All Paper VMP

Enrolment No._____

NATIONAL FORENSIC SCIENCES UNIVERSITY
GOA CAMPUS
M.Sc. DFIS - Semester -III/ M.Tech. I Term Assessment-I

Subject Code: CTMSDFIS SIII P1 **Date: 11/09/2024**

Subject Name: Network Security & Forensics

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 Multiple Choice questions, each for 1 mark (10x1=10)

Fill the appropriate answer:

Q 1 The _____ field in an IP packet is decremented at each router hop and helps prevent infinite routing loops.

Q 2 _____ is a protocol that sends error messages and operational information about network conditions, but is not used for regular data transmission.

Q 3 The organization responsible for coordinating the global Internet's systems of unique identifiers, including IP addresses and domain names, is called _____.

Q 4 On average, _____ of all possible keys must be tried to achieve success with a brute-force attack.

Q 5 The decryption of the ZHOFRPH WR ZRUOG RI FUBSWRJUDSKB is _____ (hint: use Caesar Cipher cryptoanalysis)

Q 6 The _____ model is a conceptual framework used to understand and implement standard communication protocols in network systems.

Q 7 The _____ is the total area of a system that could be compromised by security threats.

Q 8 A _____ attack involves sending fraudulent communications that appear to come from a trusted source, typically to steal sensitive information.

Q 9 A _____ is an advanced network device that operates at both the Data Link and Network layers, capable of routing data based on both MAC and IP addresses.

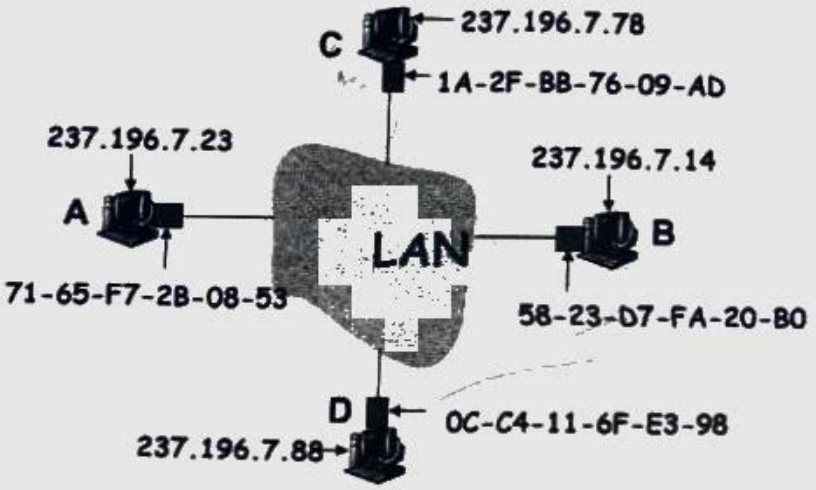
Q 10 _____ is a security measure that involves restricting user access to certain systems, applications, or data based on predefined policies.

Q11 to Q15 Descriptive 3 marks for each question (3x5=15)

Q11 Encrypt the plain text "DFIS" with the key "SQLINJECTION" using Playfair cipher. Also, verify the plain text from the generated cipher text. **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 ARP spoofing and TCP Session Hijacking in the same topology. **03 Marks**

Q14 With respect to the same network topology, explain TCP Session Hijacking and its countermeasures for this network attacks mentioned in question 13. **03 Marks**

Q 15 Explain following examples/terms: **03 Marks**

DFIS
fgnq

0 1 2 3 4 5 6 7 8
A B C D E F G H I
9 J 10 K 11 L 12 M 13 N 14 O 15 P 16 Q 17 R
18 S 19 T 20 U 21 V 22 W 23 X 24 Y 25 Z

(i) VPN vs VLAN

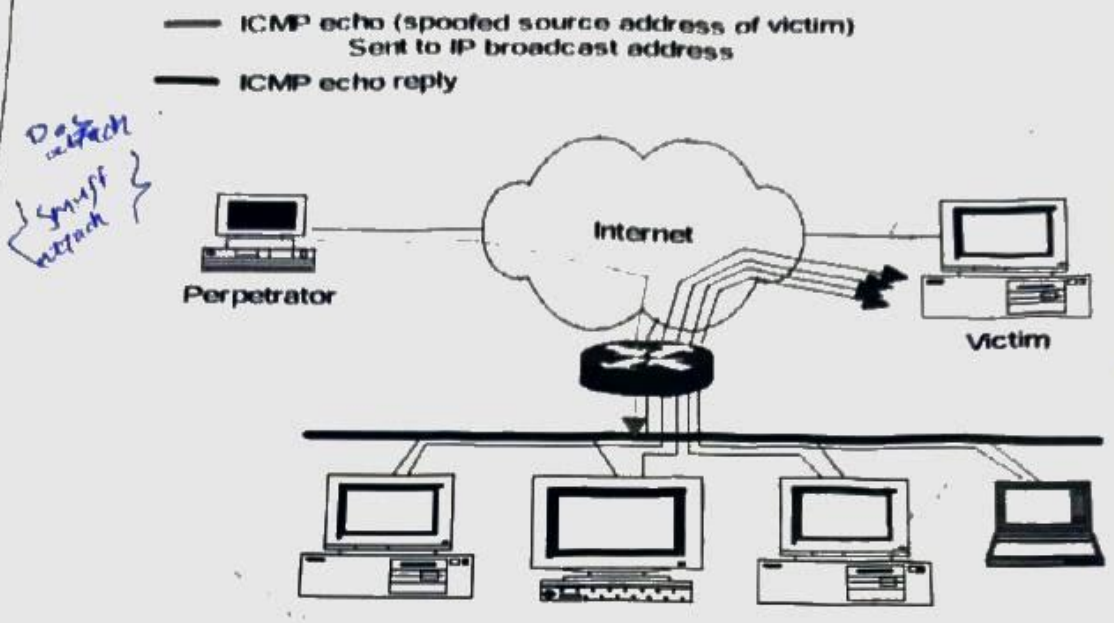
(ii) Local DNS vs TLD

(iii) IDS vs IPS

National Forensics Sciences University, Goa Campus
Mid- semester Examination
M.Sc. DFIS - Semester -III/ MTech AI&DS I

