Cybersecurity Course Content

Session 1: Networking Basics (Security Perspective)

- What is Networking & Why It Matters for Cybersecurity
- Types of Networks: LAN, WAN, MAN, WLAN
- Network Topologies (Star, Bus, Ring, Mesh)
- OSI Model vs TCP/IP Model (Security relevance)
- Data Flow & Packet Structure (Headers, Payloads)

Session 2: Network Devices & Protocols

- Network Devices:
  - Hub vs Switch vs Router
  - Firewall, IDS, IPS (intro)
- Common Protocols:
  - TCP vs UDP
  - IP, ICMP, ARP
- Understanding Ports & Services
- Practical Discussion: How attackers see networks

Core Networking Protocols & Risks

Session 3: Essential Network Services

- DNS – Working & Attacks (DNS Spoofing, Poisoning)
- DHCP – Leasing Process & Rogue DHCP Attacks
- HTTP vs HTTPS – Security Differences
- FTP, SFTP, SSH – Secure vs Insecure Protocols
- Common Ports & Their Security Implications

Session 4: IP Addressing & Network Design

- IPv4 & IPv6 Basics
- Public vs Private IPs
- Subnetting & CIDR (Security view, not math-heavy)
- NAT & PAT
- Network Segmentation & Security Zones (DMZ concept)

Network Security Fundamentals

Session 5: Network Threats & Attack Techniques

- Network-based Attacks:
  - Sniffing & Spoofing
  - Man-in-the-Middle (MITM)
  - ARP Poisoning
  - DoS & DDoS
- Insider vs External Attacks
- Real-world breach examples (network layer focus)

Session 6: Firewalls, IDS & IPS

- Firewall Types:
  - Packet Filtering
  - Stateful
  - Application-aware
- IDS vs IPS (Signature vs Anomaly-based)
- Placement in Network Architecture
- Logging, Alerts & Incident Indicators

Secure Network Architecture & Monitoring

Session 7: Secure Network Design

- Defense in Depth
- Network Segmentation & VLANs
- Zero Trust Networking (ZTN) – Core Principles
- VPNs:
  - Site-to-Site
  - Remote Access
- Secure Wireless Networks (WPA2/WPA3, Evil Twin)

Session 8: Network Monitoring & Traffic Analysis

- Importance of Network Visibility
- Logs, NetFlow & Packet Capture Concepts
- Indicators of Compromise (IoCs) in Network Traffic
- Intro to SIEM (Network logs correlation)
- Case Study: Detecting Suspicious Network Behavior

Applied Network Security & Defense

Session 9: Network Hardening & Best Practices

- Secure Configuration of Network Devices
- Disabling Unused Ports & Services
- Patch Management (Network devices)
- Secure Remote Management (SSH, SNMPv3)
- Network Security Policies & Standards

Session 10: Incident Response & Capstone

- Network Security Incident Lifecycle
- Identifying, Containing & Eradicating Attacks
- Network Forensics – What to Capture & Preserve
- Mapping Attacks to Network Layers
- Capstone Exercise:
    - Analyze a Network Attack Scenario
    - Identify vulnerabilities & propose defenses