Cyber Security Pathway 

The guide to understanding cyber security pathway

Step 1

Introduction to Cybersecurity

Objective : Understand the fundamentals of cybersecurity and its importance.

Topics Covered :

- Overview of Cybersecurity Concepts
- Common Threats and Attack Vectors
- Introduction to Security Standards and Best Practices
- Basic Cryptography Principles

Step 2

Foundations of Networking and Operating Systems

Objective : Gain knowledge of networking and operating systems to understand cybersecurity concepts.

Topics Covered :

- Networking Fundamentals (TCP/IP, DNS, DHCP)
- Operating System Basics (Windows, Linux, macOS)
- Network Protocols and Services
- Security Configuration and Hardening Techniques

Step 3

Introduction to Cyber Threats and Defense Mechanisms

Objective : Learn about different types of cyber threats and defense strategies.

Topics Covered :

- Malware Types and Behavior Analysis
- Social Engineering and Phishing Attacks

- Intrusion Detection and Prevention Systems (IDS/IPS)
- Security Controls and Countermeasures

Step 4

Secure Coding and Application Security

Objective : Understand secure coding principles and techniques to develop secure software.

Topics Covered :

- Secure Software Development Lifecycle (SDLC)
- Common Web Application Vulnerabilities (SQL Injection, XSS)
- Secure Coding Practices in Various Programming Languages
- Web Application Firewall (WAF) Implementation

Step 5

Cryptography and Data Protection

Objective : Explore cryptographic techniques for data protection and secure communication.

Topics Covered :

- Encryption Algorithms and Methods
- Public Key Infrastructure (PKI)
- Digital Signatures and Certificates
- Secure Communication Protocols (SSL/TLS)

Step 6

Network Security and Penetration Testing

Objective : Learn about network security measures and techniques for ethical hacking.

Topics Covered :

- Network Security Protocols (VPN, SSH)
- Penetration Testing Methodologies
- Vulnerability Assessment and Management
- Incident Response and Forensics Basics

Step 7

Cloud Security and Virtualization

Objective : Understand security challenges and solutions in cloud computing and virtual environments.

Topics Covered :

- Cloud Computing Models (IaaS, PaaS, SaaS)
- Cloud Security Best Practices
- Virtualization Technologies and Security Considerations
- Identity and Access Management (IAM) in Cloud Environments

Step 8

Cybersecurity Career Preparation and Advancement

Objective : Prepare for a career in cybersecurity and explore opportunities for professional growth.

Topics Covered :

- Building a Cybersecurity Portfolio (showcasing projects and certifications)
- Resume Writing and Interview Preparation
- Certifications (CISSP, CEH, CompTIA Security+)
- Continuing Education and Professional Networking