

MASTER ETHICAL HACKING THROUGH HANDS-ON LABS AND REAL-WORLD CYBERSECURITY TRAINING

Overview

This intensive 6-month program is designed for aspiring cybersecurity professionals who want to build a successful career in ethical hacking, penetration testing, and information security.

Course Modules

Phase 1 – Cybersecurity Fundamentals (3 Months)

➔ Module 1: Introduction to Cybersecurity

- * Cybersecurity fundamentals
- * CIA Triad
- * Types of cyber threats
- * Real-world cyberattack case studies

➔ Module 2: Cybersecurity Concepts & Attack Vectors

- * Security terminologies
- * Common attack techniques
- * Vulnerabilities and exploits
- * Introduction to penetration testing

➔ Module 3: OSINT & Google Dorking

- * Google Dorking
- * Open-Source Intelligence (OSINT)
- * Ethical information gathering
- * Windows, Kali Linux & Parrot OS introduction

Course Modules

Phase 1 – Cybersecurity Fundamentals (3 Months)

➔ Module 4: Network Security Fundamentals

- * Networking concepts
- * TCP/IP & OSI Model
- * Linux essentials
- * Network scanning techniques
- * Nmap, Recon-ng & Shodan

➔ Module 5: Information Gathering & Reconnaissance

- * Passive & active reconnaissance
- * DNS enumeration
- * WHOIS lookup
- * Port scanning
- * Banner grabbing
- * Professional reconnaissance tools

➔ Module 6: Web & Application Security

- * OWASP Top 10
- * SQL Injection
- * Cross-Site Scripting (XSS)
- * CSRF, LFI, RFI & RCE
- * Burp Suite
- * OWASP ZAP
- * Nessus & OpenVAS

Course Modules

Phase 2 – Advanced Ethical Hacking (3 Months)

➔ Module 7: System Security & Exploitation

- * Windows & Linux exploitation
- * SMB, FTP & SSH attacks
- * Metasploit Framework
- * Privilege escalation
- * Misconfiguration exploitation

Course Modules

➔ Module 8: Wireless Security

- * Wireless attacks
- * Wi-Fi penetration testing
- * Packet sniffing
- * Password cracking
- * Aircrack-ng
- * Wireshark
- * Hashcat
- * John the Ripper

➔ Module 9: Cyber Hygiene & Security Awareness

- * Secure browsing
- * Email security
- * Social engineering
- * Remote work security
- * Cloud security best practices

➔ Module 10: Practical Labs & AI in Cybersecurity

- * Hands-on penetration testing
- * Vulnerable machines
- * Windows & Linux labs
- * Web application testing
- * AI-powered cybersecurity tools

➔ Module 11: Ethical Hacking Career Development

- * Ethical hacking methodologies
- * Bug bounty programs
- * HackerOne & Bugcrowd
- * Cybersecurity portfolio development
- * Freelancing opportunities
- * Career guidance

Learning Outcomes

➔ Upon successful completion of this program, you will be able to:

- * Understand cybersecurity principles and security frameworks.
- * Perform vulnerability assessments and penetration testing.
- * Conduct professional reconnaissance and information gathering.
- * Identify and exploit common web application vulnerabilities.
- * Secure Windows, Linux, and network infrastructures.
- * Perform wireless security assessments.
- * Use professional ethical hacking tools including:
 - * Kali Linux
 - * Nmap
 - * Burp Suite
 - * Metasploit
 - * Wireshark
 - * Nessus
 - * OpenVAS
 - * OWASP ZAP
 - * Sqlmap
 - * Shodan
- * Apply AI tools in cybersecurity workflows.
- * Build a professional cybersecurity portfolio.
- * Prepare for bug bounty programs, freelancing, and entry-level cybersecurity careers.

Who Should Enroll?

➔ This program is ideal for:

- * Students
- * Fresh Graduates
- * IT Professionals
- * Network Engineers
- * System Administrators
- * Security Enthusiasts
- * Anyone looking to build a career in Ethical Hacking and Cybersecurity

PROGRAM DETAIL

DURATION: 6 MONTHS

FREQUENCY: 2 DAYS PER WEEK

STRUCTURE: 2 PHASES (BASIC & ADVANCED)

TRAINING FORMAT: 90% HANDS-ON LABS | 10% THEORY

FEE STRUCTURE:

PKR 10,000 PER MONTH

