1. Cybersecurity Fundamentals

- **CIA Triad (Confidentiality, Integrity, Availability)**
- **Common Threats & Attacks**: Phishing, Malware, Ransomware, DDoS, MITM attacks
- **Security Measures**: Firewalls, Encryption, Multi-Factor Authentication (MFA)
- **Basic Incident Response Process**: Identification, Containment, Eradication, Recovery

2. Networking Basics

- **OSI & TCP/IP Models** (Layers and their functions)
- **IP Addressing, Subnetting, and DNS**
- **Common Protocols**: HTTP/HTTPS, FTP, SSH, SMTP, SNMP
- **Ports & Services**: Knowing common ports (e.g., 80 for HTTP, 443 for HTTPS, 22 for SSH)

3. Security Tools & Technologies

- **SIEM (Security Information and Event Management)** Basics
- **Antivirus, IDS/IPS (Intrusion Detection/Prevention Systems)**
- **Packet Analysis Tools**: Wireshark, TCPDump
- **Vulnerability Scanners**: Nessus, OpenVAS
- **Penetration Testing Basics**: Metasploit, Burp Suite

4. System Security & Threat Management

- **Windows & Linux Security**: User privileges, File permissions, Secure configurations
- **Log Analysis & Threat Detection**
- **Incident Response Basics**: How to handle a cyber attack
- **Common Security Frameworks**: NIST, ISO 27001, OWASP Top 10

5. Industry Awareness

- Stay updated with **cybersecurity trends & threats** (Follow blogs like KrebsOnSecurity, Threatpost)
- Basic understanding of **cloud security** (AWS, Azure Security best practices)
- Familiarity with **Zero Trust Security Model**