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 are the unicast and multicast packets? By examining the addresses used, determine whether the packet is multicast or unicast.
b) How IPSec can be used to create a VPN?
c) How does two filtering routers make the screened subnet firewall most secure?
d) What basic arithmetical and logical functions are used in MD5 and SHA-1?
e) What are the Denial of Service attacks?
f) How is ASN.1 different from other data structure definition schemes?
g) What are main services provided by Computer security incident response teams?

(7x4)

2.

a) What protocol is used at the transport layer? Explain briefly the three functional areas of IP level security.
b) Why does Encapsulating Security Payload (ESP) include a padding field?
c) What is the difference between passive and active attacks with respect to security threats faced in using the web?

(6+6+6)

3.

a) What are the basic techniques that are used by firewalls to control access and enforce the site's security policy?
b) Which type of firewall does act as a relay of application level traffic? Explain, how it is better from other types of firewalls.

(12+6)

4.

a) Differentiate between both the MD5 and SHA-1 algorithms.
b) Suppose that A has a data file namely "d" that B needs. A and B want to ensure a secure transmission of file. They do not want that anyone should know the content of file even if it is intercepted during transmission. B also wants to know whether or not whatever is transmitted from A has not been corrupted or altered in transit and that the file was sent by A. It is assumed that A and B share a secret symmetric key that no one else knows and there is a public key infrastructure available.
Describe the steps that A takes to send the data file "d" meeting the requirements give as above. *Your solution should only use as few a number of symmetric and/or public key as necessary while meeting the above requirements.*

(6+12)

5.

a) What are some of the attacks that can be made on packet filtering routers and their appropriate counter measures?
b) What are the procedures involved in Quantitative Risk Assessment? How is the Annualized Loss Expectancy (ALE) calculated?

(12+6)

6.

a) What was the security problem present in SNMP V1 that was solved in SNMP v3 and how?

b) What are two most popular active contents used as tools by attackers? Describe them briefly.

(12+6)

7.

a) What is a “smurf attack” and how is it defended?

b) What are the conditions prescribed in IT Act 2000 for the purpose of Electronic Governance to retain documents, record or information in electronic form for any specified period?

(12+6)