OffSec PEN-200 (OSCP) Training

Duration: **5 Day**

BILGINC IT Academy
info@bilginc.com
bilginc.com

Overview

OffSec PEN-200 is a comprehensive hands-on penetration testing program designed for cybersecurity professionals seeking to develop advanced offensive security skills and prepare for the globally recognized OffSec Certified Professional (OSCP and OSCP+) certifications.

Built around Kali Linux and practical lab environments, the course teaches a structured methodology for identifying, exploiting, documenting, and validating security vulnerabilities in modern systems. Participants gain real-world experience through immersive exercises that simulate enterprise environments and common attack scenarios.

The program combines theoretical concepts with extensive practical application, enabling learners to understand penetration testing workflows, vulnerability assessment techniques, web application security testing, exploit development, and professional reporting practices.

Participants receive 12 months of access to the OffSec PEN-200 learning platform and laboratory environment to support ongoing skill development and certification preparation.

Prerequisites

Although there are no formal prerequisites, participants are strongly encouraged to have:

- A solid understanding of TCP/IP networking concepts
- Familiarity with Linux and Windows operating systems
- Basic scripting knowledge using Bash, Python, or similar languages
- Foundational cybersecurity knowledge

Learners new to offensive security may benefit from completing an introductory security course before attending.

Who Should Attend

This course is designed for:

- Penetration Testers
- Security Analysts
- Threat Hunters
- System and Network Administrators
- Red Team Professionals
- Offensive Security Practitioners
- Individuals pursuing OSCP certification
- IT professionals transitioning into cybersecurity roles

OffSec PEN-200 (OSCP) Training

Duration: **5 Day**

BILGINC IT Academy
info@bilginc.com
bilginc.com

What You Will Learn

By the end of this course, participants will be able to:

- Apply industry-standard penetration testing methodologies
- Conduct reconnaissance and information-gathering activities
- Perform vulnerability assessments and validation
- Exploit common web application vulnerabilities
- Execute client-side attack techniques
- Locate, evaluate, and customize public exploits
- Produce professional penetration testing reports
- Build practical skills required for OSCP and OSCP+ certification success

Outline

Introduction to Cybersecurity

- Security fundamentals and terminology
- Current threat landscape
- Ethical hacking principles
- Penetration testing lifecycle

Penetration Testing Reporting

- Documenting technical findings
- Risk assessment and prioritization
- Writing remediation recommendations
- Reporting for technical and business audiences

Information Gathering and Reconnaissance

- Active and passive reconnaissance
- Network mapping techniques
- Target identification
- Discovery using industry-standard tools

Vulnerability Assessment

- Vulnerability scanning methodologies
- Interpreting assessment results
- Prioritizing findings
- Validating vulnerabilities

Web Application Security

- Modern web application architecture
- Attack surface analysis
- Identifying common weaknesses

Common Web Attacks

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- Cross-Site Scripting (XSS)
- SQL Injection
- Session management vulnerabilities
- Authentication and authorization weaknesses

SQL Injection Techniques

- Identifying injectable parameters
- Data extraction techniques
- Privilege escalation opportunities

Client-Side Attacks

- Browser-based attack vectors
- JavaScript-related vulnerabilities
- User-focused exploitation techniques

Public Exploit Research

- Identifying trusted exploit sources
- Evaluating exploit reliability
- Integrating exploits into testing workflows

Exploit Customization

- Modifying payloads
- Bypassing defensive mechanisms
- Developing proof-of-concept attacks