B5.3-R4: NETWORK MANAGEMENT AND INFORMATION SECURITY

NOTE:

1. **Answer question 1 and any FOUR from questions 2 to 7.**
2. **Parts of the same question should be answered together and in the same sequence.**

Time: 3 Hours **Total Marks: 100**

1.

a) A password policy is a set of rules designed to enhance computer security by encouraging users to employ strong passwords and use them properly. Give your suggestion to have a strong password policy in your organization.

b) In computing, a denial-of-service (DoS) attack is an attempt to make a machine or network resource unavailable to its intended users. What are the types of DoS attack?

c) Risk Assessment is the process of quantifying the probability of a harmful effect to computer network. What are the ways to asses or determine risk in network?

d) Internet Protocol Security (IPsec) is a protocol suite for securing Internet Protocol (IP). What are the applications of it? Write down benefits of it.

e) A Virtual Private Network (VPN) is a network that uses primarily public telecommunication infrastructure. How can be implemented in your campus?

f) Once Internet Authentication Service (IAS) has authenticated the user, it can use a few authorization methods to verify that the authenticated user is permitted to access the network resource. Briefly write down those authorization methods.

g) How are Computer Viruses spread in internet?

(7x4)

2.

a) Information security means protecting information and information systems from unauthorized access. What are the elements of Information security?

b) Firewall prevents unauthorized access to personal network. What are different types of firewalls?

(10+8)

3.

a) What are the types of Network Security Attacks?

b) Describe in brief: Steps of Message Digest 5 (MD-5) algorithm.

(10+8)

4.

a) Cybercrime is any crime that involves a computer and a network. What are the types of attack comes under the category of Cybercrime? Why Cyberterrorism is an attractive option for modern terrorists.

b) What are the basics of Cryptography? What is Symmetric and public key cryptography?

c) Risk management reduces risk of the system. What are the principle and process of risk management?

(6+6+6)

5.

a) What are the different ways that hackers can attack on the system?

b) In Cryptography, a Public Key Certificate is an electronic document used to prove ownership of a public key. What are the Contents of Digital Certificate? How does Public Key Certificate authenticate clients?

(9+9)

6.

a) What are the various treatments of Risk?

b) What is TCP Session Hijacking? How is the TCP session hacked?

c) Secure Sockets Layer (SSL), are cryptographic protocols that provide communication security over the Internet. What kinds of messages are exchanged between client and server to ensure security of data?

(5+6+7)

7. Write short note on **any three** of the following:

a) Pretty-Good-Privacy (PCP)

b) Network Scanning

c) Indian Cyber IT Act 2000

d) Secured Electronic Transaction

(6+6+6)