Certified Penetration Testing Professional Training

Duration: **5 Day**

BILGINÇ IT Academy
info@bilginc.com
bilginc.com

Overview

The {*training} program is one of the most advanced**penetration testing training courses** in the world.

Designed for experienced ethical hackers and cybersecurity professionals, CPENT teaches how to conduct **real-world penetration tests** across complex enterprise networks — from on-premises systems to IoT, OT, SCADA, and cloud environments.

The course goes beyond traditional network testing. You'll learn to:

- Build your own exploits and tools
- Perform double pivoting to hidden networks
- Customize scripts and payloads
- Conduct binary exploitation and advanced reporting

This hands-on training includes access to the**CPENT Live Range**, EC-Council's advanced cyber range, simulating real enterprise attack surfaces.

The **CPENT certification** validates your ability to think like a hacker, act like a professional, and report like a leader.
It's your next step after CEH and ECSA on the path to becoming an**EC-Council Licensed Penetration Tester (LPT Master).**

Who Should Attend

- Penetration Testers & Red Teamers
- Cybersecurity Analysts & Engineers
- Network Security Professionals
- Ethical Hackers (CEH, ECSA Certified)
- Security Auditors & Consultants

Certified Penetration Testing Professional Training

Duration: **5 Day**

BILGINÇ IT Academy
info@bilginc.com
bilginc.com

What You Will Learn

By the end of this {*training}, you will have gained knowledge and skills in the following areas:

- Perform end-to-end penetration testing in enterprise environments
- Execute OSINT and social engineering operations
- Test IoT, SCADA/OT, and cloud infrastructures
- Develop and customize exploits and scripts
- Apply advanced pivoting and privilege escalation techniques
- Write professional penetration testing reports

Outline

- Introduction to Penetration Testing
- Scoping and Engagement
- Open Source Intelligence (OSINT)
- Social Engineering Testing
- External Network Penetration Testing
- Internal Network Penetration Testing
- Perimeter Device Testing
- Web Application Penetration Testing
- Wireless Penetration Testing
- IoT Penetration Testing
- OT/SCADA Penetration Testing
- Cloud Penetration Testing
- Binary Analysis and Exploitation
- Reporting and Post-Testing Activities