Cyber Security Course Curriculum for Students

Pre-Requisites:

- Basic understanding of Information Technology/Computer Science fundamentals.

---

1. **Fundamentals of Computer Networks (6 Hours)**
   Basic concepts of computer networks, network models, OSI, TCP/IP, Layered architecture, Client Server architecture, Peer-to-Peer Architecture.
2. **Application Layer (12 Hours)**
   Working of WWW, E-Mail, TELNET, FTP, Secure Shell, DNS, BitTorrrent, and some other applications. Architecture of E-Mail system, TELNET, DNS and WWW. Security Vulnerabilities in these systems.
   Cyber Security perspectives corresponding to above mentioned topics.
3. **Network Layer (10 Hours)**
   Basic services used and provided by Physical Layer, Data link layer, network layer, transport layer, application layer.
   Types of devices constituting a network. Concept of Internet Service Providers (ISPs) and overall conceptual view of the Internet. Routing fundamentals.
   Different types of networks such as LAN, WAN, VPN, etc.
   Cyber Security perspectives corresponding to above mentioned topics.
4. **Essential for understanding cyber security (7 Hours)**
   Cyber Security Concepts, essential terminologies, open source tools.
   Understanding meaning and differences in various terms such as Breaches, Threats, Attacks, Exploits, and others.
5. **Protocols and Cyber Security Vulnerabilities (14 Hours)**
   Hyper Text Transfer Protocol (HTTP) and corresponding cyber security vulneribilities.
   Various security attacks related to HTTP.
   TCP, UDP and corresponding security vulneribilities.
   MAC, IPv4, IPv6. How to do subnetting, benefits of DHCP, and other related topics.
6. **Information Security and Cryptography (12 Hours)**
   Various concepts of Cryptography, Symmetric key and Asymmetric key Cryptography.
   Digital Signatures, Applications of Cryptography. OpenSSL, Hash Values Calculations MD5, SHA, Steganography. Use of open source tools.
7. **Firewalls (10 Hours)**
   Definition, Types of Firewalls, VPN Security, Security Protocols: - security at the Application Layer- PGP and S/MIME, Security at Transport Layer- SSL and TLS, Security at Network Layer-IPSec.

8. System and Server Security (15 Hours)

DOS/ DDOS attacks. Introduction to System Security, Server Security, OS Security, Physical Security, Network packet Sniffing, Network Design Simulation. Various concepts of system and server security, intrusion detection and prevention, various tools and experiments, Internet and cloud security, cyber security vulnerabilities, safeguards, various tools. Open Source Tools

9. Malware Concepts (15 Hours)

Basics of Malware and its types (Virus, Worms, Trojans, Rootkits, Robots, Adware's, Spywares, Ransom wares, Zombies etc), Malware Analysis, anti-virus protection.

Malware Analysis using machine learning, Understanding malware analysis with the help of various source tools.

10. Web Services and Cyber Laws (15 Hours)

Basics of Web Services, SOAP, REST, Cyber laws and forensics, cyber security regulations, cyber forensics basics, some other useful tools. Secure software development, Role of design patterns, Software intensive systems.

11. **Cyber Security and Machine Learning (20 Hours)**

ML terminology: Regression, clustering, classification, association rule of learning, dimensionality reduction, generative models, supervised, unsupervised, semi-supervised, Reinforcement learning, dimensionality reduction, generative models

(a) Cyber security Tasks and Machine Learning: prediction; prevention; detection; response; monitoring. (network (network traffic analysis and intrusion detection); endpoint (anti-malware); application (WAF or database firewalls); user (UBA); process (anti-fraud).

(b) Security Check: in transit in real time; at rest; historically; etc.

(c) Examples: Network Protection (regression, classification, clustering etc); Endpoint Protection: classification for malware, spyware and ransomware; clustering for malware protection on secure email gateways (e.g., to separate legal file attachments from outliers); Application Security; User Behavior; Process Behavior

12. Cyber Security and Recent Technologies (14 Hours)

Security aspects in IoT, Cloud Computing and Image/video data. Biometrics, Mobile Computing and Hardening on android and ios, IOT Security, Android Malware Analysis, Experimentation using open source tools.