Roll No.												

PRESIDENCY UNIVERSITY

BENGALURU

School of Computer Science and Engineering

Mid - Term Examinations - November 2024

Semester: 7th | **Date**: 05/11/2024

Course Code: CSE 3102 | **Time**: 09.30am to 11.00am

Course Name: Malware Analysis | **Max Marks**: 50

Program:B.Tech(CCS) | **Weightage**: 25%

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. **5QX2M=10M**

1	Which type of malware analysis involves executing the malware in a controlled environment to observe its behavior?	**2 Marks**	**L1**	**CO1**
2	What is the primary goal of malware analysis?	**2 Marks**	**L1**	**CO1**
3	List the types of malwares designed to steal sensitive information, such as login credentials and credit card numbers, from the victim's system?	**2 Marks**	**L1**	**CO1**
4	What is the purpose of disassembling malware code during static analysis?	**2 Marks**	**L1**	**CO2**
5	Recall the purpose of disassembling malware code during static analysis.	**2 Marks**	**L1**	**CO2**

Part B

Answer ALL Questions. Each question carries 10 marks. **4QX10M=40M**

6	A user receives an email with an attachment that claims to be a software update. However, upon closer inspection, the attachment is actually a malicious executable file. What type of malware is this, and how can it be prevented in the future?	**10 Marks**	**L3**	**CO**

or

7	A company's network has been compromised by a ransomware attack. Describe the steps that the incident response team should take to respond to this incident. How would they contain the attack, eradicate the malware, and recover from the incident?	**10 Marks**	**L3**	**CO1**
8	Describe the differences between static and dynamic malware analysis. What are the advantages and disadvantages of each approach? List out the tools used in each analysis	**10 Marks**	**L2**	**CO1**
	or			
9	Describe the concept of anti-analysis techniques used by operating systems to prevent malware analysis. How do these techniques make it difficult for malware analysts to L3 malware, and what are the limitations of these techniques?	**10 Marks**	**L2**	**CO1**
10	A security researcher discovers a new malware sample that uses advanced anti-analysis techniques to evade detection. How can the researcher use basic static analysis techniques to gather information about the malware's behavior and identify potential vulnerabilities?	**10 Marks**	**L3**	**CO2**
	or			
11	A malware analyst is tasked with analyzing a new malware sample using anti-virus scanning. How can the analyst use anti-virus scanning to identify potential threats and gather information about the malware's behavior?	**10 Marks**	**L3**	**CO2**
12	Explain the methodology of conducting advanced static analysis of malware, and its significance in identifying potential threats. How do advanced static analysis techniques complement other malware analysis methods?	**10 Marks**	**L2**	**CO2**
	or			
13	Describe the process of using IDA Pro to L3 malware, and how it can be used to identify potential threats. What are the benefits and limitations of using IDA Pro in malware analysis?	**10 Marks**	**L2**	**CO2**