Course content

This course provides a foundational understanding of network security, covering both the theoretical principles and practical techniques required to secure modern computer networks. The course focuses on essential concepts, technologies, and methods used in protecting data and network resources from various threats.

Key topics covered include:

1. Cryptography: Basics of encryption algorithms, public key infrastructure (PKI), digital signatures, and secure communication.
2. Network Security Protocols: Study of network security protocols such as SSL/TLS, IPSec, and VPN technologies.
3. Firewalls and Intrusion Detection Systems (IDS): Design, configuration, and use of firewalls, and intrusion detection/prevention systems to protect networks from attacks.
4. Malware and Attack Prevention: Analysis of common malware, viruses, and strategies for preventing cyberattacks, including phishing, DDoS, and ransomware.
5. Wireless and Mobile Network Security: Security challenges and solutions in wireless networks and mobile devices.
6. Security in Network Design and Management: Methods to design, implement, and manage secure network architectures.
7. Ethical Hacking and Penetration Testing: Introduction to penetration testing, vulnerability assessment, and ethical hacking techniques.

Course Objectives

Knowledge

1. Understand the fundamental principles of network security, including key technologies and protocols.
2. Learn about various types of network security threats and the corresponding defensive strategies.
3. Gain knowledge in cryptographic methods and their application in securing network communications.

Skills

1. Implement network security measures such as firewalls, IDS, and VPNs.
2. Configure and manage secure network protocols to ensure safe communication.
3. Identify and mitigate common security vulnerabilities in computer networks.

Competencies

1. Analyze and assess the security requirements of different network architectures.
2. Apply network security best practices to safeguard sensitive data and protect against cyber threats.
3. Develop practical skills in securing wireless networks and mobile communications.
4. Conduct security assessments and penetration tests to evaluate the effectiveness of security measures.