

# ETHICAL HACKING

---

3 Month | Total Practical

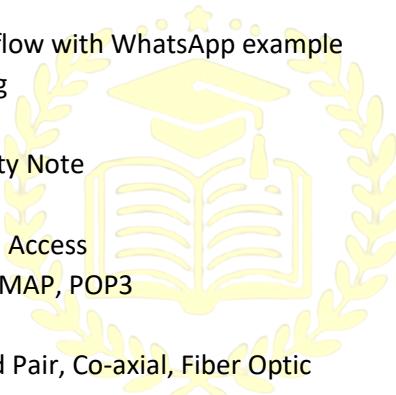
Master the Art of Ethical Hacking  
Through Hands-On Learning

# Course Index of Ethical Hacking & Cyber Security

---

## MODULE 01 – THE FUNDAMENTALS

- What is Hacking?
- What is Ethical Hacking?
- Types of Hackers – White Hat, Black Hat, Grey Hat
- What is Operating System (OS)?
- What is Software? o System Software o Application Software o Utility Software
- What is Network?
- IP Address – Local IP & Public IP
- ISP – Internet Service Provider
- MAC Address & NIC
- HUB, SWITCH, ROUTER – Basics & Difference
- Ports & Common Port Numbers
- Protocols – FTP, HTTP etc.
- TCP/IP – TCP vs UDP
- OSI 7-Layer Model – Full flow with WhatsApp example
- DNS – Concept & Working
- HTTP vs HTTPS
- DHCP – Concept & Security Note
- SSH – Secure Shell
- Telnet – Insecure Remote Access
- Email Protocols – SMTP, IMAP, POP3
- Server & Client Concepts
- Network Cables – Twisted Pair, Co-axial, Fiber Optic
- Submarine Cable – Undersea Internet Backbone



## MODULE 02 – IDENTITY CHANGING

- Change IP Address using BlackHat Methods (theory only)
- Change IP using Web Proxy
- Change IP using VPN (concept only – “Don’t use”)
- Change MAC Address – Tool: TMAC
- Change OS & Browser Identity – Tool: User Agent Switcher (Firefox)

## MODULE 03 – BASIC HACKING USING CMD

- Finding Website IP

- Finding Local System & Router IP
- Finding Computer Name and Username
- Listing All Users on System
- Changing User/Admin Password
- Finding Saved WiFi Passwords
- Enabling Windows Firewall
- Disabling Windows Firewall (lab only)

## MODULE 04 – SOCIAL MEDIA HACKING & SECURITY

- Keystroke Capturing
- Phishing – Fake Login Pages
- Stealing Saved Login Credentials from Browsers
- Spyware on Devices
- Guessing Simple Passwords
- Security Tips

## MODULE 05 – WINDOWS HACKING & SECURITY

- What is Password?
- LM & NTLM – Windows Password Storage
- Password Hashes – Concept
- SAM – Security Accounts Manager File
- Bypassing / Resetting Windows Password – Concept & Tools
- Windows Backdoor – Concept of Login Bypass
- Hardening Windows
  - Strong Passwords
  - BitLocker
  - Lock Screen
  - Disable USB Boot / BIOS Password
  - Updates & Antivirus



## MODULE 06 – WINDOWS SYSTEM MONITORING

- What is Employee Monitoring?
- Why Monitor Employee Activity?
- Legal Side – Policies & User Awareness
- Monitoring Company Computers from One System

## MODULE 07 – ANDROID PHONE HACKING & SECURITY

- What is Android OS?

