HappyMongo
Strengthen your roots

# EMPOWER YOUR DEFENSE: WE HACK TO PROTECT

## UNAUTHORISED@CCESS

Hands-on Programme in

## Cybersecurity: Advance Penetration Testing

4 Months | Live Online Training

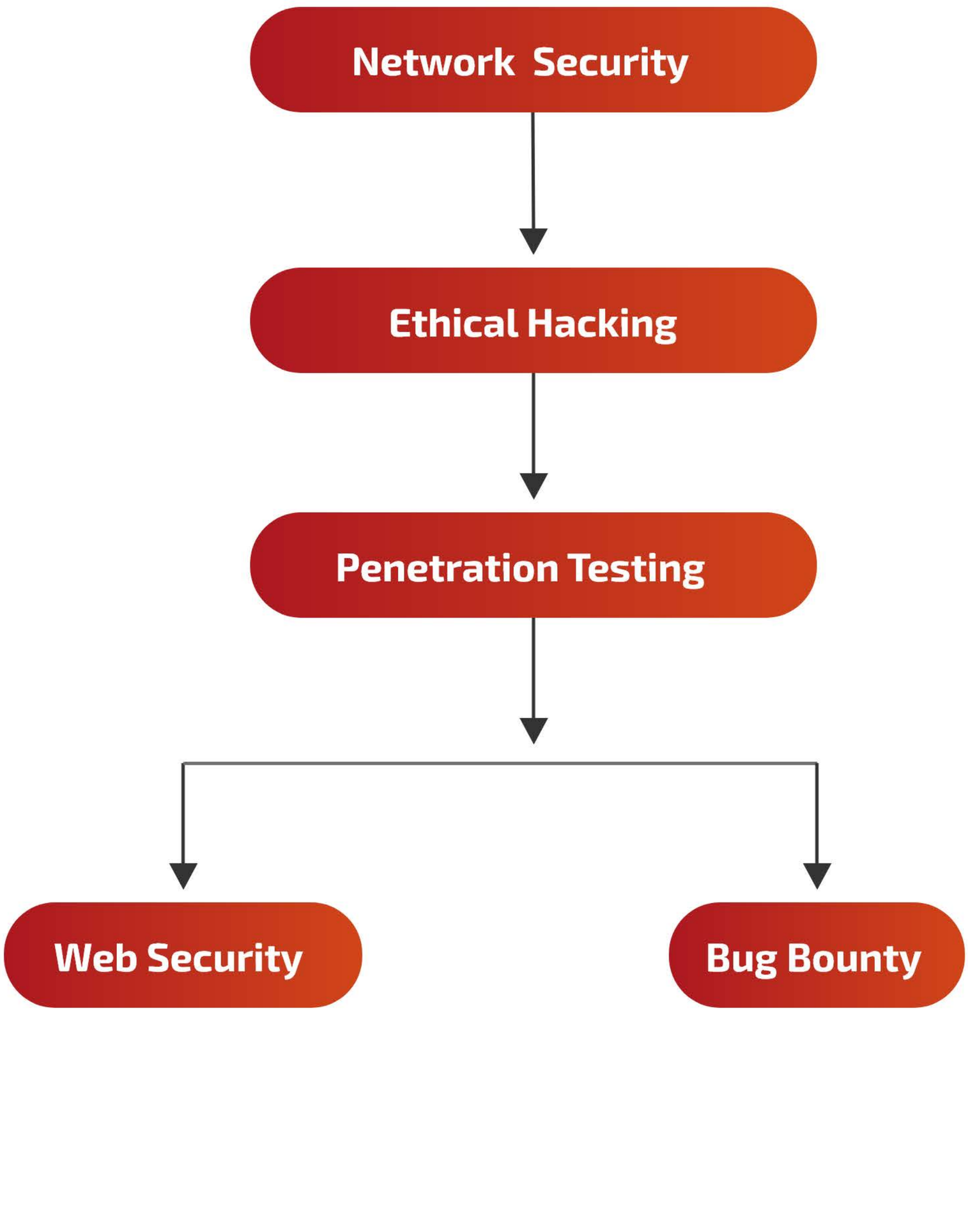
Introducing Our Comprehensive Cybersecurity Professional Training Programs with Internship, Placement, and Simulation Bot.

