1. Introduction

- **Introduction to Cybersecurity**
  - Definition and importance of cybersecurity
  - Evolution of cybersecurity practices
  - Overview of key cybersecurity domains

2. Information Security

- **Intellectual Property**
  - Definition and types of intellectual property
  - Protecting intellectual property in cyberspace
- **CAI (Confidentiality, Availability, Integrity)**
  - Key principles of information security
  - Real-world examples of CAI implementation
- **Aspects of Security**
  - Physical security
  - Personnel security
  - Information and operational security

3. Cyber Threats and Vulnerabilities

- **Types of Threats**
  - Malware, phishing, and ransomware
  - Insider threats and social engineering
- **System Vulnerabilities**
  - Common vulnerabilities in hardware and software
  - Patch management and vulnerability life cycle

4. Security Policy

- **Types & Importance of Security Policy**
  - Organizational policies and compliance standards
  - Writing effective security policies
- **Bulls Eye Model**
  - Layers of protection in the Bulls Eye framework
- **User Account Controls**

    - Importance of account management and access controls
- **Local Rights and Privileges**
    - Managing user permissions on systems

5. Networking

- **Network Fundamentals**
    - Basic concepts: IP, MAC, and subnets
    - Devices: routers, switches, and firewalls
- **Network Topologies**
    - Types of topologies: star, mesh, bus, etc.
    - Use cases and pros/cons
- **Network Analysis**
    - Tools and techniques for monitoring traffic
    - Packet analysis basics
- **Network Attacks**
    - Types of attacks: DoS, MITM, etc.
    - Case studies of major network breaches
- **Secure Network Design**
    - Best practices for designing secure networks
    - Network segmentation and zoning
- **Network Protocols**
    - Common protocols: TCP/IP, DNS, HTTP, etc.
    - Protocol vulnerabilities and mitigation

6. OS Security

- **Windows OS**
    - Hardening techniques
    - Built-in security tools
- **Linux OS**
    - Security configurations
    - Key tools and utilities

7. Cryptography

- **Digital Certificates**
    - Role in authentication and encryption

    - Certificate authorities and PKI
- **Digital Signatures**
    - Ensuring data authenticity and integrity
- **Steganography**
    - Hiding information in digital media
- **Network Security (IDS, IPS)**
    - Intrusion Detection Systems (IDS)
    - Intrusion Prevention Systems (IPS)

8. Penetration Testing (Hands-On)

- **Types of Pentests**
    - Black box, white box, and gray box
- **Pentest Phases**
    - Planning, scanning, exploitation, and reporting
- **Footprinting**
    - Information gathering techniques
- **Enumeration**
    - Identifying network resources
- **Fingerprinting**
    - Recognizing OS and service details
- **Network Sniffing**
    - Capturing and analyzing network traffic
- **Wireless Networks**
    - Identifying and exploiting Wi-Fi vulnerabilities
- **Privilege Escalation**
    - Techniques to gain higher system access

9. Internet Security

- **Types of Internet Security**
    - Securing browsers, email, and online activities
    - Threats like spam, scams, and phishing

10. Vulnerability Assessment

- **Types of Vulnerability Assessment**
    - Automated tools vs. manual assessments

- **Risk Assessment**
  - Identifying and prioritizing risks
- **Administrative Controls**
  - Policies and procedures to manage risks

11. Incident Response

- **Incident Response Process**
  - Preparation, detection, containment, eradication, recovery, and lessons learned
  - Building and training an incident response team