National Forensics Sciences University, Goa Campus
MTech I M.Sc. /CS - Semester -I
Term Assessment-2

Subject Code: CTMSCS SII P1 **Final Date of Submission: 10th Dec 2023**
Subject Name: Network Security

Total Marks: 25

Instructions - 1) Answer all questions. 2) Assume suitable data. 3) Scientific Calculator is allowed.4) Parts of the question should attend the same place.

Q.1	**Attempt All.**	**Marks**
(a)	(a) Elaborate on the Oscar Methodology.	**2**
(b)	b) If network security administrators block ***nmap*** port scans, how would you go about acquiring host information in such a scenario?	**2**
(c)	(c) Detail the operation of TKIP and CCMP protocols in the context of 802.11i.	**2**
(d)	(d) Identify three TAPs in the realm of network forensics.	**2**
Q.2	**Attempt All.**	
(a)	(a) Outline three valid business reasons for an organization to monitor network forensic data to safeguard employee privacy.	**2**
(b)	Provide an explanation of the diverse commands available in Wireshark (formerly known as Pie shark).	**2**
(c)	Clarify the purpose and utilization of OSSEC, an open-source host-based intrusion detection system (HIDS).	**2**
(d)	Delve into the purpose and application of OSINT tools in the context of network security and digital forensics investigations.	**2**
Q.3	**Attempt All.**	
(a)	Break down the following terms with examples: (i) Distinguish between VPN and VLAN. (ii) Illustrate the Avalanche Effect. (iii) Differentiate between Attack Surface and Attack Vector. (iv) Define Buffer Overflow. (v) Explain the concept of an Evil Twin.	**4**
(b)	(i) Define ***tcpdump*** and ***pcap***, and elaborate on Role-Based Access Control.	**5**
	(ii) Provide a comprehensive explanation of SOC (Security Operations Center) functionality.	
	iii) List and elucidate various commands in Wireshark	

~~~~END OF PAPER~~~~