Penetration Testing Specialist Training

Duration: **4 Day**

BILGINÇ IT Academy
info@bilginc.com
bilginc.com

Overview

Penetration Testing, often referred to as *Ethical Hacking*, is one of the most crucial areas of cybersecurity.
This course aims to teach participants how to **identify, exploit, and report vulnerabilities** within information systems —
using the same tools and techniques as real-world attackers, but within a **legal and ethical framework**.

Throughout this hands-on training, you will learn how to plan, execute, and document a full-scale penetration test —
from reconnaissance and scanning to exploitation, post-exploitation, and professional reporting.

By the end of this course, participants will have the technical and analytical skills required to conduct penetration tests in real environments, following **international standards such as OSSTMM, OWASP, and NIST**.

Who Should Attend

This training is designed for professionals who want to develop advanced cybersecurity and ethical hacking skills:

- Cybersecurity Specialists
- Network and System Administrators
- Red Team Members
- Security Auditors and Consultants
- IT Professionals aspiring to become Ethical Hackers

Basic networking and system knowledge is recommended.

What You Will Learn

Upon completion of this course, participants will be able to:

- Conduct end-to-end penetration testing projects independently
- Identify, exploit, and mitigate system vulnerabilities
- Apply ethical hacking methodologies within legal frameworks
- Analyze and report findings using industry standards
- Enhance their organization’s overall cybersecurity resilience

Penetration Testing Specialist Training

Duration: **4 Day**

BILGINÇ IT Academy
info@bilginc.com
bilginc.com

Outline

The course follows a **methodology-driven, hands-on approach**, covering both technical depth and security best practices.

Introduction and Preparation Phase

- What is a Penetration Test?
- Legal requirements and authorization process (NDA, scope definition)
- Why organizations need penetration testing
- Overview of modern testing methodologies and planning

Information Gathering and Reconnaissance

- Passive and active information gathering methods
- Using specialized search engines for reconnaissance
- Network scanning with tools such as **hping** and **Nmap**
- Packet analysis and sniffing techniques (Wireshark)

Vulnerability Analysis

- Common vulnerability scanners (Nessus, OpenVAS, Nikto)
- Understanding scan results and prioritizing risks
- Legal and compliance considerations of security testing

System-Based Penetration Testing

- **Windows Systems:** User privilege escalation, service exploitation
- **Linux / Unix Systems:** Configuration flaws, local privilege escalation
- **Cisco Network Devices:** IOS vulnerabilities, SNMP and configuration testing
- **Database Systems:** SQL injection, access control testing, and data extraction

Network Security Testing

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- Internal network security testing (LAN/WAN)
- Firewall penetration testing and bypass methods
- IPS/WAF evasion techniques
- Exploiting weaknesses in security infrastructure

Wireless and DDoS Testing

- Wireless network vulnerabilities (WEP, WPA2, WPA3)
- DoS/DDoS attack simulations and defense strategies

Exploitation Techniques

- What is Exploitation?
- Advanced exploitation and payload delivery
- Malware, Trojan, and Backdoor analysis
- Password attacks (Brute-force, Dictionary, Hybrid)

Social Engineering

- Understanding social engineering concepts
- Real-world phishing and impersonation attacks
- Psychological manipulation techniques and countermeasures

Reporting and Documentation

- How to write a professional penetration testing report
- Risk classification (CVSS, CWE)
- Executive summaries for management
- Report optimization and best practices