Ethical Hacking Bootcamp Syllabus

Basics (3 Months)

The first bootcamp session will cover the basics and will run for 3 months. It will be intense and will lay the foundation for success in ethical hacking. This foundation and the basics of all topics will be perfect for anyone interested in pursuing a career in ethical hacking or cybersecurity.

Module 1: Linux

- Introduction
- Installing Kali Linux
- Linux Structure
- Linux Terminal
- Basic Linux Commands
- Manipulating Texts
- Manage and Analyze Network

- Software Management
- File & Directory Permissions
- Process Management
- User Environment Variables
- Compressing and Archiving

Module 2: Introducing to Networking

- Networking Models
- OSI Model
- TCP/IP Model
- IP Addressing & Subnetting
- Ports and Protocols
- DNS (Domain Name System)
- Network Devices & Topologies
- VPN & Proxies

Module 3: Cryptography Basics

- Introduction to Cryptography
- Encoding and Decoding
- Encrypting and Decrypting
- Symmetric vs. asymmetric encryption
- Hashing algorithms

Module 4: Introduction to Information Security & Penetration Testing Process

- Overview of Information Security Domains
- Introduction to Penetration Testing
- Bug Bounty Programs: Overview and Scope
- Standards and Frameworks (ISO 27001, PCI DSS, HIPAA)
- Legal and Ethical Considerations

- Types of Penetration Tests
- **Penetration Testing Process:**
    - Pre-engagement Activities
    - Reconnaissance
    - Vulnerability Assessment
    - Exploitation
    - Post-exploitation
    - Reporting and Documentation

Module 5: Web Enumeration and Footprinting

- OSINT and Google Dorking
- Web Fuzzing Tools
- Banner Grabbing
- Whois and Dig Commands
- Zone Transfer Attacks
- Subdomain and Vhost Enumeration
- External Web Reconnaissance

Module 6: Web Hacking (Basics)

- Overview of Burpsuite
- SQL Injection
- Cross-Site Scripting (XSS)
- Open Redirect
- File Inclusion Vulnerabilities
- Command Injection
- Cross-Site Request Forgery (CSRF)

Advanced (3 Months)

The second bootcamp session will cover advanced ethical hacking concepts, exposing individuals to in-depth topics and providing a strong grasp of web and network testing. Only those who have completed the basics bootcamp will be eligible to participate in the advanced session. If you haven't completed the basics bootcamp, you may be required to take a short test to assess your fundamental knowledge.

Module 7: Enumeration and Service Footprinting

- Using Nmap for Enumeration
- Service Enumeration & Exploitation (SMB, FTP, NFS, SMNP, SMTP, RDP, etc.)

Module 8: Web Hacking (Advanced)

- XML External Entity (XXE) Attacks
- File Upload Vulnerabilities
- IDOR
- Access Control Weaknesses
- JWT Attacks
- API Enumeration & Attacks

Module 9: Vulnerability Research

- Researching Potential Vulnerabilities
- Finding Relevant CVEs for Real-world Scenarios

Module 10: Vulnerability Assessment Tools

- Nessus Overview
- OpenVAS Overview

Module 11: Exploitation & Lateral Movement Techniques

- Shell Types (Reverse Shell & Bind Shell)
- Metasploit Framework
- Port Forwarding Techniques (SSH, Chisel, etc...)

- File Transfer Methods
- Credentials Harvesting in Windows/Linux

Module 12: Privilege Escalation

- Windows Privilege Escalation
- Linux Privilege Escalation

Module 13: Reporting and Documentation

- Penetration Testing Reports
- Bug Bounty Reports
- Tools for Reporting