" EXIN Cyber and IT Security Foundation"

Course Introduction

1. TCP/IP Networking

1.1 Nodes, Connectivity, and TCP/IP Addressing

- Definition of Nodes
- Node Connection Methods
- TCP/IP Addressing Concepts
    - IPv4 Addressing
    - IPv6 Addressing

1.2 OSI Model, TCP/IP Model, and Network Protocols

- OSI Model: Layers and Functions
- TCP/IP Model: Layers and Functions
- Core Network Protocols and Their Role in OSI and TCP/IP Models

---

2. Computer Systems

2.1 Computer Architecture and Operating Systems

- Components of a Computer System
- How Operating Systems Work
- Overview of Major Operating Systems

2.2 Computer System Vulnerabilities

- Common Types of System Vulnerabilities

2.3 Computer System Security Measures

- Technical and Logical Security Measures for Computer Systems

---

3. Applications and Databases

3.1 Application Development

- Systems Development Life Cycle (SDLC) Phases
- SDLC Models: Advantages and Disadvantages
- Integrating Security into the SDLC

3.2 Databases

- Database Models
- Database Functionality
- Database Management Systems (DBMS)

3.3 Application and Database Security

- Common Security Issues in Applications and Databases
- Security Countermeasures and Best Practices

---

4. Cryptography

4.1 Encryption Methodologies and Standards

- Symmetric vs. Asymmetric Encryption
- Encryption Algorithms and Standards

4.2 Digital Signatures and Hashing

- Digital Signatures: Authenticity and Non-Repudiation
- Hashing and Data Integrity
- Common Hashing Standards

4.3 Public Key Infrastructure (PKI)

- PKI Components, Roles, and Processes
- Digital Certificates and Their Use Cases

4.4 Secure Communication Protocols

- SSL/TLS: Technology and Use Cases
- IPsec: Technology and Use Cases

5. Identity and Access Management (IAM)

5.1 Identification and Authentication

- Identification vs. Authentication
- Authentication Technologies and Two-Factor Authentication
- Biometrics and Use Cases
- Single Sign-On (SSO): Concepts and Types
- Password Management and Best Practices

5.2 Authorization

- Authorization Principles:
  - Need to Know
  - Least Privilege
  - Separation of Duties (SoD)
- Authorization Models: RBAC and ABAC
- OpenID Connect and OAuth

---

6. Cloud Computing

6.1 Cloud Characteristics and Deployment Models

- Public Cloud
- Private Cloud
- Hybrid Cloud

6.2 Cloud Service Models and Risks

- SaaS, PaaS, IaaS
- SECaaS and IDaaS
- Cloud Computing Risks

---

7. Exploiting Vulnerabilities

7.1 Attack Categories and Threat Types

- Major Cybercrime Attack Categories

7.2 Threat Actors and Tools

- Types of Threat Actors:
  - Black Hat, White Hat, Grey Hat
  - Script Kiddies
  - Hacktivists
- Common Cybercrime Tools
- Steps Used to Exploit Vulnerabilities