

# NETWORK SECURITY

Course Code	: 18EC821	CIE Marks	: 40
Lecture Hours/Week	: 3	SEE Marks	: 60
Total Number of Lecture Hours	: 40 (08 Hrs / Module)	Exam Hours	: 03
CREDITS – 03			

**Course Learning Objectives:** This course will enable students to:

- Describe network security services and mechanisms.
- Understand Transport Level Security and Secure Socket Layer
- Know about Security concerns in Internet Protocol security
- Discuss about Intruders, Intrusion detection and Malicious Software
- Discuss about Firewalls, Firewall characteristics, Biasing and Configuration

## Module-1

Attacks on Computers and Computer Security: Need for Security, Security Approaches, Principles of Security Types of Attacks.

**(Chapter1-Text2)**

**L1, L2**

## Module-2

Transport Level Security: Web Security Considerations, Secure Sockets Layer, Transport Layer Security, HTTPS, Secure Shell (SSH)

**(Chapter15- Text1)**

**L1,L2**

## Module-3

IP Security: Overview of IP Security (IPSec), IP Security Architecture, Modes of Operation, Security Associations (SA), Authentication Header (AH), Encapsulating Security Payload (ESP), Internet Key Exchange.

**(Chapter19-Text1)**

**L1,L2**

## Module-4

Intruders, Intrusion Detection. **(Chapter20-Text1)**

**MALICIOUS SOFTWARE:** Viruses and Related Threats, Virus Counter measures,

**(Chapter21-Text1)**

**L1,L2**

## Module-5

Firewalls: The Need for firewalls, Firewall Characteristics, Types of Firewalls, Firewall Biasing, Firewall location and configuration

**(Chapter22-Text 1)**

**L1, L2**

**Course Outcomes:** After studying this course, students will be able to:

1. Explain network security services and mechanisms and explain security concepts
2. Understand the concept of Transport Level Security and Secure Socket Layer.
3. Explain Security concerns in Internet Protocol security
4. Explain Intruders, Intrusion detection and Malicious Software
5. Describe Firewalls, Firewall Characteristics, Biasing and Configuration

**Question paper pattern:**

- Examination will be conducted for 100 marks with question paper containing 10 full questions, each of 20 marks.
- Each full question can have a maximum of 4 sub questions.
- There will be 2 full questions from each module covering all the topics of the module.
- Students will have to answer 5 full questions, selecting one full question from each module.
- The total marks will be proportionally reduced to 60 marks as SEE marks is 60.

**TEXT BOOKS:**

1. Cryptography and Network Security Principles and Practice , Pearson Education Inc., William Stallings, 5<sup>th</sup> Edition, 2014, ISBN: 978-81-317- 6166-3.
2. Cryptography and Network Security, Atul Kahate, TMH, 2003.

**REFERENCE BOOKS:**

1. Cryptography and Network Security, Behrouz A. Forouzan, TMH, 2007.