Roll No.												

PRESIDENCY UNIVERSITY

BENGALURU

Mid - Term Examinations – October 2025

Date: 29-10-2025 **Time:** 02.30pm to 04.00pm

School: SOCSE	**Program:** B Tech CSE (Cyber Security)	
Course Code : CSE3102	**Course Name:** Malware Analysis	
Semester: VII	**Max Marks**: 50	**Weightage**: 25%

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

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. **5Q x 2M=10M**

1	Describe what is meant by a computer virus.	**2 Marks**	**L1**	**CO1**
2	Explain the main function of spyware in a computer system.	**2 Marks**	**L1**	**CO1**
3	Distinguish the term unauthorized access in the context of system security.	**2 Marks**	**L1**	**CO1**
4	Demonstrate two advantages of performing malware analysis using virtual machines.	**2 Marks**	**L1**	**CO2**
5	Use examples to show two general-purpose registers in x86 assembly language.	**2 Marks**	**L1**	**CO2**

Part B

Answer the Questions. **Total Marks 40M**

6.	**a.**	Explain how malware can be used for data theft and discuss its impact on information security.	**10 Marks**	**L2**	**CO1**
	b.	Illustrate the importance of malware fingerprinting using hashes and YARA rules, and explain with an example how they assist in malware detection.	**10 Marks**	**L3**	**CO2**
		Or			
7.	**a.**	Describe the main objectives of malware analysis and discuss its role in mitigating modern cyber threats.	**10 Marks**	**L2**	**CO1**
	b.	Demonstrate how entropy analysis and overlay data are applied in identifying packed or obfuscated executables, highlighting their significance in static analysis.	**10 Marks**	**L3**	**CO2**

8.	**a.**	Explain the rise of ransomware attacks and discuss their significance in the overall evolution of modern cyber threats. Highlight how ransomware has transformed the threat landscape and influenced cybersecurity defense strategies.	**10 Marks**	**L2**	**CO1**
	b.	Interpret the role of section headers in the Portable Executable (PE) file format. Discuss how anomalies such as unusual section names, sizes, or attributes can serve as indicators of malicious activity or packed executables.	**10 Marks**	**L3**	**CO2**
		Or			
9.	**a.**	Explain the concept of ransomware and discuss the potential threats it poses to users, organizations, and critical systems. Illustrate its impact on data confidentiality, integrity, and availability.	**10 Marks**	**L2**	**CO1**
	b.	Examine the role of section headers in the Portable Executable (PE) file format. Discuss how anomalies such as unusual section names, sizes, or attributes can serve as indicators of malicious activity or packed executables.	**10 Marks**	**L3**	**CO2**