School of Cybersecurity

Duration: 12 Weeks

Mode: Hybrid (Physical & Virtual Options)

Certification: Completion Certificate + Real-World Project Management Simulation

Week 1-2: Introduction to Cybersecurity Cybersecurity Basics:

Understanding the importance of cybersecurity in today's digital world

Types of cyber threats: Malware, Phishing, Social Engineering, Ransomware

Cybersecurity Goals: Confidentiality, Integrity, Availability (CIA Triad)

Understanding Cyber Attacks: Anatomy of a cyber-attack and various types (DDoS, Man-in-the-Middle, SQL Injection)

Week 3-4: Computer Networks and Security Fundamentals Networking Fundamentals:

Basics of computer networks: IP addresses, MAC addresses, OSI model, and TCP/IP

Network security concepts: VLANs, DMZs, and Network Address Translation (NAT)

Security Layers: Physical Security: Securing devices physically

Network Security: Use of firewalls, IDS/IPS

Week 5-6: Encryption and Cryptography

Encryption Basics

Symmetric vs. Asymmetric Encryption, Hashing, and Public Key Infrastructure (PKI)

Cryptographic Tools:

Using tools like OpenSSL for encrypting and decrypting data

Real-World Use Cases: How encryption is used to secure communication (e.g., SSL/TLS)

Week 7-8: Identity and Access Management (IAM)

Authentication vs Authorization:

Understanding the difference between authentication and authorization

Types of Authentications: Passwords, Multi-Factor Authentication (MFA), Biometrics Access Control

Role-Based Access Control (RBAC) Least Privilege Principle to minimize access

Week 9-10: Ethical Hacking and Penetration Testing

Ethical Hacking Introduction:

Ethics of hacking: White hat, Black hat, and Grey hat hackers

Introduction to the phases of penetration testing: Reconnaissance, Scanning, Exploitation, Reporting

Hands-On Practice: Setting up a virtual lab using VirtualBox and Kali Linux Scanning Networks with tools like Nmap Implementing a simple project with dynamic data

Week 11: Incident Response and Security Monitoring

Incident Response Lifecycle:

Preparation, Detection, Containment, Eradication, Recovery, Lessons Learned Monitoring and Detection:

Using Security Information and Event Management (SIEM) systems Understanding log analysis, event correlationCreating a multi-page React application (e.g., a blog app)

Week 12: Capstone Project and Career Preparation Capstone Project:

Conduct a Penetration Test on a simulated network

Document vulnerabilities found, propose security measures

Career Development:

Building a cybersecurity portfolio: Documenting tools and methodologies

Certification Pathways: Introduction to certifications like CompTIA Security+, CEH (Certified Ethical Hacker)

Freelancing Opportunities: Securing remote gigs in cybersecurity

Maximizing the 12-Week Training:

Hands-On Labs: Emphasis on building a home lab environment to practice security skills.
Industry Tools: Exposure to industry-standard tools like Wireshark, Metasploit, Nessus, and Splunk.

Group Projects: Collaborative assignments to simulate real-world cybersecurity team scenarios.

Simulated Attacks: Experience running and defending against simulated attacks to reinforce learning.

The School of Cybersecurity will not only teach students the technical aspects of securing networks but also how to think critically like a hacker, understand evolving threats, and stay ahead in a rapidly changing field. Graduates will be prepared for entry-level roles in cybersecurity, ethical hacking, or network security administration