Cyber Security Course Modules

Course Overview

The Cyber Security course is designed to provide a foundational understanding of information security principles, practices, and technologies. This course explores the threats and vulnerabilities faced by modern digital systems and teaches strategies to protect networks, data, and systems from cyber attacks. Learners will gain insights into critical areas such as network security, cryptography, ethical hacking, and risk management.

Through theoretical lessons and hands-on exercises, students will develop practical skills to detect, analyze, and respond to security breaches. The course also covers legal and ethical issues related to cyber security, preparing students for roles in IT security and cyber defence.

Learning Outcomes:

- Identify and mitigate various types of cyber threats.
- Analyze and design secure network architectures.
- Apply cryptographic techniques for data protection.
- Conduct vulnerability assessments and penetration tests.
- Develop and implement security policies and procedures.

Prerequisites:

1. Basic proficiency in mathematics and familiarity with spreadsheets.

2. No prior programming experience required.

Course Modules

Module	Title	Topics
1.	**Introduction to Cyber Security**	➢ Basics of information security ➢ Cyber threats & attack vectors ➢ CIA triad (Confidentiality, Integrity, Availability) ➢ Security policies and standards
2.	**Network Security**	➢ TCP/IP, ports, and protocols ➢ Firewalls, IDS/IPS, VPNs, ➢ Packet sniffing and network scanning ➢ Secure network architecture

3.	**System & Application Security**	➢ Operating system hardening (Windows/Linux) ➢ Secure software development lifecycle (SDLC) ➢ Web application vulnerabilities (OWASP Top 10) ➢ Patch management
4.	**Threat Intelligence & Incident Response**	➢ Threat hunting & indicators of compromise (IoCs) ➢ Digital forensics basics ➢ Incident response lifecycle (Preparation to Lessons Learned) ➢ SIEM tools (e.g., Splunk, IBM QRadar)
5.	**Ethical Hacking & Penetration Testing**	➢ Reconnaissance, scanning, exploitation ➢ Tools: Metasploit, Nmap, Burp Suite ➢ Vulnerability assessment ➢ Social engineering
6.	**Cryptography**	➢ Symmetric vs Asymmetric encryption ➢ Hashing, digital signatures ➢ SSL/TLS, HTTPS ➢ Key management
7.	**Identity & Access Management (IAM)**	➢ Authentication methods (MFA, biometrics) ➢ Authorization models (RBAC, ABAC) ➢ SSO, LDAP, Active Directory ➢ Identity federation
8.	**Cyber Law, Compliance & Governance**	➢ GDPR, HIPAA, ISO 27001, NIST ➢ Risk assessment & management ➢ Business continuity & disaster recovery (BC/DR) ➢ Security auditing and reporting
9.	**Cloud Security**	➢ Shared responsibility model ➢ Cloud platforms (AWS, Azure, GCP) security ➢ Identity & access in cloud ➢ Cloud-native security tools
10.	**Emerging Technologies & Trends**	➢ AI/ML in cybersecurity ➢ Blockchain security ➢ IoT & mobile security ➢ Zero Trust Architecture