

Network Security

Course Title: Network Security

Course No: CSC416

Nature of the Course: Theory + Lab

Semester: VII

Full Marks: 60 + 20 + 20

Pass Marks: 24 + 8 + 8

Credit Hrs: 3

Course Description:

This course covers the fundamental concepts of network security protocols, wireless security concepts, basics of security in cloud and IoT.

Course Objectives:

The main objective of this course is to provide knowledge of network security so that students will be able to implement a secure network architecture using different security protocols and technologies.

Course Contents:

Unit 1: Computer Network Security Fundamentals (3 Hrs.)

- 1.1. Introduction
- 1.2. Securing the Computer Network
- 1.3. Forms of Protection
- 1.4. Security Standards

Unit 2: User Authentication (4 Hrs.)

- 2.1. Remote User-Authentication Principles
- 2.2. Remote User-Authentication Using Symmetric Encryption
- 2.3. Remote User-Authentication Using Asymmetric Encryption
- 2.4. Federated Identity Management

Unit 3: Transport Level Security (6 Hrs.)

- 3.1. Web Security
- 3.2. Transport Layer Security (TLS)
- 3.3. HTTPS
- 3.4. Secure Shell (SSH)

Unit 4: Wireless Network Security (6 Hrs.)

- 4.1. Wireless Security
- 4.2. Mobile Device Security
- 4.3. IEEE 802.11 Wireless LAN Overview
- 4.4. IEEE 802.11i Wireless LAN Security

Unit 5: Electronic Mail Security (8 Hrs.)

- 5.1. Internet Mail Architecture
- 5.2. E-mail Formats
- 5.3. Email Threats and Comprehensive Email Security
- 5.4. S/MIME

- 5.5. Pretty Good Privacy (PGP)
- 5.6. DNSSEC
- 5.7. DNS-Based Authentication of Named Entities
- 5.8. Sender Policy Framework
- 5.9. Domain Keys Identified Mail
- 5.10. Domain-Based Message Authentication, Reporting, and Conformance

Unit 6: IP Security (6 Hrs.)

- 6.1. IP Security Overview
- 6.2. IP Security Policy
- 6.3. Authentication Header
- 6.4. Encapsulating Security Payload
- 6.5. Security Associations
- 6.6. Internet Key Exchange

Unit 7: Network Endpoint Security (5 Hrs.)

- 7.1. Firewalls
- 7.2. Intrusion Detection System
- 7.3. Malicious Software
- 7.4. Distributed Denial of Service Attacks

Unit 8: Cloud and Internet of Things (IoT) Security (7 Hrs.)

- 8.1. Cloud Computing
- 8.2. Cloud Security Concepts
- 8.3. Cloud Security Risks and Countermeasures
- 8.4. Cloud Security as a Service
- 8.5. Open-source Cloud Security Module
- 8.6. Internet of Things (IoT)
- 8.7. IoT Security Concepts and Objectives
- 8.8. Open-source IoT Security Module

Laboratory Works:

The laboratory work includes implementation and simulation of Network Security Protocols, Intrusion Detection Systems, DDoS Attacks, Cloud Security and IoT Security Systems.

Text Books:

1. William Stallings, Cryptography and Network Security: Principles and Practice, 8th Edition, Pearson, 2020
2. Joseph Migga Kizza, Computer Network Security Fundamentals, 5th Edition, Springer, 2020

Reference Books:

1. William Stallings, Network Security Essentials: Applications and Standards, 6th Edition, Pearson, 2017
2. Sarhan M. Musa, Network Security and Cryptography: A Self-Teaching Introduction, Mercury Learning and Information LLC, 2018