DIY
DATA IN YOURSELF

Foundations of Cybersecurity & Networking

Module 1: Introduction to Cybersecurity

- Importance & Scope of Cybersecurity
- Common Threats: Malware, Phishing, Ransomware
- Types of Hackers (White Hat, Black Hat, Gray Hat)
- CIA Triad: Confidentiality, Integrity, Availability
- Real-World Use Cases of Cybersecurity

Module 2: Networking Essentials for Security

- OSI & TCP/IP Models
- IP Addressing, Subnetting & Ports
- Protocols: HTTP, HTTPS, DNS, FTP, SSH, TCP/UDP
- VPNs, Firewalls, and Proxies
- Packet Sniffing & Monitoring using **Wireshark**

Module 3: Ethical Hacking & Penetration Testing (Beginner)

- Footprinting & Reconnaissance
- Network Scanning Tools: **Nmap**
- Vulnerability Assessment & Exploitation
- Introduction to **Kali Linux** and **Metasploit**
- Brute Force & Password Cracking (Demo-Based)

Module 4: Web Application Security

- OWASP Top 10 Vulnerabilities
- Hands-on: SQL Injection, Cross-Site Scripting (XSS)
- Web App Testing using **Burp Suite (Community Edition)**
- Secure Development Practices
- Basic Security Headers & Cookies

Module 5: System & Cloud Security

- Linux/Windows Security Basics
- Permissions, User Roles, Password Policies
- Introduction to Cloud Security (AWS, Azure Concepts)
- Best Practices for Cloud & Data Protection

Module 6: SOC & Incident Response

- What is a Security Operations Center (SOC)?
- Role of SOC Analyst
- SIEM Tools Overview (like Splunk – demo access)
- Incident Response Lifecycle
- Logs, Alerts & Monitoring

Career Preparation

- Resume Building (Cybersecurity-Focused)
- Interview Preparation & Mock Sessions
- Freelancing & Remote Job Opportunities
- Final Assessment + Mini Project