TARCiN

Cybersecurity

Course Modules & Topics

🔐 Module 1: Introduction to Cybersecurity

- Importance of Cybersecurity
- Types of Cyber Attacks (Malware, Phishing, DoS, Ransomware)
- CIA Triad: Confidentiality, Integrity, Availability
- Cybersecurity Roles & Responsibilities

🌐 Module 2: Network Security

- OSI & TCP/IP Models
- Firewalls, IDS/IPS
- Secure Network Architecture
- VPNs and Tunneling Protocols

💻 Module 3: System & Endpoint Security

- OS Hardening (Windows/Linux)
- Antivirus & Antimalware Techniques
- Patch Management
- Device Control & Endpoint Detection Response (EDR)

🛡️ Module 4: Cryptography

- Symmetric vs Asymmetric Encryption
- Hashing Algorithms (MD5, SHA)
- Digital Signatures & Certificates
- SSL/TLS & Public Key Infrastructure (PKI)

👤 Module 5: Identity & Access Management (IAM)

- Authentication vs Authorization
- Multi-Factor Authentication (MFA)
- Role-Based Access Control (RBAC)
- Single Sign-On (SSO)

▯ Module 6: Threats, Vulnerabilities & Attacks

- OWASP Top 10
- Social Engineering
- SQL Injection, XSS, CSRF
- Zero-Day Exploits

🔍 Module 7: Security Tools & Techniques

- Kali Linux Basics
- Nmap, Wireshark, Metasploit
- Password Cracking (John the Ripper, Hashcat)
- Vulnerability Scanning (OpenVAS, Nessus)

⚖ Module 8: Cyber Laws, Compliance & Ethics

- GDPR, HIPAA, PCI-DSS Overview
- Incident Response Plan
- Ethical Hacking & Legal Boundaries
- Cyber Forensics Basics

▯ Module 9: Capstone Project

- Choose One:
    - Penetration Test of a Web App
    - Secure Network Setup Design
    - Malware Analysis Report
- Final Presentation