Name: **Enrolment No:**	

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES
End Semester Examination, December 2022

Course: Forensic Tools **Semester: III**
Program: MCA **Time: 03 hrs.**
Course Code: CSCS8002 **Max. Marks: 100**

Instructions: Attempt all Questions

SECTION A
(5Qx4M=20Marks)

S. No.		Marks	CO
Q 1	Illustrate Huffman Compression with the help of an example.	**4**	**CO1**
Q 2	Discuss the approach of investigating in Computer Investigations.	**4**	**CO2**
Q 3	Mention the role of File System in Cyber Forensics.	**4**	**CO3**
Q 4	Assuming that each is correctly implemented, should the selective repeat protocol perform much better than go-back-n on a fiber optic link between two nodes about a half-mile apart?	**4**	**CO4**
Q 5	Illustrate the different Anti Digital Forensics methodologies with suitable example.	**4**	**CO1**

SECTION B
(4Qx10M= 40 Marks)

Q 6	You're sitting in a coffee shop enjoying a latte and doing some relaxing computer security reading at http://awesome-security-stuff.com. You're connected on the coffee shop's Wi-Fi network. You notice that each article has a Facebook Like button, loaded as such: allowing you to indicate on Facebook that you enjoyed this article. If Facebook wanted to, could it track what articles you are visiting, if you don't click on the Like button? Justify your answer.	**10**	**CO2**

Q 7	Demonstrate the functionality of NAT with suitable diagram. State 2 different problems associated with NAT.	**10**	**CO3**
	OR		
Q 7	List three unique attributes of a user's browser that a fingerprinting script could use to persistently identify the user even if they clear their cookies and other site data.	**10**	**CO3**
Q 8	Illustrate the Incident Response Methodology and the six steps associated with it.	**10**	**CO4**
Q 9	Request: GET /view?filename=hello.txt HTTP/1.1 Host: localhost:4000 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_1) Response: HTTP/1.1 200 OK Content-Type: text/html; charset=utf-8 Date: Tue, 10 Dec 2019 00:00:00 GMT Hello, world! There is a glaring security vulnerability in this server. What is the issue? How could the issue be fixed?	**10**	**CO1**
SECTION-C (2Qx20M=40 Marks)			
Q 10	To understand the effect of window size on the performance of sliding window protocol, consider an error free channel of 1 Mbps with 20 msec propagation delay. The frame size is 256 bytes with negligible header. Acknowledgement frames can be ignored. Calculate the performance of sliding window protocol for window sizes varying from 1 to 32 in steps of 5 and plot them.	**20**	**CO2**

Q 11	During a security review, you encounter the following C function, which may be called by untrusted code:
	
	int table [800];
	int insert_in_table(int val, int pos) {
	if (pos > sizeof(table) / sizeof(int)) return -1;
	table[pos] = val;
	return 0 ;
	}
	
	(a) Identify potential vulnerabilities and provide a fixed version.
		20	**CO3**

	(b) An application process receives information via a UDP packet over a wired Ethernet LAN connection. If the packet carries a source port number below 1024, under which conditions can the information be trusted?		
	OR		
Q 11	The One Laptop Per Child project aims to supply millions of rugged low-cost laptops to children in less-developed countries. The machines run Linux, have 2 Gb Flash rather than a hard disk, and have a wireless LAN capability that may be used either in the conventional way or to set up ad-hoc peer-to-peer networks. Your task is to design the security policy for these laptops. If the project is to supply standard security software with each machine, what should it try to do, and how?	**20**	**CO3**