ETHICAL HACKING

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
MONTH 01

Module 01: Introduction to Cybersecurity

- Fundamentals and importance of cybersecurity
- CIA Triad: Confidentiality, Integrity, Availability
- Cyber threats: Malware, phishing, ransomware, and DoS
- Case studies: Equifax, WannaCry, and Uber breach

Module 02: Cybersecurity Terminologies & Attack Vectors

- Key concepts: Vulnerabilities, exploits, threat actors, and patching
- Attack techniques: Brute force, Man-in-the-Middle, and SQL injection
- Introduction to penetration testing

MONTH 02

Module 03: OSINT & Advanced Google Search Techniques

- Google Dorking and advanced search techniques
- Open-Source Intelligence (OSINT)
- Introduction to Windows, Kali Linux, and Parrot OS

Module 04: Network Security Basics

- Networking fundamentals: IP, DNS, TCP/IP, and OSI Model
- Network scanning: SYN, ACK, and UDP scans
- Virtual lab setup using VirtualBox/VMware
- Linux commands and Bash scripting
- Tools: Nmap, Recon-ng, and Shodan

Module 05: Information Gathering & Reconnaissance

- Passive and active reconnaissance
- Port scanning and network reconnaissance
- WHOIS lookup, DNS, and subdomain enumeration
- Banner grabbing and service enumeration
- Tools: theHarvester, Maltego, Recon-ng, and Shodan

MONTH 03

Module 06: Web & Application Security

- OWASP Top 10 vulnerabilities
- File upload vulnerabilities
- SQL Injection, XSS, CSRF, LFI, RFI, and RCE
- Vulnerability scanning: Nessus, OpenVAS, and OWASP ZAP
- Tools: Burp Suite, OWASP ZAP, and SQL map
- Real-world web exploitation case studies

MONTH 04

Module 07: System Security & Misconfiguration

- Security assessment of SMB, FTP, SSH, and other services
- Identifying and testing misconfigured services
- Hands-on exploitation in controlled labs using Metasploit
- Privilege escalation: Windows permissions, registry weaknesses, and scheduled tasks

Module 08: Wireless Security & Password Auditing

- Wireless security fundamentals
- Common threats: Evil Twin, packet sniffing, deauthentication, and jamming
- Password auditing with Hashcat and John the Ripper
- Tools: Aircrack-ng, Fluxion, and Wireshark
- Real-world wireless attack case studies

MONTH 05

Module 09: Cyber Hygiene & Personal Security

- Cybersecurity best practices for individuals
- Safe browsing and email security
- Social engineering awareness
- Cyber hygiene for remote work
- Secure cloud usage: Google Drive, Dropbox, and other services

Module 10: Practical Labs & AI in Cybersecurity

- Vulnerable lab environments: Metasploitable and DVWA
- Windows Server security testing
- Web applications: OWASP Juice Shop and BodgeIt
- AI applications in cybersecurity

MONTH 06

Module 11: Ethical Aspects & Career Path

- Bug bounty fundamentals and ethical hacking guidelines
- Responsible vulnerability disclosure
- Building a cybersecurity portfolio
- Freelancing opportunities in cybersecurity
- Bug bounty platforms: HackerOne and Bugcrowd

PROGRAM DETAILS

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

