Roll No.											

PRESIDENCY UNIVERSITY

BENGALURU

End - Term Examinations – December 2025

Date: 18 – 12- 2025 **Time:** 01:00pm – 04:00pm

School : SOCSE	**Program:** B Tech CSE (Cyber Security)	
Course Code : CSE3102	**Course Name:** Malware Analysis	
Semester: VII	**Max Marks**: 100	**Weightage**: 50%

CO - Levels	CO1	CO2	CO3	CO4	CO5
Marks	**26**	**24**	**24**	**26**	**-**

Instructions:

(i) Read all questions carefully and answer accordingly.
(ii) Do not write anything on the question paper other than roll number.

Part A

Answer ALL the Questions. Each question carries 2marks. **10Q x 2M=20M**

1.	State the main goal of performing dynamic malware analysis.	**2 Marks**	**L1**	**CO1**
2.	Define the primary function of a Remote Access Trojan (RAT).	**2 Marks**	**L1**	**CO1**
3.	Tabulate one advantage and one disadvantage of static malware analysis.	**2 Marks**	**L1**	**CO1**
4.	Outline how signature-based antivirus scanning detects malware.	**2 Marks**	**L1**	**CO2**
5.	Identify the significance of the .rsrc section in a PE file.	**2 Marks**	**L1**	**CO2**
6.	Recognize how dynamic analysis helps detect Indicators of Compromise (IoCs).	**2 Marks**	**L1**	**CO3**
7.	Describe how malicious documents use macros to deliver malware payloads.	**2 Marks**	**L1**	**CO3**
8.	Outline the concept of similarity-based detection in antivirus systems.	**2 Marks**	**L1**	**CO4**
9.	Relate privilege escalation to the success of targeted attacks.	**2 Marks**	**L1**	**CO4**
10.	List any two ways malware maintains persistence after reboot.	**2 Marks**	**L1**	**CO4**

Part B

Answer the Questions. **Total Marks 80M**

11.	**a.**	Differentiate between a virus and a worm, explaining their modes of propagation and the potential effects they have on infected systems.	**10 Marks**	**L2**	**CO1**
	b.	Examine the process of antivirus scanning and discuss the common evasion techniques used by malware authors to bypass detection mechanisms.	**10 Marks**	**L3**	**CO2**
		Or			
12.	**a.**	Describe the main characteristics of spyware and adware, highlighting how they affect system performance	**10 Marks**	**L2**	**CO1**
	b.	Classify the structure of the Portable Executable (PE) file format and illustrate its significance in malware analysis and investigation.	**10 Marks**	**L3**	**CO2**

13.	**a.**	Describe the process of static malware analysis and explain how it helps in understanding the internal behavior, nature, and capabilities of malicious software. Illustrate how this analysis contributes to effective detection and classification of malware.	**10 Marks**	**L2**	**CO1**
	b.	Demonstrate the role of reverse engineering in advanced static malware analysis by explaining how it helps uncover the internal logic and hidden functionalities of malicious code. Discuss the key tools and methodologies commonly employed in this process.	**10 Marks**	**L3**	**CO2**
		Or			
14.	**a.**	Describe a botnet and explain the mechanisms through which attackers control and coordinate multiple compromised systems within it.	**10 Marks**	**L2**	**CO1**
	b.	Interpret how virtual machines are configured and utilized to create a safe, isolated environment for conducting malware analysis. Illustrate how this setup prevents damage to the host system during experimentation.	**10 Marks**	**L3**	**CO2**

15.	**a.**	Demonstrate the step-by-step process of setting up and operating a malware sandbox environment.	**10 Marks**	**L3**	**CO3**
	b.	Interpret and analyze the concept of process replacement and APC injection, highlighting how they aid in stealthy malware execution.	**10 Marks**	**L3**	**CO4**

		Or			
16.	**a.**	Illustrate the procedure used to analyze malicious documents and interpret how embedded macros function.	**10 Marks**	**L3**	**CO3**
	b.	Determine and explain the limitations of traditional signature-based detection methods against metamorphic and polymorphic malware.	**10 Marks**	**L3**	**CO4**

17.	**a.**	Produce a detailed workflow to demonstrate how dynamic analysis leads from sandbox setup to behavioral reporting.	**10 Marks**	**L3**	**CO3**
	b.	Predict how malware developers modify existing binaries to evade similarity-based detection techniques.	**10 Marks**	**L3**	**CO4**
		Or			
18.	**a.**	Use dynamic analysis methods to predict evasion techniques that advanced malware may use against sandbox environments.	**10 Marks**	**L3**	**CO3**
	b.	Prepare and illustrate a detailed explanation of malware signatures, including packed and polymorphic malware signatures.	**10 Marks**	**L3**	**CO4**