2/71

0105N107

Candidate's Seat No :_____

MSc Sem.-2 Examination

407

Cybersecurity Forensic

Time : 2-30 Hours] **May-2025** **[Max. Marks : 70**

Question 1 Answer the following questions:

i. Explain the architecture and libraries of Metasploit Framework. 7Marks

ii. Explain Buffer overflow vulnerability in Windows 7 and how it can be exploited using Metasploit Framework. 7Marks

OR

i. What is msfconsole? Also Explain all seven modules of Metasploit framework in details. 7Marks

ii. What is backdoor? How it can be exploited in Metasploitable 2 through FTP service running on part 21? 7Marks

Question 2 Answer the following questions:

i. Explain Caesar Cipher with an example. Discuss its strengths and weaknesses. 7Marks

ii. Describe the Advanced Encryption Standard (AES). How does it ensure strong encryption? 7Marks

OR

i. Explain the structure and working of the Data Encryption Standard (DES). Why is it considered weak today? 7Marks

ii. What are the main challenges in modern cryptography? How do they impact system security? 7Marks

Question 3 Answer the following questions:

i. Explain the step-by-step process of how blockchain works, from the creation of a transaction to its validation and addition to the chain. 7Marks

ii. Explain the Proof of Work (PoW) consensus mechanism. How does it ensure security and decentralization in blockchain networks? Discuss the advantages and disadvantages of PoW as a consensus method in blockchain. 7Marks

OR

i. Describe the Proof of Stake (PoS) consensus mechanism and its key differences from Proof of Work. Explain how validators are selected in PoS and how this reduces the environmental impact compared to PoW. 7Marks

(P.T.O)

N 107-2

ii. Describe how the combination of decentralization, transparency, and immutability makes blockchain reliable and secure. 7Marks

Questions 4 Answer the following questions:

i. Explain the concept of a Message Authentication Code (MAC) and how it ensures message integrity and authentication. 7Marks

ii. Compare and contrast MD5 and SHA-1 in terms of design, security, and output. 7Marks

OR

i. Describe the working of the Digital Signature Standard (DSS). What cryptographic algorithms does it use? 7Marks

ii. Explain how hash functions are used in authentication. Why are they preferred over other methods? 7Marks

Questions 5: Attempt any Seven out of Twelve. 14 Marks

1. Differentiate between a Metasploit exploit and a payload.
2. What is the key principle behind the Caesar Cipher?
3. State one major difference between a Vigenère Cipher and a Caesar Cipher.
4. Define Confidentiality and Integrity in the context of cybersecurity.
5. What is a Row Transposition Cipher?
6. Name two key applications of blockchain technology.
7. What is a Message Authentication Code (MAC)?
8. Mention two common hashing algorithms used in digital security.
9. State the basic principle of RSA algorithm.
10. What is the significance of prime numbers in public key cryptography?
11. What is Meterpreter?
12. Differentiate between reverse shell and bind shell.

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