CompTIA PenTest+ is the most comprehensive exam covering all penetration testing stages.** Unlike other penetration testing exams that only cover a portion of stages with essay questions and hands-on, PenTest+ uses both performance-based and knowledge-based questions to ensure all stages are addressed.

- **PenTest+ is the only exam on the market to include all aspects of vulnerability management.** It not only covers hands-on vulnerability assessment, scanning, and analysis, but also includes planning, scoping, and managing weaknesses, not just exploiting them.

- **PenTest+ is the most current penetration testing exam covering the latest techniques against expanded attack surfaces.** It is a unique exam that requires a candidate to demonstrate the most relevant pen testing skills for the cloud, hybrid environments, web applications, customized systems (IoT), and traditional on-premises.

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. The CompTIA PenTest+ certification exam will verify successful candidates have the knowledge and skills required to:

- Plan and scope a penetration testing engagement
- Understand legal and compliance requirements
- Perform vulnerability scanning and penetration testing using appropriate tools and techniques, and then analyze the results
- Produce a written report containing proposed remediation techniques, effectively communicate results to the management team, and provide practical recommendations
How does PenTest+ Compare to Alternatives?

<table>
<thead>
<tr>
<th>Certification</th>
<th>PenTest+</th>
<th>EC-Council Certified Ethical Hacker (CEH)</th>
<th>GIAC Penetration Tester (GPEN)</th>
<th>Offensive Security Certified Professional (OSCP)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performance-based Questions</td>
<td>Yes</td>
<td>No Second exam required, CEH Practical</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Exam Length</td>
<td>1 exam, 90 questions, 165 minutes</td>
<td>1 exam, 4 hours</td>
<td>1 exam, 3 hours</td>
<td>1 exam, 24 hours</td>
</tr>
<tr>
<td>Experience Level</td>
<td>Intermediate</td>
<td>Beginner / Intermediate</td>
<td>Intermediate</td>
<td>Intermediate / Advanced</td>
</tr>
<tr>
<td>Exam Focus</td>
<td>Penetration testing and vulnerability assessment</td>
<td>Penetration testing</td>
<td>Penetration Testing from a Business-value</td>
<td>Real World-based with a Lab and submitted report</td>
</tr>
<tr>
<td>Prerequisites</td>
<td>Network+, Security+ or equivalent knowledge. Minimum of 3-4 years of hands-on experience working in a security consultant or penetration tester job role.</td>
<td>CEH Training, 2 years information security experience, Endorsement</td>
<td>None</td>
<td>Must first complete the Penetration Testing with Kali Linux training course (self-paced)</td>
</tr>
</tbody>
</table>

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.

Top PenTest+ job roles

- Penetration Tester
- Security Consultant
- Cloud Penetration Tester
- Web App Penetration Tester
- Cloud Security Specialist
- Network & Security Specialist
- Information Security Engineer
- Security Analyst
## Technical Areas Covered in the Certification

<table>
<thead>
<tr>
<th>Planning and Scoping 14%</th>
<th>Information Gathering and Vulnerability Scanning 22%</th>
<th>Attacks and Exploits 30%</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Compare and contrast governance, risk, and compliance concepts</td>
<td>• Given a scenario, be able to perform passive and active reconnaissance and analyze the results of the reconnaissance exercise</td>
<td>• Given a scenario, research attack vectors and have the ability to perform network attacks, wireless attacks, application-based attacks, and attacks on cloud technologies</td>
</tr>
<tr>
<td>• Explain the importance of scoping and organizational/customer requirements</td>
<td>• Ability to perform vulnerability scanning</td>
<td>• Explain common attacks and vulnerabilities against specialized systems</td>
</tr>
<tr>
<td>• Given a scenario, demonstrate an ethical hacking mindset by maintaining professionalism and integrity</td>
<td></td>
<td>• Given a scenario, perform a social engineering or physical attack</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Ability to perform post-exploitation technique</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Reporting and Communication 18%</th>
<th>Tools and Code Analysis 16%</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Compare and contrast important components of written reports</td>
<td>• Explain the basic concepts of scripting and software development</td>
</tr>
<tr>
<td>• Given a scenario, analyze the findings and recommend the appropriate remediation within a report</td>
<td>• Given a scenario, analyze a script or code sample for use in a penetration test</td>
</tr>
<tr>
<td>• Explain the importance of communication during the penetration testing process and potential post-report delivery activities</td>
<td>• Explain use cases of various tools used during the phases of a penetration test</td>
</tr>
</tbody>
</table>

“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
Organizations that contributed to the development of PenTest+

- Paylocity
- SecureWorks
- Micro Focus
- Tata Consultancy Services
- All in One – Benin
- The Mako Group
- Archdiocese of Philadelphia
- RxSense
- Cricket Health
- Washington Patrol Service
- John Hopkins University Applied Physics Laboratory
- U.S. Navy Center for Information Dominance
- U.S. Army
- Target Corp.
- General Dynamics IT (GDIT)
- Tanium
- Ricoh
- aeSolutions Industrial Cybersecurity

Research and Statistics

Fastest-Growing Job Category
The U.S. Bureau of Labor Statistics predicts that information security analysts will be the fastest-growing job category, with 31 percent overall growth between 2019 and 2029.

Growing Priority
The penetration testing market is expected to grow 22 percent from 2020 to 2025. Factors driving the market include enterprises implementing security measures to respond to an increase of sophisticated cyberattacks and rise in mobile-based critical business apps that require more secure endpoint protection.

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 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 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.