National Forensics Sciences University, Goa Campus

M.Sc. CS - Semester -II

Term Assessment-2/ Assignment-1

Branch – MSC DFIS/ M.Tech AI&DS Sem – III/I Submission Date- 21/11/2024

Subject Name- Network Secur~~ity & Forensic~~ Subject Code- CTMSDFIS SIII P1Max. Marks- 10

Instructions - 1) Answer all questions. 2) Assume suitable data. 3) ONLY Handwritten Note.

Q.1	**Attempt All.**	**Marks**
(a)	(a) Elaborate on the Oscar Methodology.	**1**
(b)	b) If network security administrators block ***nmap*** port scans, how would you go about acquiring host information in such a scenario?	**1**
(c)	Describe the concept of a digital signature and explain how it is used to ensure message integrity and authenticity.	**1**
(d)	(d) Given a message M, a key K, and a hash function H, calculate the HMAC value using the HMAC algorithm.	**1**
Q.2	**Attempt All.**	
(a)	(a) Outline three valid business reasons for an organization to monitor network forensic data to safeguard employee privacy.	**1**
(b)	Discuss the strengths and weaknesses of different cryptographic algorithms such as AES, DES, and ECC, and compare their performance in terms of security and efficiency.	**1**
(c)	Describe the differences between symmetric and asymmetric encryption. Explain scenarios where each type is preferred over the other.	**1**
(d)	Delve into the purpose and application of OSINT tools in the context of network security and digital forensics investigations.	**1**
Q.3	**Attempt All.**	
(a)	Break down the following terms with examples: (i) Distinguish between VPN and VLAN. (ii) Define Buffer Overflow. (iii) Explain the concept of an Evil Twin.	**2**
(b)	(i) Suppose Alice wants to digitally sign a message using the RSA digital signature scheme. She chooses her prime numbers as p=11 and q=13, and her private key d=7. Calculate her public key e, then digitally sign the message "Hello" and verify the signature.	**2**
	(ii) explain the AES Algorithm in detail.	
	iii) In the context of SSL/TLS handshake, describe the steps involved in establishing a secure connection between a client and a server, including the role of public-key cryptography, symmetric-key cryptography, and digital certificates.	