- What is Spyware on Mobile?
- Why Android is Hackable
- Why iOS is Not Easily Hackable – Closed System, Strict Store, No Side-loading,

## MODULE 08 – VIRUS CREATION & PREVENTION

- What is Malware?
- What is Virus?
- Educational Virus Examples (Batch Scripts)
  - System Crasher
  - Data Hider
  - Data Wiper
  - WinLocker
- Creating EXE from BAT – Bat to Exe Converter
- Trojan & RAT – Concept and Backdoor Access
- Virus Detection & Protection
  - Online Scanners – VirusTotal
  - Windows Defender – Built-in Antivirus

## MODULE 09 – WEB ATTACKS & PREVENTION



- What is Website?
- What is Domain?
- What is Hosting?
- Types of Hosting – Shared, VPS, Dedicated, Cloud
- What is Web Server?
- Types of Web Server – Apache, Nginx, IIS, LiteSpeed
- DOS Attack – Concept
- DDOS Attack – Concept & Botnets
- Demo Tool – LOIC (Lab Only)
- Identifying DDOS Protection – Cloudflare & others
- Cyber Law about DOS/DDOS – IT Act & Section 66F (overview)
- Security from Web Attacks
- DDOS Protection Service – Cloudflare

## MODULE 10 – DATA SECURITY

### System Security

- Lock Keyboard & Mouse
- Disable USB Ports

- Turn ON Windows Firewall
- Turn ON Windows Defender – Virus & Threat Protection Data Security
- Hide Drives – Disk Management
- Data Backup Policy – System, Cloud, External
- Data Recovery from Windows – Disk Drill
- Data Recovery from Mobile – Disk Digger Internet Security
- Block Websites – Simple Website Blocker
- Block Porn Websites – Tueagles

## MODULE 11 – WIFI HACKING & SECURITY

- Introduction to WiFi
- SSID – WiFi Name
- WiFi Security Modes – WEP, WPA, WPA2, WPA3
- Why Properly Secured WiFi is Hard to Hack
- Finding Saved WiFi Passwords
- Finding Who is Connected
- Killing Internet of Selected Users
- Finding Router IP
- Accessing Router Panel
- Changing WiFi Name (SSID) & Password – Router Settings



## MODULE 12 – DEEP WEB: THE HIDDEN INTERNET

- Surface Web – Normal Indexed Internet
- Deep Web – Non-indexed, Login-based Content
- Dark Web – Hidden Anonymous Networks (.onion)
- TOR Network – Concept & Working
- TOR Browser – Anonymous Access
- TOR Search Engine – Ahmia
- Useful / Legal Deep Web Services
- Harmful / Illegal Dark Web Areas
- Payment Methods – Bitcoin & Other Crypto
- Precautions for Deep Web Use – Legal & Security Warnings

## MODULE 13 – CYBER CRIME & CYBER LAW

- What is Cyber Law?
- IT Act 2000 – Basic Cyber Law Framework
- IT Amendment Act 2008 – Updated Cyber Provisions

- Cyber Law Sections & Punishments
  - Section 66C – Hacking / Account Misuse / Virus Spreading
  - Section 66B – Buying/Selling Stolen Digital Devices
  - Section 65 – Software Source Code Theft
  - Section 66D – Fake Profiles & Online Cheating
  - Section 66A – Stalking & Cyber Bullying
  - Section 66F – Cyber Terrorism (Life Imprisonment)

## MODULE 14 – Introduction to Cyber Security

- Need of cyber security, types of attacks
- CIA Triad, basic security controls
- Types of hackers & their motives

## MODULE 15 – Mastering Kali Linux

- Installing & updating Kali
- Basic Linux commands & permissions
- Overview of key tools (Nmap, Wireshark, Burp Suit ,Metasploit)



## MODULE 16 – Penetration Testing – 5 Phases

- Information Gathering (Recon)
- Scanning & Enumeration
- Gaining Access
- Maintaining Access
- Clearing Tracks

## MODULE 17 – Penetration Testing With Metasploit

- Metasploit interface & modules
- Exploits, payloads, sessions
- Basic post-exploitation & reporting

## MODULE 18 – Web Pentesting Fundamentals (Manual & Automated)

- Manual: HTTP basics, XSS, SQL Injection, CSRF, authentication issues
- Automated: ZAP / scanners, reading reports, validating findings