Seat No.: ________ Enrolment No. 2401030007003

# NATIONAL FORENSIC SCIENCES UNIVERSITY

**Semester End Examination (December – 2024)**
**M.Tech. AI and Data Science (Specialization in Cyber Security)**
**Semester - I**

**Subject Code: CTMTAIDS SI P2** **Date: 04/12/2024**
**Subject Name: Network Security and Forensics**
**Time: 02:30 PM to 5:30 PM** **Total Marks: 100**

**Instructions:**

1. **Write down each question on a separate page.**
2. **Attempt all questions.**
3. **Make suitable assumptions wherever necessary.**
4. **Figures to the right indicate full marks.**
5. **Use of Scientific Calculator is allowed.**

**Marks**

**Q.1** **Attempt any three.**

**(a)** Describe the OSI Security Architecture (X.800). What are the five primary security services it provides? **08**

**(b)** What are the differences between IDS and IDPS? How are they implemented in a secure network environment? **08**

**(c)** Explain how threat intelligence is integrated into SOC operations. How does it differ from the predictive analytics used in a NOC? **08**

**(d)** Explain how MAC Flooding is conducted. Detail the steps involved in carrying out this attack. **08**

**Q.2** **Attempt any three.**

**(a)** What is a firewall, and what role does it play in network security? Also explain its various types. **08** 3

**(b)** How do Dumpster Diving and War Driving enable attackers to gather sensitive information? What countermeasures can organizations implement? **08** 3

**(c)** ***Scenario:*** A company's internal network is compromised by external hackers, potentially exploiting vulnerabilities in the system. As a network forensic investigator, how would you conduct the investigation to uncover the methods of intrusion and any potential backdoors? **08**

i. What network-based digital evidence would you focus on to trace the external hackers' actions within the compromised network?

ii. Discuss the process of evidence acquisition during a network intrusion investigation. What potential challenges could affect the preservation and integrity of digital evidence?

**(d)** How does the WPA protocol ensure secure communication over wireless networks? Explain its major components. Compare and contrast WEP and WPA in terms of security features, encryption methods, and susceptibility to attacks. **08**

**Q.3** **Attempt any three.**

(a) How does the penetration testing lifecycle progress from scope definition to reporting? Discuss each phase with examples and explain why each step is essential for a thorough security evaluation. **08**

(b) Given two prime numbers, p = 17 and q = 23, and public exponent e = 17, calculate the RSA public key and private key. Use these keys to encrypt the message M = 3. Show all necessary steps. **08**

(c) Construct any Monoalphabetic Cipher for following: **08**
***Key: 11***
***Plaintext: Welcome to the world of forensics.***

(d) Discuss the role of digital signatures, key management, and hash functions in ensuring secure communication. **08**

**Q.4** **Attempt any two.**

(a) In the context of digital forensics, what role does live acquisition play in preserving volatile data? Discuss the techniques used and the potential challenges involved. **07**

(b) An organization has experienced a data breach. Discuss the tools and techniques you would use to capture and analyze network traffic to identify the source of the breach. **07**

(c) ***Scenario:*** A business wants to enable employees to securely connect to its internal network from various remote locations while ensuring that the company's network resources are properly segmented based on departments.

(i) Describe the differences between VPN and VLAN in terms of securing data communication and network segmentation. **07**

(ii) Explain how DNS and DHCP would work together to resolve hostnames and assign dynamic IP addresses to devices within this secure network environment.

**Q.5** **Attempt any two.**

(a) A network device is receiving more data than it can process, leading to buffer overflow and potential denial of service (DoS). How would flow control techniques prevent these attacks? **07**

(b) Outline the key principles of the OSCAR methodology in digital forensics and explain how they are implemented during an investigation. **07**

(c) Differentiate the Non-repudiation, DoS, and DDoS. **07**

**--- End of Paper---**