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) Distinguish between Host based and Network based Intrusion Prevention Systems.

b) Why is the Domain Security policy required? How is it different from local security policy?

c) What are the short comings of IT Act 2000 that deter companies from approaching the cyber cell for the enforcement?

d) How is Dictionary attack different from Brute Force attack?

e) What is the use of Active Directory in Windows 2000?

f) How can IPsec be used to create a VPN?

g) In most of the campus/corporate networks, we find firewalls preceded by a router, but not the reverse. Why has this become almost a de-facto standard?

(7x4)

2.

a) What are the various categories of Denial of Service Attack (DOS) available? State at least three ways by which this attack could be launched by an intruder.

b) Explain the various measures required to be taken in Security Testing of a financial institution with respect to IT.

(9+9)

3.

a) In RSA Encryption method if the prime numbers *p* and *q* are 3 and 17 respectively, the encryption exponent *e* is 11, find the following:
   i) the least positive decryption exponent *d*
   ii) public and private key
   iii) cipher text when the plain text P is encrypted using the public key ?

b) How does User Based Security Model provide integrity protection with or without delay detection and privacy protection?

(10+8)

4.

a) How is a virus different from a worm? What are the various types of viruses?

b) Compare the strength and weaknesses of Intrusion Detection System (IDS)?

c) How does Digital Signature prevent E-mail spoofing?

(8+6+4)

5.

a) Alice sends some message M to Bob using RSA public-Key encryption Algorithm where public key is (5,119) and private key is (77,119). The Cipher text is 66. Find the message M sent to Bob.

b) How does biometric help in secure electronic banking?

c) Why can IP spoofing not be prevented by using Packet Filter Firewall Technique?

(5+8+5)

6.

a) What is Trojan Horse? Explain some functions of the Trojan. Also suggest any three ways to detect Trojan.

b) How does Asymmetric key encryption ensure “Non-Repudiation”? Explain with an example.

c) Why are each initiator and each target assigned to one or more security groups in an access control scheme based on security labels?

(7+5+6)

7.

a) How is Kerberos designed to provide strong authentication for client/server applications by using secret key cryptography? Also mention the short comings of Kerberos.

b) How does SET make a digital wallet similar to a real wallet and secure for e-commerce payment transaction?

c) Explain briefly the three modes that a snoop can configure.

(6+6+6)