



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

Subject Code: CTMSCS SII P1		Final Date of Submission: 26th June 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)	Explain Oscar Methodology in detail.	2
(b)	What would you do if nmap port scans are blocked by network security administrator? How would you gather host information in such case?	2
(c)	With reference to 802.11i , describe the operation of TKIP and CCMP protocols?	2
(d)	Three TAP in network forensics	2
Q.2	Attempt all.	
(a)	Corporate network surveillance is a computer forensic activity that is very common. In order for an organization to prevent violations of the privacy of employees, the first requirement is to establish the business purpose of monitoring network forensic data. List three valid business reasons why a business or other organization may be able to monitor network forensic data.	2
(b)	Explain various commands of Pie shark.	2
(c)	Explain the purpose and usage of OSSEC, an open-source host-based intrusion detection system (HIDS).	2
(d)	Describe the purpose and usage of OSINT (Open Source Intelligence) tools in network security and digital forensics investigations.	2
Q.3		
(a)	Explain following terms with example: (i) VPN vs VLAN (ii) Avalanche Effect (iii) Attack Surface vs Attack Vector (iv) Buffer Overflow (v) Evil Twin	4
(b)	(i) What <i>tcpdump</i> and <i>pcap</i> ? Explain. Also explain the Role base Access Control. (ii) Explain SOC Functionality in detail. (iii) Various commands of Pie shark	5