Cyber Security & Ethical Hacking

Course Duration: 4 Months

Eligibility:

Open to all (Basic Computer & Networking knowledge recommended)

Outcome:

Students will be capable of performing security audits, identifying vulnerabilities, and understanding the defensive/offensive side of digital security.

Program Details:

The program has been divided into 4 modules Consequently; there will be examinations at every end of module. For beginners it is first important to build command over programming concepts. on this course our goal is to help you to be confident with the coding fundamentals.

Module 1: Foundations of Cyber Security & Networking

- **Cyber Security Landscape:** The CIA Triad, types of hackers, and the 2026 threat environment (Deepfakes, AI Phishing).
- **Networking for Defenders:** OSI & TCP/IP models, IP addressing (IPv4/IPv6), DNS, and DHCP.
- **OS Mastery (Windows & Linux):** Linux File System, CLI commands, and User Access Control (UAC).
- **Virtualization:** Setting up a secure sandbox lab using VirtualBox or VMware.
- **Practical Lab:** Network reconnaissance and port scanning using **Nmap**.

Module 2: Network Defense & Cryptography

- **Defensive Infrastructure:** Types of Firewalls, IDS (Intrusion Detection), and IPS (Intrusion Prevention).
- **Cryptography:** Symmetric vs. Asymmetric encryption, Hashing (SHA-256), and Digital Certificates (SSL/TLS).

Email: info@trayoinfotech.com
Contact: 7838032551

- **Zero Trust Architecture:** The "Never Trust, Always Verify" principle and Multi-Factor Authentication (MFA).
- **Traffic Analysis:** Monitoring and filtering live data packets.
- **Practical Lab:** Analyzing network traffic for suspicious patterns using **Wireshark**.

Module 3: Offensive Security (Ethical Hacking)

- **The Hacking Lifecycle:** Reconnaissance, Scanning, Gaining Access, and Maintaining Access.
- **Web Application Security:** OWASP Top 10 vulnerabilities, SQL Injection, and Cross-Site Scripting (XSS).
- **Social Engineering:** Phishing techniques, Quishing (QR Code Phishing), and Baiting.
- **Wireless Security:** Understanding Wi-Fi encryption (WPA2/WPA3) and common vulnerabilities.
- **Practical Lab:** Simulated penetration testing in a controlled lab using **Metasploit** and **Burp Suite**.

Module 4: Incident Response, Forensics & AI Security

- **Digital Forensics:** Evidence collection, disk imaging, and timeline reconstruction.
- **AI in Cybersecurity:** How AI is used for automated threat detection and how hackers use AI for automated attacks.
- **Governance & Ethics:** Indian IT Act, GDPR basics, and ISO 27001 standards.
- **Career Readiness:** Mock interviews, building a security portfolio on GitHub, and resume building.
- **Final Project:** Conducting a full Vulnerability Assessment & Penetration Test (VAPT) on a mock company network.