6.1 NETWORK SECURITY

L	T	P
3	-	3

RATIONALE

This course has been designed by keeping in view the basic computer users and information system managers. The concepts needed to read through the ripe in the market place and understanding risks and how to deal with them. It is hoped that the student will have a wider perspective on security in general and better understanding of how to reduce and manage the security risks.

DETAILED CONTENTS

1. Introduction (6 hrs)

   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. What is hacking? attacker, phreaker etc.

2. Securing Data over Internet (12 hrs)

   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

3. Virus, Worms and Trojans (8 hrs)

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

4. Firewalls (4hrs)

   Definition and types of firewalls, firewall configuration, Limitations of firewall.

5. Intrusion Detection System (IDS) (3 hrs)

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

6. Handling Cyber Assets- Configuration policy as per standards, Disposable policy (3 hrs)

7. Virtual Private Network (VPN) (6 hrs)

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

8. Disaster and Recovery (6 hrs)

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

Note: A visit to organizations must be organized for the demonstration about network security and exposure to available software

INSTRUCTIONAL STRATEGY

Since the facilities are not available in the polytechnic, students need exposure to various security systems and software available in some organisations, universities and engineering colleges. For this, visits may be organized for students. The teachers should also be exposed in this area. Some practicals can be conducted in the laboratory.

LIST OF PRACTICALS

1. Installation and comparison of various anti virus 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 Mc Graw Hill Education Pvt Ltd, New Delhi
2. Cryptography and Network Security by Atul Kahate, Tata Mc Graw 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

SUGGESTED DISTRIBUTION OF MARKS

Topic No.	Time Allotted (hrs)	Marks Allotted (%)
1.	6	10
2.	12	20
3.	8	20
4.	4	10
5.	3	10
6.	3	10
6.	6	10
7.	6	10
Total	**48**	**100**