6.4 PROGRAMME ELECTIVE - II
6.4.1 NETWORK SECURITY

L	P
2	2

RATIONALE

This course has been designed keeping in view basic computer users and information system managers. The students are acquainted with the concepts needed to secure a network, understanding risks and how to deal with them. It is hoped that the students will have a wider perspective on security in general and better understanding of how to reduce and manage the security risks.

COURSE OUTCOMES

After undergoing the subject, the students will be able to:

CO1: Learn the need of network security.
CO2: Study various encryption and decryption techniques.
CO3: Differentiate and deploy virus protection.
CO4: Describe Firewalls and intrusion detection systems.
CO5: Setup and configure virtual private network.

DETAILED CONTENTS

UNIT I

INTRODUCTION

Need for securing a network; Principles of Security, Type of attacks, introduction to cyber-crime, cyber law-Indian Perspective (IT Act 2000 and amended 2008), cyber ethics, ethical hacking. Hacking, Skimming, attacker, phreaker , hackivist, bluejacking, bluesnarfing, IOS Jailbreaking.

UNIT II

SECURING DATA OVER INTERNET

Introduction to basic encryption and decryption, concept of symmetric and asymmetric key cryptography, overview of DES, RSA and PGP. Introduction to Hashing: MD5, SSL, SSH, HTTPS, Digital Signatures, Digital certification, IPSec.

UNIT III

VIRUS, WORMS AND TROJANS

Definitions, preventive measures – access central, checksum verification, process configuration, virus scanners, heuristic scanners, application level virus scanners, deploying virus protection, Zombie, Ransomware.

UNIT IV

FIREWALLS

Definition and types of firewalls, firewall configuration, Limitations of firewall. Whitelisting Vs blacklisting.

INTRUSION DETECTION SYSTEM (IDS)/IPS

Introduction; IDS limitations – teardrop attacks, counter measures; Host based IDS set up

UNIT V

HANDLING CYBER ASSETS- Configuration policy as per standards, Disposable policy.

VIRTUAL PRIVATE NETWORK (VPN)

Basics, setting of VPN, VPN diagram, configuration of required objects, exchanging keys, modifying security policy

DISASTER AND RECOVERY

Disaster categories; network disasters – cabling, topology, single point of failure, save configuration files; server disasters – UPS, RAID, Clustering, Backups, server recovery

PRACTICAL EXERCISES

1. Installation and comparison of various antivirus software.
2. Installation and study of various parameters of firewall.
3. Writing program in C to Encrypt/Decrypt using XOR key.
4. Study of VPN.
5. Study of various hacking tools.
6. Practical applications of digital signature.

RECOMMENDED BOOKS

1. Cryptography and Network Security by Forouzon; Tata McGraw Hill Education Pvt Ltd, New Delhi.

2. Cryptography and Network Security by Atul Kahate; Tata McGraw Hill Education Pvt Ltd, New Delhi.

3. Cryptography and Network Security by Padmanabham; Wiley India Pvt Ltd. Daryaganj, New Delhi.

4. Network Security by Eric Cole, Bible; Wiley India Pvt Ltd. Daryaganj, New Delhi.

5. Network Security by William Stalling.

6. e-books/e-tools/relevant software to be used as recommended by AICTE/HSBTE/NITTTR.

RECOMMENDED WEBSITES

1. https://swayam.gov.in/

INSTRUCTIONAL STRATEGY

This is hands on practice based subject and topics taught in the class should be practiced in the Lab regularly for development of required skills among the students. This subject contains five units of equal weightage.