0944 -DIPLOMA IN INFORMATION TECHNOLOGY & ENGINEERING
SEMESTER -I
094462 (a) NETWORK SECURITY
(Common with Computer Engineering)

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

Why Secure Network – Attackers Vs Hackers; attack from within and external

2. How Much Security

Promoting Risk analysis; developing security policy – accessibility, defining security goals, justifying the policy, roles and responsibility, consequences of non-compliance, level of privacy

3. Firewalls

Defining and access control policy, definition of firewalls and types, Firewalls (UNIX and NT), address translation, firewall logging, firewall deployment

4. Intrusion Detection System (IDS)

IDS introduction; IDS limitations – teardrop attacks, counter measures; Host based IDS setup

5. Authentication and Encryption

Authentication: Clear text transmission, session tracking; Encryption – methods, weaknesses, government interaction; Solutions – data encryption standards, digital certificate servers, IP security, Point to Point Tunneling Protocol (PPTP), RSA encryption, Secure Socket Layer (SSL), secure shell, Simple Key Management for IP (SKIP)

6. Visual Private Network (VPN)

Basics, setting of VPN – proposing with firewalls, VPN diagram, configuration of required objects, exchanging keys, modifying security policy

7. Virus, Trojans and Worms

What is Virus: replication, concealment, bomb, social engineering viruses; Worms; Trojan Horses; Preventive measures – Access Central, checksum verification, process neutering, virus scanners, neuristic scanners, application level virus scanners, deploying virus protection.

8. Disaster, Prevention and Recovery

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

LIST OF PRACTICALS

1. Installation of Anti-virus Package
2. Checking and removal of virus from the system
3. Expert lectures on Firewall
4. Expert lectures on Encryption, Decryption and Security Measures
5. Visit to higher organizations for the demonstration about Network security and exposure to software available

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 organised for students. The teachers should also be exposed in this area. Some practicals can be conducted in the laboratory.

RECOMMENDED BOOKS

1. Mastering Network Security by Christ Breton; BPB Publication, New Delhi
2. Web-sites by Chris Breton, BPB Publication, New Delhi
3. Network Firewalls by Kiranjeet Syan; New Rider Publication
4. Internet Security, New Rider Publication