Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

PenTest+

Course Description & Overview

SecureNinja's CompTIA PenTest+ (PT0-003) certification training prepares cybersecurity professionals to plan, execute, and manage penetration testing and vulnerability assessment initiatives across diverse environments. This vendor-neutral course covers the latest skills required to identify network and system vulnerabilities, simulate real-world attacks, and provide actionable remediation strategies.

The PenTest+ certification is listed under the DoD 8140 framework and meets requirements for offensive security job roles within government and defense-related organizations. SecureNinja's expert instructors guide students through each domain of the current PT0-003 exam with clear explanations, realistic examples, and access to a proprietary quiz engine that reinforces key concepts and helps students assess their readiness for certification.

Why Choose CompTIA PenTest+

- DoD 8140 Approved: Recognized for offensive cybersecurity roles within the U.S. government and military sectors.
- Vendor-Neutral Credential: Applicable across a wide variety of networks, tools, and platforms.
- Current, Real-World Relevance: Aligned with the latest penetration testing tools and techniques.
- Pathway to Advanced Certifications: Serves as a foundation for further offensive security certifications such as RCCE and CEH.

Topics Covered

- Planning and Scoping: Defining testing goals, legal constraints, and compliance requirements.
- Information Gathering and Vulnerability Scanning: OSINT, active/passive reconnaissance, and vulnerability analysis.
- Attacks and Exploits: Exploiting vulnerabilities in networks, applications, and physical environments.
- Reporting and Communication: Creating reports for different audiences and recommending remediation.
- Tools and Code Analysis: Using tools and basic scripting to automate and enhance testing.

Who is it for

- Penetration Testers: Professionals focused on red teaming and attack simulations.
- Vulnerability Assessment Analysts: Security team members performing scans and assessments.
- Cybersecurity Analysts: Those looking to expand into offensive security testing.

Who Would Benefit

Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

- Security Engineers and Consultants: Engaged in threat modeling and proactive testing engagements.
- Network Administrators: Seeking to understand security from an attacker's perspective.
- Government and DoD Contractors: Requiring 8140-aligned certifications for red team roles.

Prerequisites

While not mandatory, it is recommended that candidates hold Network+ and Security+ certifications and have 3–4 years of hands-on information security or related experience.

Course Outline

1. Planning and Scoping

- Define scope and rules of engagement.
- Understand legal concepts and compliance frameworks.

2. Information Gathering and Vulnerability Scanning

- Conduct passive and active reconnaissance.
- Analyze vulnerabilities using scanning tools and techniques.

3. Attacks and Exploits

- Exploit wireless, application, and network vulnerabilities.
- Evade defenses and escalate privileges during simulated attacks.

4. Reporting and Communication

- Create actionable and audience-appropriate reports.
- Document exploitation steps and provide risk-based recommendations.

5. Tools and Code Analysis

- Use tools such as Metasploit, Burp Suite, Nmap, and Wireshark.
- Understand basic scripting concepts for automating testing.

Course Length

- 5 Days
- 40 Hours

Exam Details

- Exam Code: PT0-003
- Number of Questions: Maximum of 85
- Question Types: Multiple choice and performance-based
- Duration: 165 minutes

Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

- Passing Score: 750 (on a scale of 100–900)

The CompTIA PenTest+ certification provides the practical skills needed to assess system and network vulnerabilities through penetration testing. SecureNinja’s instructor-led training ensures students are well-prepared to pass the PT0-003 exam and contribute to security assurance and offensive operations in both commercial and DoD 8140-aligned environments.