



# **Course: Ethical Hacking Courses**

Duration: 70 Hrs (Changeable) | Fees: Individual / Batch

Since 2007, Nestsoft TechnoMaster has been providing training, internships, and services in IT technologies, both online and offline, with the expertise of over 250 industry experts. We have delivered internships, training, and seminars to more than 50,000 students, resulting in numerous success stories. We offer 100% placement support through JobsNEAR.in

### **Our Courses/Internship**

- Python/Django Fullstack
- Artificial Intelligence
- Machine Learning
- Data Science
- Software Testing (All)
- Wordpress, Woocommerce
- Digital Marketing, SEO
- Php/MySQL, Laravel
- Flutter, Android, IOS
- Asp.net MVC
- Web Design, Javascript
- Angular JS, React JS
- CCNA, MCSA, CCNP
- AWS, GCP, Azure
- Odoo, SalesForce, Sap
- Microsoft Excel
- Ethical Hacking



Syllabus on the Next Page ..



Our Head Office: Nestsoft TechnoMaster, Infopark, Cochin - 42, Kerala, India



**\*\*** +91 9895490866

**\*\*** +91 8301010866



ioin@nestsoft.com







#### **MODULE 1**

- \* Ethical hacking
- \* Types of hackers and terminologies
- \* Cybercrime and types
- What is ethical hacking
- Why ethical hacking
- \* The legality of ethical hacking

#### **MODULE 2**

- \* Footprinting, concepts
- \* Techniques for web footprinting
- Techniques for email footprint
- Techniques for competitive intelligence
- Techniques in WHO footprint
- Techniques in-network footprinting
- Footprinting tools
- Network footprinting
- \* DNS Footprinting
- \* Website footprinting

#### MODULE 3

- \* Network scanning
- \* Techniques to check for live system
- Techniques to check for open ports
- \* Scanning techniques

Our Head Office: Nestsoft TechnoMaster, Infopark, Cochin - 42, Kerala, India



**\*\*** +91 9895490866





join@nestsoft.com







- \* Banner grabbing
- \* Scanning and pen testing
- \* Host discovery
- \* Scanning beyond IDS and firewall

#### **MODULE 4**

- \* Enumeration
- Introduction to Enumeration
- \* Enumeration Types
- \* Enumerating User Accounts.
- \* Enumeration Countermeasures.

#### **MODULE 5**

- \* System Hacking
- \* Password Cracking
- \* Types of Password Attacks
- \* Keyloggers
- Spyware
- \* Detecting RootKits
- \* Covering Tracks

#### **MODULE 6**

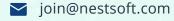
- \* Trojans and Backdoors
- \* What is a Trojan?
- \* Trojan Attacks and Indications.

Our Head Office: Nestsoft TechnoMaster, Infopark, Cochin - 42, Kerala, India



**\*** +91 9895490866











- \* How to deploy a Trojan
- \* Types of Trojans
- \* Anti-Trojans Software
- \* Penetration Testing

#### **MODULE 7**

- Viruses and Worms
- Introduction to Viruses
- Stages of a Virus Life.
- \* Working with viruses.
- \* Writing a Simple Virus Program
- \* Computer Worms
- \* Malware Analysis Procedure.
- \* Anti-Virus Tools.

#### **MODULE 8**

- \* Sniffing techniques
- **\*** MAC attacks
- \* DHCP attacks
- \* ARP poisoning
- Spoofing attacks
- \* DNS poisoning
- \* Sniffing pen testing
- \* Social engineering concepts, techniques

Our Head Office: Nestsoft TechnoMaster, Infopark, Cochin - 42, Kerala, India



**\*\*** +91 9895490866





join@nestsoft.com







\* Networking sites

#### **MODULE 9**

- \* Social Engineering.
- \* What is Social Engineering?
- \* Phases of a Social Engineering Attack
- Social Engineering through Impersonation on Social Networking Sites.
- \* Identify Theft.
- \* How to Steal Identity?
- \* Social Engineering Pen Testing.

#### **MODULE 10**

- \* Denial Of Service.
- \* What is a DoS and DDoS Attack?
- \* How do DoS Attacks work?
- \* Symptoms of a DoS Attack
- \* DoS Attack Techniques.
- \* DDoS Case Study.
- \* Protection Tools.

#### **MODULE 11**

- \* Session Hijacking
- \* What is Session hijacking?
- \* Hijacking Techniques.
- \* Brute Forcing.

