3/101 **2804E466** Candidate's Seat No :_____

IM.Sc. (CSF) (NEP) Sem.-4 Examination

DSC-C-ICSF-243 T

Network Security

Time : 2-00 Hours] **April-2025** **[Max. Marks : 50**

Question 1 Answer the following questions:

i. Explain the role of DHCP servers and how they interact with IP addresses and subnet masks in a networked environment. Use a small LAN setup example to illustrate your answer. 5Marks

ii. Compare the OSI and TCP/IP models in terms of data transmission from source to destination. Analyze the functions of three corresponding layers and explain how routers and switches operate within these layers. 5Marks

OR

i. Briefly explain how the TOR network ensures anonymity through layered encryption. Discuss its advantages for privacy and potential misuse in cybercrime, along with possible countermeasures. 5Marks

ii. Explain the concept of an IP address and differentiate between IPv4 and IPv6 addressing schemes. Describe how IP addresses are allocated in a network and discuss their significance in routing and network communication. 5Marks

Question 2 Answer the following questions:

i. Briefly describe common network layer attacks such as IP spoofing, packet sniffing, and DoS. How do these attacks impact communication, and what are the key countermeasures? 5Marks

ii. What is a firewall? Briefly explain its types and how each helps in securing a network. 5Marks

OR

i. How does an IDS differ from an IPS in terms of function and deployment in network security? 5Marks

ii. Explain the roles of any three network devices and relate them to OSI layers. What attacks can target them and how can these be mitigated? 5Marks

Question 3 Answer the following questions:

i. Define a Virtual Private Network (VPN). Explain its purpose and differentiate between the major types of VPNs such as remote access VPN, site-to-site VPN, and client-based VPN. 5Marks

(P.T.O)

ii. Illustrate how tunnelling protocols like PPTP, L2TP, and SSTP are used to establish secure VPN connections. Include the significance of tunnel and transport modes in IPsec-based VPNs. 5Marks

OR

i. Design a secure enterprise VPN solution using Generic Routing Encapsulation (GRE) and IPsec. Justify your choice of tunnelling protocol, encryption method, and implementation strategy for a multi-branch organization. 5Marks

ii. What is a VPN? Explain its role in secure communication and compare remote access, site-to-site, and client-based VPNs with suitable use cases. 5Marks

Questions 4 Answer the following questions:

i. What is network sniffing? Explain how sniffing tools capture network traffic and discuss their legitimate uses as well as potential risks in cybersecurity. 5Marks

ii. Define packet analysis. How does it aid in detecting security threats and monitoring network traffic? 5Marks

OR

i. What is Wireshark and how is it used in network analysis? Describe its key features and explain how it assists in diagnosing network issues and detecting malicious activity. 5Marks

ii. What is ARP poisoning in computer networks? Explain how it is executed, its impact on network communication, and the security measures that can be taken to detect and prevent it. 5Marks

Questions 5: Attempt any Ten out of Twelve. 10 Marks

1. Which OSI layer is responsible for routing, and how do routers operate at that layer?
2. How does NAT help in conserving IP addresses in a local network?
3. What is the difference between public and private IP addresses in a network?
4. Which networking devices operate at Layers 1, 2, and 3 of the TCP/IP model.
5. Name two common types of network layer attacks and state how they disrupt communication.
6. An Intrusion Prevention System (IPS) is a network security tool that not only detects threats but also actively _____ them.
7. A VPN tunnel provides _____ and _____ by encrypting data and hiding the source and destination addresses.
8. L2TP is often used in combination with _____ to provide encryption and security.
9. WEP has been largely replaced by more secure standards such as _____and _____.

E466-3

10 DNS poisoning typically targets the _____ layer of the OSI model.

11 Network sniffing is the process of _____ and analysing network traffic to capture data packets.

12 Sensitive information such as usernames and passwords can be exposed during sniffing if _____ is not implemented.

.....X.....X.....