Are you ready to embark on a rewarding and promising career in the dynamic field of Cybersecurity? Look no further! Our cutting-edge Cybersecurity Professional Training Programs.

## ABOUT THE PROGRAM

Our Cybersecurity Professional Training Programs are meticulously designed by industry experts to equip you with Hands-On Penetration Testing and Cybersecurity Skills enabling you to land in a high paying Cybersecurity job. With an emphasis on practical learning, we aim to empower you with real-world expertise that sets you apart in the job market.

## LEARNING PATH



# CORE DETAILED CURRICULUM

## FOUNDATION (5 Hours)

### Networking

- Introduction to Networks
- OSI Model Explained
- TCP/IP Protocol Suite
- Network Devices: Routers, Switches, Firewalls
- Network Security Fundamentals (firewalls, access control)
- Hands-on Lab (using a network simulator to explore basic network concepts)

### Operating Systems

- Introduction to Operating Systems (Linux)
- File Systems and Directory Structures
- User Accounts and Permissions
- Basic Linux Commands for Navigation and File Manipulation
- Hands-on Lab (practicing basic commands in a Linux VMware)

### Web Technologies

- Introduction to Web Applications
- Hypertext Mark-up Language (HTML)
- Cascading Style Sheets (CSS)
- Introduction to JavaScript

### Databases

- Introduction to Databases
- SQL vs. NoSQL Databases (basic concepts)

### Servers

- Introduction to Servers
- Types of Servers (Web Servers, Database Servers)
- Server Operating Systems
- Basic Server Administration Tasks (starting/stopping services, user management)

# INTERMEDIATE (20 Hours)

## Module 1: Ethical Hacking

- Course Overview
- Type of Hacker
- Difference Between Hacker & Ethical Hacker
- Penetration Testing & Its Types
- Methodologies of Penetration Testing

## Module 2: Setup Installation

- VMware Installation
- Network Configuration
- Kali Linux, Windows 7, Ubuntu

## Module 3: Footprinting

- Footprinting Through Search Engine
  - Google - Shodan - Search Engine Colossus
  - Duckduckgo - Censys.Io - Wayback Machine
- Footprinting Through Social Engineering
  - Fake Email ID - Iplogger - Fake WhatsApp
  - Fake Name Generator - Fake Mobile No
- Footprinting Through Social Networking Sites
  - Facebook - LinkedIn - Twitter
  - Pipl - Namecheck.Com
- Whois Footprinting
- DNS Footprinting
- Network Footprinting
  - Top 10 Networking Command
- Website Foorprinting
  - Foca - Httrack - Web Data Extractor
- Competitive Intelligence
  - Changedetecton.Com - Website Watcher
- Email Footprinting
  - Gmail Last Login - Email Tracker
  - Boomerang for Gmail - Track Email Activity

## Module 4: Networks & Scanning Networks

- Find Connected PC in Network
  - Netdiscover - Fing
  - Angry IP Scanner - Fast Resolver
- Basic Nmap Scan
  - Host Scan - TCP Scan - Stealth Scan
  - UDP Scan - OS Scan -Version Scan
  - Aggressive Scan - Output Scan
- Ngrok
- TOR Network Browser
- Online Web Proxies

## Module 5: Enumeration

- Network Resources
- Network Shares
- Routing Tables
- Users & Group
- Machine Names
- Application & Banners
- Currport
- Netstat - Whoami
- SMBMAP - Showmount
- FTP Anonymous

## Module 6: System Hacking

- Introduction to Metasploit Framework
  - Auxiliary - Exploit - Payloads
  - Evasion - Encoders
- Metasploit Hacking
  - Msfvenom Windows - Msfvenom Linux
  - Msfvenom Android
- Introduction to Meterpreter Commands
  - Background - Cat - Upload - Webcam
  - Download - Screenshot - Run Vnc
  - Hash dump. - Idle Time - Keystrokes
- Dumping and Cracking SAM Hashes to Extract
- Auditing LOG
- Eventvwr
- Windows 10 Password Hack
  - Stealing Passwords from Different locations
- Password in Cleartext
  - Wce - Mimikatz
- Password Dumping from Web Browser

