ETHICAL HACKING



3 Hours per Day | **Total Duration: 30 Hours (10 Days)**

DAY 1 — Introduction to Ethical Hacking & Cybersecurity

- Introduction to Cybersecurity
- Ethical Hacking Concepts & Objectives
- Types of Hackers & Cyber Threats
- Cybersecurity Attack Lifecycle
- Common Security Vulnerabilities
- Ethical & Legal Considerations
- **Practical:** Setting Up a Safe Security Lab

DAY 2 — Networking & Security Fundamentals

- Networking Fundamentals
- IP Addressing & Subnetting
- TCP/IP, Ports & Protocols
- DNS, HTTP/HTTPS & Network Services
- Firewalls & Network Security
- Introduction to Network Scanning
- **Practical:** Network Discovery in a Controlled Lab

DAY 3 — Information Gathering & Reconnaissance

- Reconnaissance Concepts
- Passive & Active Information Gathering
- OSINT Fundamentals
- Domain & DNS Information
- Identifying Hosts, Services & Technologies
- Vulnerability Information Gathering
- **Practical**: Reconnaissance Using Authorized Lab Targets

DAY 4 — Vulnerability Assessment

- Vulnerabilities & Security Weaknesses
- Vulnerability Assessment Process
- Common Vulnerability Types
- Introduction to CVE & CVSS
- Security Scanning Concepts
- Risk Identification & Reporting
- **Practical:** Vulnerability Scanning in a Lab Environment

DAY 5 — Web Application Security

- Web Application Security Fundamentals
- HTTP Requests & Responses
- Authentication & Session Management
- OWASP Top 10 Overview
- Common Web Vulnerabilities
- Input Validation & Secure Coding
- **Practical:** Web Security Testing on a Legal Lab

DAY 6 — Password & Authentication Security

- Authentication & Authorization
- Password Security Concepts
- Password Hashing & Salting
- Multi-Factor Authentication
- Account Security & Access Controls
- Credential Security Best Practices
- **Practical:** Password Security Analysis in a Lab

DAY 7 — Network & System Security Testing

- Network Security Assessment
- Host & Service Enumeration
- System Hardening Concepts
- Wireless Security Fundamentals
- Endpoint Security
- Security Logs & Monitoring
- **Practical:** Security Assessment of an Authorized Lab System

DAY 8 — Social Engineering & Security Awareness

- Social Engineering Concepts
- Phishing & Common Attack Methods
- Email & Communication Security
- Human Factors in Cybersecurity
- Security Awareness & Prevention
- Incident Reporting
- **Practical:** Simulated Phishing Awareness Exercise

DAY 9 — Penetration Testing & Incident Response

Penetration Testing Methodology

- Planning & Scope Definition
- Vulnerability Validation
- Evidence Collection & Documentation
- Incident Detection & Response
- Remediation & Security Recommendations
- **Practical:** Controlled Penetration Testing Workflow

DAY 10 — Ethical Hacking Project & Security Assessment

- Complete Ethical Hacking Methodology
- Reconnaissance & Vulnerability Assessment
- Security Testing & Risk Analysis
- Documentation & Professional Reporting
- Remediation & Security Best Practices
- Cybersecurity Career & Certification Overview
- **Final Project:** Authorized Security Assessment & Report