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

# CPENT Training and Certification

## Course Description & Overview

SecureNinja's Certified Penetration Testing Professional (CPENT) certification training prepares advanced cybersecurity professionals to demonstrate their ability to perform penetration testing in real-world enterprise environments. The CPENT program is designed by EC-Council to evaluate a candidate's expertise across a wide array of offensive cybersecurity disciplines within a fully mapped cyber range. Participants are challenged with network, application, and multi-layered attacks under extreme conditions.

This elite program goes far beyond standard pen testing courses by placing students in scenarios that reflect true enterprise networks and defense systems. From IoT to SCADA, CPENT exposes students to bleeding-edge attack surfaces and requires advanced skills in pivoting, exploit development, evasion, and lateral movement. The CPENT training also prepares candidates to earn the prestigious Licensed Penetration Tester (LPT) Master designation—awarded to those who score 90% or higher on the CPENT practical exam.

### Why Choose Certified Penetration Testing Professional (CPENT)

- Advanced Skills Assessment: CPENT evaluates capabilities in a live, fully configured cyber range.
- LPT Master Eligibility: Candidates scoring 90% or higher earn the prestigious Licensed Penetration Tester designation.
- Real-World Focus: Emulates advanced security challenges found in enterprise networks.
- 8140 Compliance: CPENT is approved under the DoD 8140 framework, qualifying candidates for several cybersecurity work roles.

### Topics Covered

- Advanced Penetration Testing Methodologies: Network, application, and wireless testing techniques.
- Pivoting and Privilege Escalation: Gaining deeper access across segmented networks.
- Bypassing Filters: Evading endpoint protection, firewalls, and WAFs.
- Binary Exploitation: Creating and deploying custom shellcode.
- SCADA and IoT Attacks: Assessing modern operational technology infrastructure.
- Web Application and API Testing: Fuzzing, injection, and logic flaw exploitation.

### Who is it for

- Experienced Penetration Testers: Security professionals with hands-on red teaming experience.
- Red Team Members: Those looking to validate their capabilities in real-world offensive operations.
- Cybersecurity Engineers: Seeking advanced certifications aligned with the DoD 8140 framework.

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

## Who Would Benefit

- Government Contractors and Federal Cyber Specialists: Especially those needing 8140-aligned certifications.
- Security Operations and Offensive Teams: Working in red team environments, threat emulation, or penetration testing roles.

## Prerequisites

Candidates should have significant hands-on penetration testing experience and should ideally already hold CEH and/or ECSA certifications. Advanced knowledge of networking, Linux, scripting, and cybersecurity tools is expected.

## Course Outline

1. Advanced Windows Attacks

- Bypass Windows Defender and UAC
- Abuse tokens and services for privilege escalation
- Perform Active Directory enumeration and attacks

2. Attacking IoT and OT Networks

- Explore vulnerabilities in smart devices and embedded systems
- Understand Industrial Control System (ICS) and SCADA attack vectors
- Deploy exploitation frameworks tailored for IoT

3. Writing Advanced Binaries

- Develop custom shellcode and payloads
- Practice exploit writing and buffer overflow techniques
- Bypass exploit mitigation technologies

4. Bypassing Defense Mechanisms

- Evade endpoint detection and response (EDR) tools
- Use living-off-the-land binaries (LOLBins)
- Apply stealthy post-exploitation techniques

5. Pentesting Operational Technology (OT)

- Target systems like programmable logic controllers (PLCs)
- Simulate real-world ICS exploitation scenarios

6. Accessing Remote Systems and Cloud Environments

- Leverage credential attacks to pivot across domains
- Perform enumeration and exploitation of AWS and Azure services

7. Web Application Attacks

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

- Execute advanced injection, authentication, and authorization attacks
- Analyze and exploit modern web application vulnerabilities

8. WLAN and Wireless Pentesting

- Perform wireless reconnaissance and cracking
- Compromise WPA2/WPA3 environments

9. Report Writing and Documentation

- Document findings clearly and professionally
- Present executive and technical summaries

## Course Length

- 5 Days
- 40 Hours

## Exam Details

- Exam Name: CPENT Practical Exam
- Duration: 24 hours (two 12-hour sessions)
- Format: Fully practical exam in a controlled cyber range
- Scoring: 70% required to earn CPENT; 90% or more to be awarded the LPT (Master)

The CPENT program by EC-Council is one of the most rigorous penetration testing certifications available today. With SecureNinja's expert-led training, you'll gain the practical skills and theoretical knowledge required to not only pass the exam but excel in real-world red teaming operations. Completing CPENT is also your gateway to becoming a Licensed Penetration Tester (Master), one of the most prestigious titles in the cybersecurity industry.