Network Security

1. Introduction to Network Security & Foundations

- Definition and importance of network security
- Security goals: Confidentiality, Integrity, Availability (CIA)
- Types of security threats, vulnerabilities, and countermeasures

2. Network Architectures, Protocols & TCP/IP Security

- Overview of network models, OSI and TCP/IP stacks
- Key protocols (IP, TCP, UDP, HTTP, DNS) and how they affect security
- Common protocol vulnerabilities and hardening

3. Security Policies, Procedures & Risk Management

- Importance of security policies and compliance
- Risk assessment frameworks
- Security governance basics

4. Firewalls & Perimeter Defense

- Types of firewalls: packet filtering, stateful, proxy
- Firewall rule creation and policy design
- Perimeter security strategies and firewall deployment

5. Virtual Private Networks (VPNs) & Secure Tunnels

- Concepts of VPNs for secure communication
- IPSec, SSL/TLS VPNs
- Site-to-site vs remote access VPNs

6. Intrusion Detection & Prevention Systems (IDS/IPS)

- **Differences between IDS and IPS**
- **Signature-based and anomaly-based systems**
- **Deployment strategies**

---

7. Network Monitoring & Logging

- **Network traffic analysis and log collection**
- **Tools for monitoring (e.g., Wireshark, SNMP)**
- **Detecting suspicious activity and alerts**

---

8. Wireless & Mobile Network Security

- **Securing Wi-Fi networks (WPA2/WPA3)**
- **Mobile device security concerns**
- **Wireless attacks and mitigation** OBJ

---

9. Cryptography & Secure Communications

- **Basics of cryptography: encryption, hashing**
- **Public Key Infrastructure (PKI)**
- **SSL/TLS and secure channel concepts**

---

10. Network Attacks & Threat Mitigation

- **Common network attacks: DoS/DDoS, spoofing, MITM**
- **Attack detection and response**
- **Patch and update management** OBJ

---

11. Secure Network Design & Protection Strategies

- **Network segmentation and DMZ**
- **Zero-trust architecture principles**
- **Defense-in-depth strategies** OBJ

---

12. Network Security Tools & Hands-on Labs

- **Practicals with firewalls, packet sniffers, vulnerability scanners**
- **Using tools like Nmap, Wireshark, Suricata** OBJ

---

13. Incident Response & Forensic Basics

- **Incident handling lifecycle**
- **Basic forensic evidence collection**
- **Post-incident analysis** OBJ

---

14. Projects, Case Studies & Emerging Trends

- **Real-world network security case studies**
- **Project work implementing network protection solutions**
- **Emerging topics: cloud security, adaptive firewalls, threat intel** OBJ