B5.3-R4: NETWORK MANAGEMENT & 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 firewall is used to control traffic between networks. Briefly explain the main categories of firewall with reference to the layers where the traffic can be intercepted.

b) What is authentication? What is the difference between one-way authentication, two-way authentication and three-way authentication?

c) What is the difference between configuration management and configuration control in Network Management?

d) Mandatory access control (MAC) is an access policy determined by the system, not the owner. Is it true or false? Justify.

e) Explain briefly SNMP protocol and its use in message delivery.

f) What is the purpose of Windows registry? What are the methods to secure the windows registry?

g) Define the terms: Virus, Worm, Trojan Horse and Logic Bomb.

(7x4)

2.

a) RSA algorithm involves a public and private key. The public key can be known to everyone and is used for encrypting messages. How are the keys for the RSA algorithm generated? Write the steps of encryption and decryption for RSA algorithm.

b) The Internet Protocol (IP) is a network-layer protocol in the OSI model to enable packets being routed in network. What are its primary responsibilities? Explain the packet structure of IP / IPv4 (Internet Protocol version 4).

(9+9)

3.

a) The Internet Control Message Protocol (ICMP) is a troubleshooting tool used by technicians to find errors on a network, and it communicates errors on a network as they occur. How ICMP differs from TCP and UDP? Does ICMP guarantee delivery? Justify.

b) What are the three characteristics of crypto system for achieving security? Discuss each.

(9+9)

4.

a) Internet Protocol Security (IPsec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. Explain various IPSec services.

b) L2TP does not provide any encryption or confidentiality by itself; it relies on an encryption protocol that it passes within the tunnel to provide privacy. Explain L2TP.

c) What is RARP? How is it different from ARP (Address Resolution Protocol)?

(6+8+4)

5.

a) Kerberos is a network authentication protocol, which allows nodes communicating over a non-secure network to prove their identity to one another in a secure manner. Explain, how does it work?

b) Pretty Good Privacy (PGP) is a data encryption and decryption computer program that provides cryptographic privacy and authentication for data communication. Briefly explain how PGP encryption works.

(10+8)

6.

a) Explain the Diffie-Hellman key exchange algorithm. How is it prone to man in the middle attack?

b) What do you mean by digital signature? Explain Digital Signature Standard (DSS).

(9+9)

7. Write short notes on the following:

a) Differences between Symmetric and Asymmetric cryptosystem

b) Indian IT Act 2000

c) Biometric authentication

(3x6)