CYBERSECURITY

Week 1: Introduction to Cybersecurity

- What is cybersecurity?
- Importance of cybersecurity in today's digital world
- Types of threats: viruses, worms, ransomware, phishing, spyware
- Careers in cybersecurity (ethical hacker, SOC analyst, penetration tester, etc.)

Week 2: Fundamentals of Networking

- Basics of computer networks
- OSI and TCP/IP models
- IP addresses, ports, protocols (HTTP, HTTPS, FTP, SMTP, DNS)
- Firewalls, VPNs, and proxies
- How data travels over the internet

Week 3: Types of Cyber Threats

- Malware (viruses, worms, Trojans, ransomware, spyware, adware)
- Phishing and social engineering
- Denial of Service (DoS/DDoS) attacks
- Man-in-the-Middle (MITM) attacks
- Insider threats
- Case studies of real cyberattacks

Week 4: Cybersecurity Tools & Practices

- Antivirus and anti-malware tools
- Firewalls and intrusion detection/prevention systems (IDS/IPS)
- Password management and multi-factor authentication (MFA)
- VPNs and encryption
- Security Information and Event Management (SIEM) tools

Week 5: Cryptography Basics

- What is cryptography?
- Symmetric vs. asymmetric encryption
- Hashing (MD5, SHA)

- Public Key Infrastructure (PKI)
- Applications of cryptography (SSL, digital signatures, blockchain)

Week 6: Cybersecurity Policies & Best Practices

- Strong password policies
- Data protection and privacy laws (GDPR, HIPAA, NDPR)
- Security awareness training for individuals and organizations
- Importance of backups and disaster recovery
- Cyber hygiene practices for everyday users

Week 7: Ethical Hacking & Penetration Testing

- Difference between ethical hackers and malicious hackers
- Phases of penetration testing (Reconnaissance → Scanning → Exploitation → Reporting)
- Common tools: Nmap, Wireshark, Metasploit, Burp Suite
- Basics of vulnerability scanning

Week 8: Web & Application Security

- Common web vulnerabilities (OWASP Top 10: SQL Injection, XSS, CSRF, etc.)
- Securing web applications and APIs
- Secure software development practices
- Testing applications for vulnerabilities

Week 9: Cybersecurity in Cloud & Mobile

- Cloud security challenges (data breaches, misconfigurations)
- Shared responsibility model in cloud computing
- Mobile security risks (malicious apps, insecure Wi-Fi)
- Best practices for securing cloud and mobile devices

Week 10: Incident Response & Digital Forensics

- Steps in incident response (Preparation → Detection → Containment → Eradication → Recovery → Lessons learned)
- Basics of digital forensics
- Log analysis and evidence collection
- Reporting and documentation of incidents

Week 11: Emerging Trends in Cybersecurity

- Artificial Intelligence (AI) in cybersecurity
- Zero Trust security model
- Blockchain in security
- Internet of Things (IoT) security challenges
- Quantum computing and its impact on cybersecurity

Week 12: Final Project & Career Development

- Conduct a mini penetration test on a demo website/lab
- Write a cybersecurity policy for a small business
- Create awareness materials on phishing and social engineering
- Build a personal cybersecurity roadmap (certifications, skills, career paths)