

Ethical Hacking: OWASP Top 10 & Network Pentesting

6 Days

48 HOURS

15

MODULES

36

TOPICS

LEARNING OBJECTIVES

- Explain the phases and core concepts of ethical hacking
- Apply footprinting and reconnaissance to gather target information
- Perform network scanning and enumeration to identify hosts and services
- Assess vulnerabilities using vulnerability scanning tools
- Apply password attack and privilege escalation techniques
- Identify malware types and anti-virus evasion techniques
- Exploit OWASP Top 10 flaws including SQL injection and XSS
- Analyse wireless, mobile, IoT and cloud security threats

15 Modules, 36 Topics

01

Introduction to Ethical Hacking

TOPICS

- Overview of Ethical Hacking and Penetration Testing
- **Core Concepts:** Information Security and Threat Landscapes
- Phases of Ethical Hacking

02

Footprinting and Reconnaissance

TOPICS

Footprinting Concepts and Techniques · Active vs. Passive Reconnaissance · Tools for Reconnaissance

03

Scanning Networks

TOPICS

Network Scanning Techniques · Tools for Scanning · Identifying Open Ports and Services

04

Enumeration

TOPICS

- Enumerating Users, Groups, and Shared Resources
- Tools for Enumeration

05

Vulnerability Analysis

TOPICS

Understanding Vulnerability Assessment · Using Vulnerability Scanners

06

System Hacking

TOPICS

- Understanding Password Attacks (Brute Force, Dictionary)
- Privilege Escalation Techniques
- Clearing Tracks and Covering Traces

07

Malware Threats

TOPICS

- Types of Malware (Viruses, Trojans, Ransomware)
- Evading Anti-Virus Mechanisms

08

Sniffing and Evasion

TOPICS

Packet Sniffing Concepts and Tools · Techniques to Evade IDS/IPS and Firewalls

09

Social Engineering

TOPICS

Understanding Social Engineering Techniques · Real-Life Social Engineering Scenarios

10

Session Hijacking

TOPICS

Session Hijacking Concepts · Tools and Techniques for Session Hijacking

11

Hacking Web Applications

TOPICS

- OWASP Top 10 Vulnerabilities
- Exploiting SQL Injection and Cross-Site Scripting (XSS)
- Tools for Web Application Testing

12

Hacking Wireless Networks

TOPICS

- Wireless Encryption Protocols (WEP, WPA, WPA2)
- Cracking Wireless Networks

13

Hacking Mobile Platforms and IoT

TOPICS

Security Challenges in IoT Devices · **Mobile Security:**
Tools and Techniques

14

Cloud Security

TOPICS

Cloud Vulnerabilities and Threats · Hacking and
Securing Cloud Platforms

15

Ethical Hacking Process Wrap-Up

TOPICS

- Reporting and Documentation in Ethical Hacking
- Remediation Techniques and Recommendations
- Ethics and Legal Considerations in Ethical Hacking

WHAT IS INCLUDED

Everything You Need to Succeed

- Koenig course material for every module
- Delivery by certified instructors and subject matter experts
- Hands-on exercises throughout the course
- Course completion certificate from Koenig

Who We Are

Established in 1993, Koenig Solutions is a globally recognised training provider with 35+ technology partnerships, 5,000+ training programmes and a network of certified instructors and subject matter experts, supporting individuals and enterprise teams worldwide.

FLEXIBLE DELIVERY

Learn the Way That Suits You

Classroom Training

Live Online Classes (ILO)

Fly-Me-A-Trainer (FMAT)

Flexi (Self-Paced)

1-on-1 Training

Ready to Get Started?

Talk to a learning advisor about schedules, group training and customised delivery.

Visit koenig-solutions.com

✉ info@koenig-solutions.com