Our Head Office: Nestsoft TechnoMaster, Infopark, Cochin - 42, Kerala, India



**\*\*** +91 9895490866

**\*\*** +91 8301010866









- \* Spoofing vs. Hijacking.
- \* Types of Session Hijacking
- \* Session Hijacking in OSI Model.
- TCP/IP Hijacking.
- # Hijacking Tools.
- IPSec Architecture.
- \* Penetration Testing.

#### **MODULE 12**

- \* Web service hacking
- \* Web service concepts, attacks, methodology, tools
- \* Web service pen testing
- \* Web application
- \* Web application concepts, threats, methodology, tools

#### **MODULE 13**

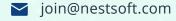
- \* Hacking Web Applications.
- \* Introduction to Web Applications.
- \* How do Web Applications work?
- \* Web Applications Architecture.
- \* Unvalidated Input
- \* Parameter / Form Tampering.
- \* Injection Flaws.
- \* Hidden and Manipulated Attacks.

Our Head Office: Nestsoft TechnoMaster, Infopark, Cochin - 42, Kerala, India



**\*\*** +91 9895490866











- \* Cross-Site Scripting
- Hacking Methodology
- \* Web Application Security Tools.
- Web Application Firewalls.
- \* Web Application Pen Testing.

#### **MODULE 14**

- \* SQL Injection.
- \* Introduction to SQL Injection.
- Threats of SQL Injection Attacks.
- \* SQL Injection Detection.
- \* Simple / Union Injection Attacks.
- \* What is a Blind SQL Injection?
- \* SQL Injection Tools.

#### **MODULE 15**

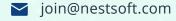
- \* Hacking Wireless Networks.
- \* Introduction to Wireless Networks.
- Wi-Fi Authentication Modes.
- \* WEP Encryption
- \* WPA / WPA2 Encryption.
- \* Wireless Threats.
- Wireless Hacking Methodology.
- \* Wireless Hacking Tools.

Our Head Office: Nestsoft TechnoMaster, Infopark, Cochin - 42, Kerala, India



**\*\*** +91 9895490866











- \* Bluetooth Hacking.
- \* How to defend against Wireless Attacks.
- \* Wireless Penetration Testing Framework.

#### **MODULE 16**

- \* Evading IDS, Firewalls, and Honeypots.
- \* Intrusion Detection Systems (IDS).
- \* Ways to detect an Intrusion.
- \* Types of Intrusion Detection Systems.
- \* Types of Firewalls.
- \* Firewall Identification Techniques.
- \* Honeypot.
- \* Types of honeypot.
- \* Evading IDS.
- Evading Firewalls.
- \* Detecting Honeypots.
- \* Firewall Evading Tools.

#### **MODULE 17**

- \* Buffer Overflow.
- \* Buffer Overflows.
- \* Stack-Based / Heap-Based Overflows.
- Stack Operations.
- \* Buffer overflow Steps.

Our Head Office: Nestsoft TechnoMaster, Infopark, Cochin - 42, Kerala, India



**\*\*** +91 9895490866

**\*\*** +91 8301010866









- \* Smashing the Stack.
- \* Examples of Buffer Overflow Attacks.
- \* BoF Detection Tools.

#### **MODULE 18**

- \* Cryptography.
- \* Introduction to Cryptography
- Ciphers.
- \* Advanced Encryption Standard (AES)
- \* RC4, RC5, Rc6 Algorithms.
- \* RSA (Rivest Shamir Adleman).
- \* Message Digest 5 ( MD5 ).
- \* Secure Hashing Algorithm (SHA).
- \* Cryptography Tools.
- Public Key Infrastructure (PKI).
- Digital Signatures.
- SSS (Secure Socket Layer).
- \* Disk Encryption.
- \* Cryptography Attacks.

#### **MODULE 19**

- \* Penetration Testing.
- \* Penetration Testing (PT).
- \* Security Assessments.

Our Head Office: Nestsoft TechnoMaster, Infopark, Cochin - 42, Kerala, India



**\*\*** +91 9895490866











- \* Risk Management.
- \* Automated Testing.
- \* Manual Testing.
- \* Enumerating Devices.
- \* Denial of Service Emulation.
- Hacker Shield.
- \* Pentest using various Devices.

#### **MODULE 20**

- \* Hacking Mobile Platforms.
- \* Understanding Mobile Platforms Terminology
- \* Android / IOS / Windows Phones.

(Click on Course for more details)

**Course: Ethical Hacking Courses** 

Duration: 70 Hrs (Changeable) | Fees: Individual / Batch

### - Thank You -

N.B:This syllabus is not final and can be customized as per requirements / updates.

Our Head Office: Nestsoft TechnoMaster, Infopark, Cochin - 42, Kerala, India

**\*\*** +91 9895490866

**\*\*** +91 8301010866

join@nestsoft.com

