2/106 **2604N449** Candidate's Seat No :________

Integ. MSc (CSF) Semester-4 Examination

ICSF - 208

Network Security

April-2024

Time : 2-30 Hours] **[Max. Marks : 70**

Instructions: Illustrate your answers with neat diagrams wherever necessary.

Que 1 Write the following

(i) Explain the difference between client-server and peer-to-peer network architectures. Provide examples of each type of network. (7 Marks)

(ii) Describe the Open Systems Interconnection (OSI) model. Explain the functionalities of each layer in the OSI model. (7 Marks)

OR

(i) Compare and contrast the functionalities of switches, routers, and hubs in a network. Explain how each device contributes to data forwarding. (7 Marks)

(ii) Explain the importance of network security in modern computing. Identify the CIA triad and describe its significance in securing networks. (7 Marks)

Que 2 Write the following

(i) Briefly explain the functionalities of the following network devices: Router, Switch, and Firewall. (7 Marks)

(ii) Discuss the concept of risk assessment in network security. Explain the various steps involved in a risk assessment process. How does risk management help address security vulnerabilities? (7 Marks)

OR

(i) What is ACL? Explain in detail with diagram. (7 Marks)

(ii) Explain the role of Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) in network security. How do these systems differ in their functionalities? (7 Marks)

Que 3 Write the following

(i) Explain the concept of IP address and subnet mask. How does a subnet mask help with network management? (7 Marks)

(ii) Describe the two main types of network architectures: client-server and peer-to-peer. Give an example of each. (7 Marks)

OR

(i) What is the CIA triad in network security, and how does it relate to securing a network? (7 Marks)

(ii) Briefly differentiate between the functionalities of hubs and switches in a network. (7 Marks)

Que 4 Write the following

(i) Briefly explain the concept of risk assessment in network security. What are some key steps involved in this process? (7 Marks)

(ii) Briefly explain the concept of network sniffing and its potential dangers for network security. (7 Marks)

(P.T.O)

N449-2

OR

(i) Explain the functionalities of any two of the following protocols and their roles in network security: Kerberos, EAP, RADIUS, DAP (7 Marks)

(ii) Describe different types of network layer attacks. Explain how firewalls and their functionalities (e.g., packet filtering) help mitigate these attacks. (7 Marks)

Que 5 Attempt any seven out of twelve (14 Marks)

(i) Briefly describe the historical evolution of computer networking. What were some of the key milestones?

(ii) Identify two common network topologies. Briefly explain the advantages and disadvantages

(iii) Define two basic networking terms from the following list: IP Address, NAT, Subnetting, DHCP Server, Ports (Choose any two).

(iv) Briefly differentiate between the OSI model and the TCP/IP model.

(v) Differentiate between a firewall and packet filtering. Briefly mention their roles in network security.

(vi) What is the purpose of a DMZ (Demilitarized Zone) in a network security context?

(vii) Explain the role of the Authentication Header in the IPSec protocol suite.

(viii) Differentiate between OAuth 2.0 and TACACS+. Briefly mention a use case for each.

(ix) What are LDAP and RADIUS protocols used for in network security?

(x) Explain the concept of a VPN (Virtual Private Network) and its benefits in network security.

(xi) Briefly describe two methods used for network sniffing in information gathering.

(xii) How can dictionary attacks be mitigated in network security?