## Module 7: Malware Threats

- Introduction to Malware and Its Types
  - Trojan - Rootkits - Virus
  - Worms - Adware - Spyware
  - Ransomware Explanation
- Trojan
  - Njrat
- Virus Maker
  - Batch File Virus - JPS Virus Maker
- Virutotal.Com
- Process Explorer
- Binder and Cryptor
  - Shelter - Thefatrat
- Spyware
  - Family Keylogger

## Module 8: Sniffing

- Introduction Sniffing Its Types
  - Active Sniffing & Passive Sniffing
  - Spoofing - Man In the Middle Attack
  - ARP Poisoning - DNS Poisoning
- Password Sniff
  - HTTP Password Capture
  - Telnet Password Capture
  - FTP Password Capture
- Xerosploit
- XARP Detect Sniffing

## Module 9: Social Engineering

- Introduction to Social Engineering & Its Types
  - Phishing - Vishing
  - Pretexting - Baiting
- Payload Attack
- HTA Attack
- Credential Harvester Attack
- Shellter

## Module 10: Denial of Service

- Introduction of DOS Attack & Its Types
- Distributed Denial of Service DDOS
- Bonet
- DOS Attack
  - LOIC - HOIC - Hping

## Module 11: Webservers Hacking (Metasploitable2)

- Web Services & Major Services
  - Apache2 - FTP - Telnet
  - SSH - MySQL - PHP - PhpMyAdmin
- Webserver Reconnaissance
  - Netcraft - Whatweb
- Webserver Vulnerability Scanning
  - FTP Password - SSH Password
- Password Brute force (Metasploit)

## Module 12: Evading IDS, Firewalls & Honey Pots

- Introduction To IDS, IPS Firewall , DMZ & Honeypots
- Honey Bot, Kfsensor
- Windows Advanced Firewall Rules
- Evading Firewall
  - Firewall Enable/Disable
  - Metasploit HTTPS Payload
  - Migrate Process - Bypass UAC

## Module 13: Maintaining Access

- Persistence & Its importance
- Persistence_Exe
- Persistence through Registery

## Module 14: Cryptography & Steganography

- Basic Concept of Steganography
  - Audio Steganography - Video Steganography
  - Image Steganography - Spam mimic.
- Introduction to Cryptography
  - Classic Cryptography - Modern Cryptography
- Modern Cryptography
  - AES Encryption - PGP Key Generation
- Basic Concept of Hashing
- Hash Calculator

## ADVANCE (40 Hours)

### Advance Penetration Testing / Bug Bounty

- Introduction to Web Pentesting and types of pentesting
- Intro to Bug Bounty
- Bug Bounty Methodology
- Web Server Configuration
- Web Application Lab Setup
- Burpsuite Pro with Licence
- Burpsuite Installation and proxy setup
- HTTP Headers and their importance
- HTTP methods Exploitation
- Broken Authentication
- Broken Access Control
- Information Disclosure
- Information Leakage in Debug Pages
- CSP Bypass
- Source code Disclosure via Backup Files
- Session Hijacking
- Understanding of Error Messages
- Cookie Manipulation
- Accessing Private User Data
- Understanding of Request Parameter
- Privilege Escalation
- Directory Traversal
- Bypassing Absolute Path Restriction
- Bypassing Hard-coded Extensions
- Bypassing Filtering
- Bypassing Advance Filtering
- Learning LFI with automation
- LFI to Remote code Execution
- LFI to Apache log poisoning
- SSH log poisoning
- RFI and its exploitation
- OS Command Injection
- Blind OS command Injection with time delays
- Understanding OS with out-of-band exfiltration
- Different types of File Upload
- HTML Injections and their types
- Creating different types of web payloads
- Open Redirect Attack
- Understanding of Regex
- SQL Injection and its types
- Cross Site Scripting and its types
- CSRF
- Violation of secure designed principles
- SSRF
- VAPT report writing & samples walkthrough