Branch – DFIS/AI&DS **Sem –** III **Date-** 07/10/2024
Subject Name- Network Security & Forensic **Subject Code-** CTMSDFIS SIII P1
Time- 1.5 Hours **Max. Marks-** 50
Instructions - 1) Answer all questions. 2) Assume suitable data.

Q.1	Attempt all.	**20 Marks**
	a. Explain the concepts of Threat, Vulnerability, and Attack Vector with relevant examples.	5 Marks
	b. Use *Vigenere Cipher* with key ***SAFE*** to encrypt the message ***"Life is full of joy".*** Ans → DIkIASkYDLTJBOD	5 Marks
	c. Encrypt the following message using *Playfair* cipher. Message: ***microprojectors*** Keyword: ***quasijudicial*** Ans → I/J → TEBOPRTPEMOPTAY Ans → P/Q → TQLOMATREBORTAY Ans → Y/Z → RQBOPRPEMJWMLS	5 marks
	d. Explain why the order of operations is crucial when performing digital signatures and encryption together. Discuss the implications of different sequences in which these processes can be executed.	5 Marks
Q.2	Attempt all questions **(Q 2(a)- 2 (c)):**	**15 Marks**
	a. Explain X.800 services with an example.	5 Marks
	b. What is the significance of flow control? Why is it important for the security point of view?	5 Marks
	c. During an analysis of an IPS (Intrusion Prevention System) log, you find that it detected 50 instances of ARP poisoning attacks over a week. If these attacks are consistent, calculate the average number of ARP poisoning attacks detected per day. Ans → 7 to 8 ans	5 Marks
Q. 3	Attempt any **two:**	**8 Marks**
	a. Calculate the multiplicative inverse of 7 under mod 19.	4 Marks
	b. Calculate: (i) $99^{1000000} \bmod 1000000$ (ii) $123456^{99999} \bmod 123455$ Ans → 99	4 Marks
	c. Explain cryptanalysis with an example.	4 Marks

Q.4	Attempt **any one**	**Marks**
	a. Consider the following network scenario:  1. Identify and explain the attack on the above scenario. 2. Also mention the countermeasures to protect this kind of attacks.	7 Marks
	OR	
	a. A firewall is configured with the following rules: • Allow HTTP (port 80) • Allow HTTPS (port 443) • Deny all other traffic. If an internal user attempts to access an FTP server on port 21, explain how the firewall will handle this request and the implications of this configuration for the organization.	7 Marks

National Forensics Sciences University, Goa Campus
Block Semester Examination
M.Sc. DFIS - Semester -III/ MTech AI&DS I

Branch – DFIS/AI&DS **Sem –** III **Date-** 23/10/2024
Subject Name- Network Security & Forensics **Subject Code-** CTMSDFIS SIII P1/ CTMTAIDS SI P1
Time- 1.5 Hours **Max. Marks-** 50
Instructions - 1) Answer all questions. 2) Assume suitable data.

Q.1	Attempt all.	**20 Marks**
	a. Explain the concepts of eavesdropping, masquerading and sniffing attack with relevant examples.	5 Marks
	b. Use *AutoKey Cipher* with key ***NFSU Goa*** to encrypt the message ***"At the end of the day, the goals are simple: safety and security."***	5 Marks
	c. Encrypt the following messages using *Polybius Cipher*: Message1: ***NFSU Gandhinagar*** Message2: ***World of Cryptography***	5 marks
	d. Explain the role and importance of SOC (Security Operations Center) and SIEM (Security Information and Event Management) in network security.	5 Marks
Q.2	Attempt all questions **(Q 2(a)- 2 (c)):**	**15 Marks**
	a. Consider a Phishing attack and a DoS attack. Explain how each attack is carried out and suggest two preventive measures for each.	5 Marks
	b. What are the differences between DNS and DHCP servers? How do they contribute to network management and security?	5 Marks
	c. Describe the principles and working of the rotor machine and its historical importance in encryption.	5 Marks
Q. 3	Attempt any **two:**	**8 Marks**
	a. Calculate the multiplicative inverse of ***5 under mod 23.***	4 Marks
	b. Calculate: ***(i) $7^{1000} \bmod 19$ (ii) $3^{200} \bmod 17$***	4 Marks
	c. Describe the principles and working of the rotor machine and its historical importance in encryption.	4 Marks
Q.4	Attempt **any one**	**Marks**
	Discuss ARP poisoning and MAC flooding attacks and propose possible countermeasures.	7 Marks
	OR	
	b. A user sends a message **"*HELLO*"** using RSA encryption, where the public key is ***(e = 3, n = 33)***. Find the public key, private key ciphertext, and plaintext.	7 Marks