BATTLE CARD

CompTIA **PenTest+** (PTO-002)

CompTIA PenTest+ Intro

CompTIA PenTest+ is the most comprehensive cybersecurity exam covering all red team activities and is designed for cybersecurity professionals tasked with penetration testing and vulnerability management.

VALUE Prop 1 (Student)

PenTest+ is a unique exam that demonstrates hands-on skills and knowledge of the most relevant pen testing skills for the cloud, hybrid environments, web applications, customized systems (IoT), and traditional on-premises that employers seek to improve the overall resiliency of enterprise networks.

VALUE Prop 2 (Employer)

PenTest+ validates the most up-to-date skills and competencies needed to determine the resiliency of any network. It focuses on the latest pen testing techniques, attack surfaces, vulnerabilities management, post-delivery, and compliance tasks that are ideal for your company's red team employees to develop a robust security strategy that meets business objectives.

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

Key Differentiators:

- PenTest+ is the most comprehensive exam covering all penetration testing stages. It 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 covering hands-on vulnerability assessment, scanning, and analysis, including planning, coping, and managing weaknesses, not just exploiting them.
- PenTest+ is the most current penetration testing exam covering the latest techniques against expanded attack surfaces, such as cloud, hybrid environments, web applications, customized systems (IoT), and traditional on-premises.

Skills and Competencies Acquired:

- 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

By the Numbers:

- The U.S. Bureau of Labor Statistics predicts that information security analysts will be the fastest-growing job category, with **31%** overall growth between 2019 and 2029.
- The penetration testing market is expected to grow **22%** from 2020 to 2025.

Resources:

- Average Salary:
  - U.S. Penetration Tester: Indeed.com **(https://indeedhi.re/2KN2Zdv)**
  - UK Penetration Tester: ITJobsWatch.co.uk **(https://bit.ly/2XyFh9K)**
- PenTest+ Additional Information: **CompTIA.org/certifications/pentest**
- Recommended Pathways: **CompTIA.org/certifications/which-certification**
- Posts: **https://bit.ly/2WvfkaJ**

Competitors	Talking Points / PenTest+ Advantages
EC-Council Certified Ethical Hacker (CEH)	• CEH assesses vulnerability tools, such as scanners, but NOT vulnerability management like PenTest+. • CEH does NOT cover soft skills, such as business processes, project flow, best practices and professionalism in penetration testing. PenTest+ cover both technical and soft skills. • CEH only covers penetration testing job roles, while PenTest+ covers two job roles, both pen testing and vulnerability assessment and management.
GIAC Penetration Tester (GPEN)	• Unlike GPEN, PenTest+ is based upon cybersecurity industry survey results, providing a heightened real-word applicability compared to other certs.
Offensive Security Certified Professional (OSCP)	• OSCP tests at an advanced level of experience and costs **2X** as much. • OSCP is a 24 hour "capture the flag" exam making PenTest+ both cost and time efficient.

Companies that Endorse PenTest+:

- Paylocity
- SecureWorks
- Jon Hopkins University Applied Physics Laboratory
- Ricoh
- U.S. Navy Center for Information Dominance

Job Roles:

- Penetration Tester
- Security Consultant
- Cloud Penetration Tester
- Web App Penetration Tester
- Cloud Security Specialist
- Network & Security Specialist
- Information Security Engineer
- Security Analyst

CompTIA **PenTest+** (PTO-002)

How does CompTIA Compare?

	CompTIA PenTest+	CEH Certified Ethical Hacker	GPEN	OFFENSIVE security OSCP
Certification	**PenTest+**	**EC-Council Certified Ethical Hacker (CEH)**	**GIAC Penetration Tester (GPEN)**	**Offensive Security Certified Professional (OSCP)**
Performance-based Questions	Yes	No. Second exam required, CEH Practical	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	Beginner / Intermediate	Intermediate	Intermediate / Advanced
Exam Focus	Penetration testing and vulnerability management	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 experience working in a security consultant or penetration tester job role.	CEH Training, 2 years information security experience, Endorsement	None	Must first complete the Penetration Testing with Kali Linux training course (self-paced)

Learn more about PenTest+