B5.3-R3: NETWORK MANAGEMENT & INFORMATION SECURITY

NOTE:

1. **Answer question 1 and any FOUR questions from 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) What do you understand by mandatory (nondiscretionary) access control? What are the mandatory access control rules?

b) What are the different types of messages define in SNMP?

c) How is Dictionary Attack method different from Heuristic Attack method?

d) List three penalties related to Cyber crimes from the IT act of India.

e) Compare and contrast between TCP spoofing and DNS Spoofing?

f) What do you understand by authentication? Explain authentication using public key cryptography.

g) Explain a method to secure the windows registry?

(7x4)

2.

a) What do you understand by a firewall? What is the packet filter? Explain the application level gateway mechanism in firewall to protect the vulnerable network.

b) Explain the protocol which allows newly booted workstation to broadcast its Ethernet address? Describe its advantages and disadvantages.

(10+8)

3.

a) How does a Virtual Private Network (VPN) work? Explain two most common types of IPSec VPN products.

b) What is a SNMP? Explain the SNMP model of a managed network with block diagram showing all the components.

(8+10)

4.

a) What are the various classes of Digital certificates? List three primary functions of CERT.

b) How does biometrics facilitate the IT security efforts of the Financial Institutions?

c) Differentiate between DOS attack and DDOS attack.

(9+6+3)

5.

a) What is encryption? Why is it required? Explain the RSA algorithm of encryption with example.

b) What are the major differences between MD4 and MD5?

c) Explain the difference between authentication and identification.

(9+6+3)

6.

a) What are the possible sources of threats in an enterprise network? Also identify the various types of threats and its targets in enterprise network?

b) How does Asymmetric Key Encryption ensures “Non-Repudiation and Privacy”? Explain with an example.

c) How do IP addresses get mapped on to data-link layer addresses, such as Ethernet? Explain by illustrating class ‘C’ networks of a university.

(6+6+6)

7.

a) What is the difference between passive and active attacks with respect to security threats faced in using the web?

b) What is CRL? How is it used to validate digital certificates?

c) What are Key Loggers? Write about the hardware Key Loggers? Why does a hacker uses the Key Loggers?

(6+6+6)