

Ethical Hacking and Penetration Testing

Learn the essential skills for ethical hacking and penetration testing.

Category: Cyber Security · Duration: 4 days

WHO IT IS FOR

- Security engineers and system administrators
- Teams that want hands-on practice on real scenarios

In this comprehensive course, participants will gain the knowledge and skills necessary to conduct ethical hacking and penetration testing. Through interactive lectures, hands-on exercises, and real-world scenarios, learners will understand the methodologies, tools, and techniques used for identifying vulnerabilities and strengthening cybersecurity defenses. Prerequisites include basic understanding of networking and computer systems.

Prerequisites

Basic understanding of networking and computer systems

Syllabus

- Introduction to Ethical Hacking
- Reconnaissance and Footprinting
- Scanning and Enumeration
- System Hacking and Trojans
- Sniffing and Spoofing
- Wireless Network Attacks
- Web Application Security
- Database Penetration Testing
- Network and Firewall Bypassing
- Malware Analysis and Reverse Engineering
- Social Engineering and Phishing
- Wireless Security Auditing
- Exploitation and Post-Exploitation Techniques
- Mitigation and Countermeasures

- Secure Configuration and Hardening
- Mobile Application Security
- Cloud Security and Virtualization
- IoT Security
- Legal and Ethical Considerations
- Hands-on Assessments and Labs