FACULTY OF COMPUTER APPLICATIONS
Computer Networks & Security

- **Sem.** : 1
- **Subject Code** : 05CS0106
- **Subject** : Computer Networks & Security
- **Course Objectives** :

Students will be able to

- Understand the fundamental concepts of computer networks and their role in modern communication.
- Identify and explain the key components of network architectures, including network types, devices, and communication protocols.
- Comprehend the principles of IP addressing and the differences between IPv4 and IPv6, along with their significance in network design.
- Apply cryptographic techniques to secure data transmission and understand key security protocols such as SSL/TLS.
- Analyze common network security threats and apply appropriate methods to mitigate risks and enhance network security.

FACULTY OF COMPUTER APPLICATIONS
Computer Networks & Security

- **Prerequisites** :

Unit No	Topics Covered	No of lectures required

1	• **Introduction to Computer Networks**
	• Overview of Computer Networks
	• Types of Networks
	  ○ (Overview of LAN, MAN, WAN, PAN, and Internetworks)
	• Network Communication
	  ○ Purpose of Networks
	  ○ Communication Mediums(Wired Media: Ethernet cables, fiber optics, Wireless Media: Radio waves, Wi-Fi, Bluetooth.)
	• Key Devices in Networking
	  ○ Router, Switch, Hub, Modem
	• Design Issues for Network Layers
	  ○ Connection-Oriented
	  ○ Connectionless
	  ○ Connection-oriented vs. connectionless service
		12

2	• **OSI and TCP/IP reference models** • Introduction to Reference Models • OSI Reference Model • TCP/IP Reference Model • Comparison Between OSI and TCP/IP Models • IP (Internet Protocol), TCP, HTTP, FTP, SMTP.	**12**

FACULTY OF COMPUTER APPLICATIONS
Computer Networks & Security

3	• **Basic Networking Concepts** • Introduction to IP Addressing • Overview of IPv4 • Overview of IPv6 • Difference between IPv4 vs IPv6 • Introduction to Packets and Frames • Different Protocols (HTTP/HTTPS, SMTP, TCP/IP, FTP) • Basics of Network Address Translation	**12**

4	• **Introduction to Authentication Mechanisms**
	• Introduction to CIA Triad
	• Authentication Methods
	  ○ Passwords
	  ○ Biometrics
	  ○ Two-factor authentication.
	  ○ Access Control Models
	• Implementation of authentication mechanisms using:
	• Passkeys
	• Multi-Factor Authentication (MFA)
	• Cryptographic keys
	• Web Application Firewall (WAF)
	• Data Loss Prevention (DLP)
	• Endpoint Security Solutions
		12

5	• **Network Security** • Introduction to Network Security • Types of Security Threats • Malware, Phishing, • Man-in-the-Middle Attacks, • Denial of Service (DoS) • **Introduction to Network Security Attacks** • Active Attacks • Passive Attacks • Insider vs Outsider Attacks • Targeted vs Untargeted Attacks • Physical vs Logical Attacks • Application-layer vs Network-layer Attacks	**12**

Course Outcomes :

- Demonstrate a clear understanding of computer network fundamentals, including various types of networks and communication protocols.
- Describe and compare OSI and TCP/IP reference models, and explain the functions of different layers in network communication.
- Configure and manage basic network addressing (IPv4 and IPv6), and understand how addressing impacts network communication and security.
- Implement cryptographic techniques to secure data, including symmetric/asymmetric encryption, and apply protocols like SSL/TLS for secure communication.
- Identify and mitigate network security threats, and apply techniques such as authentication methods and access control models to enhance network security.

Text Book :

1 Computer Networks, Andrew S Tanenbaum, David. J. Wetherall, Pearson Education, 2011

2 Cryptography and Network Security – Principles and Practice, William Stallings, Pearson Education, 2011

Reference Books :

Computer Networks, Computer Networks, Bhushan H Trivedi, Oxford University Press, 2016

Web References :

1. **http://www.cloudbus.org/**
2. **https://aws.amazon.com/**

References :

1. **Coursera**
2. **Udemy**

Syllabus Coverage from text /reference book & web/app reference:

Unit #	Chapter Numbers
1	Book 1 Chapter 1 and 2
2	Book 2 Chapter 2
3	Book 2 Chapter 3
4	Book 3 Chapter 1
5	Book 3 Chapter 2

FACULTY OF COMPUTER APPLICATIONS
Computer Networks & Security

Suggested List of Experiments:

Unit #	Chapter Numbers	No. of Hrs
1	● Identify networking devices (router, switch, modem) ● Create a basic LAN using Ethernet cables ● Compare wired vs wireless speed using Speedtest by Ookla ● Set up a Bluetooth PAN connection between devices	3
2	● Capture and analyze packets using Wireshark ● Identify protocols (HTTP, HTTPS, TCP, IP) in real traffic ● Compare HTTP vs HTTPS using browser inspection	3
3	● Run networking commands: ipconfig, ping, tracert ● Identify IPv4 and IPv6 addresses on system ● Demonstrate NAT using router settings ● Analyze packets and frames basics	3
4	● Set up Multi-Factor Authentication using Google Authenticator ● Test password strength (weak vs strong passwords) ● Configure basic firewall settings on system ● Demonstrate secure login using passkeys	3
5	● Simulate phishing email and identify threats ● Demonstrate DoS concept using LOIC (controlled lab) ● Perform basic MITM demo using Ettercap ● Classify types of attacks (active, passive, insider, outsider)	3