Fundamentals of Computer Network Security Specialization

Duration: 3 Days (8 Hours Per Day)

Module 1: Introduction to Computer Networks & Security

- What is a Computer Network?
- Types of Networks (LAN, WAN, Internet)
- Why Security is Important
- Common Threats & Attacks (in simple language)
- Real-life examples: hacking, phishing, ransomware

Module 2: Basics of Cryptography

- What is Encryption & Decryption?
- Symmetric vs Asymmetric Encryption
- Hashing & Digital Signatures
- Real-life application: Online Banking, WhatsApp encryption

Module 3: Authentication & Access Control

- What is Authentication? (Passwords, Biometrics, Tokens)
- Multi-Factor Authentication (MFA)
- Access Control: Who can access what?
- Role-Based Access in organizations

Module 4: Network Security Fundamentals

- Firewalls (basic explanation)
- VPNs (Virtual Private Networks)
- IDS vs IPS (Intrusion Detection & Prevention Systems)

- Securing Wi-Fi & Cloud Access

Module 5: Malware & Attack Techniques

- Types of Malware (Viruses, Worms, Trojans, Ransomware, Spyware)
- Social Engineering & Phishing
- Denial-of-Service (DoS/DDoS) Attacks
- Case studies: Famous cyberattacks

Module 6: Secure Communication & Protocols

- HTTPS vs HTTP
- SSL/TLS Basics
- Secure Email & Messaging
- VPN Protocols (IPSec, PPTP, L2TP explained simply)

Module 7: Security Policies & Best Practices

- Importance of Policies in Organizations
- Password Management
- Data Backup & Recovery
- Security Awareness Training for Employees

Module 8: Hands-On Practice & Case Studies

- Simulating a Phishing Attack & Prevention
- Configuring a Firewall (basic demo)
- Using Wireshark to see network packets
- Reviewing Real-world Case Studies (e.g., WannaCry, Equifax breach)

Module 9: Future of Network Security

- AI & Machine Learning in Cybersecurity
- Cloud Securit
- Zero Trust Architecture
- Careers in Cybersecurity