

## 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) What are the main categories of firewall with reference to the layers where the traffic can be intercepted and control?
  - 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) Define and briefly explain SNMP protocol and also explain how is it used 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 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 steps.
  - b) The Internet Protocol (IP) is a network-layer protocol in the OSI model to enable packets being routed in network. What are the primary responsibilities of it? Explain the packet structure of IP / IPv4 (Internet Protocol version 4).
  - c) Briefly Explain Steganography and also explain how it works? What are its advantages and application?

**(6+6+6)**
  
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) Confidentiality, Integrity and Availability form the core principles of information security. Briefly explain each of them.
  - c) What is Brute Force Attack? Explain.

**(8+4+6)**
  
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 is 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) What are the two main branches of public key cryptography? Briefly explain each of them.
- b) Explain key generation, encryption and decryption in RSA algorithm.
- c) Role-based access control (RBAC) is an approach to restricting system access to authorized users. Explain the three primary rules defined for role based access control.

**(4+10+4)**

7.

- a) A firewall is a device or set of devices designed to permit or deny network transmissions based upon a set of rules and is frequently used to protect networks from unauthorized access while permitting legitimate communications to pass. How a stateful firewall works? Explain.
- b) What are the design goals when any security service is designed for any organization?
- c) What is access control method? Explain the following access control model.
  - i) Bell-La Padula Model
  - ii) Biba Integrity Model

**(8+4+6)**