Enrolment No._____

NATIONAL FORENSIC SCIENCES UNIVERSITY
GOA CAMPUS
M.Sc. Cyber Security - Semester -II Term Assessment-I

Subject Code: CTMSCS SII P1
Date: 28/02/2024 **Subject Name: Network Security**
Time: 45 Minutes **Total Marks: 25**

Instructions:

1. **Attempt all questions.**
2. **Make suitable assumptions wherever necessary.**
3. **Figures to the right indicate full marks.**

Q1 to Q10 Fill in the blanks/Multiple Choice questions, each for 1 mark (10x1=10)

Select your appropriate answer:

Q 1 _____layer of the OSI model is responsible for establishing, maintaining, and terminating connections between systems? **01 Mark**

Q 2 _____attack floods a network with a large volume of bogus traffic to disrupt normal operation? **01 Mark**

Q 3 _____ server filters and forward network traffic. **01 Mark**

Q 4 _____ attack involves sending fraudulent emails to trick individuals into revealing sensitive information? **01 Mark**

Q 5 Transport layer aggregates data from different applications into a single stream before passing it to _____ layer.

Q 6 What is the primary purpose of a Network Operations Center (NOC)? **01 Mark**

(i) Monitor and manage network infrastructure
(ii) Block malicious traffic
(iii) Investigate security incidents
(iv) Assign IP addresses to devices on a network
(v) All of these.

Q 7 In Three-Way Handshaking process, the situation where both the TCP's issue an active open is _____ **01 Mark**

(i) Mutual open
(ii) Mutual Close
(iii) Simultaneous open
(iv) Simultaneous close
(v) Never Close.

Q 8 What is the main function of a Firewall in a network? **01 Mark**

(i) To filter and control network traffic based on security rules
(ii) To route data packets between different networks
(iii) To provide dynamic IP addressing
(iv) To enhance network performance
(v) All of the above

Q 9 Which protocol is used by mail servers to send and receive emails? **01 Mark**

i) SMTP
ii) POP3
iii) IMAP
iv) SNMP

Q 10 What is the purpose of a SIEM system? **01 Mark**

i) To prevent unauthorized access to a network

ii) To manage DNS requests

iii) To monitor and analyze security events

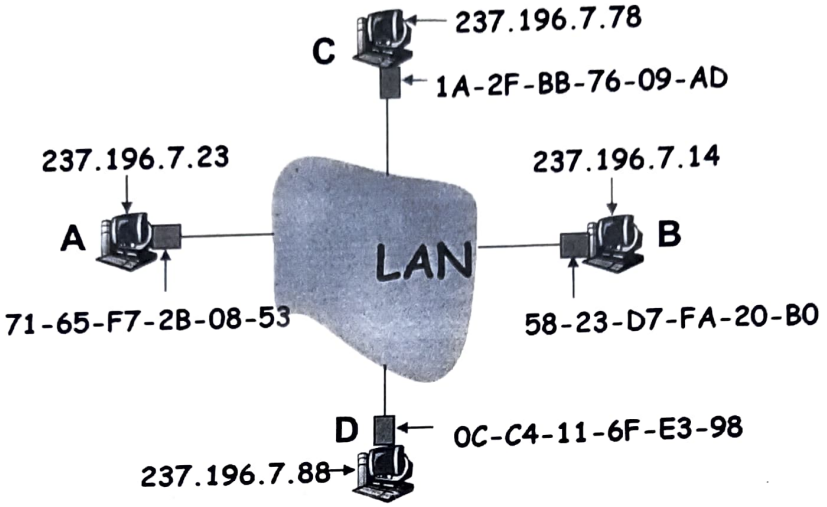
iv) To assign IP addresses to devices on a network

Q11 to Q15 Descriptive 3 marks for each question (5x3=15)

Q11 Discuss the differences between IDS and IPS in terms of detection and prevention mechanisms. **03 Marks**

Q 12 Differentiate the Non repudiation, Eavesdropping, and Masquerading. **03 Marks**

Consider the following Network: **(for Q 13-14)**



Q 13 Consider the above network topology, **User A** wants to communicate with **User B**. Explain the explain ARP protocol with respect to this scenario. Further consider **User C** as the attacker and explain the any ARP attack in the same topology. **03 Marks**

Q14 With respect to the same network topology, highlight the all-possible attack vectors and attack surfaces. **03 Marks**

Q 15 Read the following scenario and answer the questions below: **03 Marks**

Scenario: A medium-sized company operates a network infrastructure consisting of multiple offices interconnected through a Wide Area Network (WAN). The company's network includes servers for various services, such as DNS, DHCP, email, and applications. Recently, the company experienced a series of DDoS attacks that disrupted its operations and caused financial losses.

a) Identify potential vulnerabilities in the company's network infrastructure that could have been exploited to launch the DDoS attacks.

b) Recommend preventive measures and countermeasures to enhance the company's network security and mitigate the impact of future DDoS attacks.

~END OF PAPER~