Enrolment No./Seat No_____

GUJARAT TECHNOLOGICAL UNIVERSITY

BE- SEMESTER–VII (NEW) EXAMINATION – WINTER 2024

Subject Code:3174506 Date:30-11-2024

Subject Name: Malware Analysis

Time:10:30 AM TO 01:00 PM Total Marks:70

Instructions:

1. **Attempt all questions.**
2. **Make suitable assumptions wherever necessary.**
3. **Figures to the right indicate full marks.**
4. **Simple and non-programmable scientific calculators are allowed.**

			MARKS
Q.1	**(a)**	What are the goals of malware analysis? Explain in brief.	**03**
	(b)	List out some of the malicious actions performed by malware.	**04**
	(c)	Define the following terms: (1) Virus (2) Worm (3) Rootkit (4) Trojan (5) Botnet (6)Spyware (7) Information stealer	**07**
Q.2	**(a)**	What is the role of dynamic link libraries in malware analysis?	**03**
	(b)	Explain PE Headers and Sections in detail with suitable figures.	**04**
	(c)	Why is it necessary to perform malware analysis? Give the reasons.	**07**
		OR	
	(c)	Explain signature-based malware techniques.	**07**
Q.3	**(a)**	Explain any five common DLL files functionalities.	**03**
	(b)	How does OllyDbg is applicable to analyze malware? Explain with suitable example.	**04**
	(c)	What hex values "Magic" field in Optional header is set to? How to determine total size of header in Disk? Explain with suitable example.	**07**
		OR	
Q.3	**(a)**	Explain Kernel Vs User mode debugging.	**03**
	(b)	Explain the level of abstraction in malware analysis.	**04**
	(c)	How ransomware works? How to apply prevention mechanism to defend ransomware attacks?	**07**
Q.4	**(a)**	List the IDA Pro functionalities.	**03**
	(b)	Explain Windows API concepts with respect to malware analysis.	**04**
	(c)	How to extract Indicators of Compromise (IOCs) from Malware using Basic Static Analysis? Explain with suitable example.	**07**
		OR	
Q.4	**(a)**	Distinguish Hook Injection Vs. APC Injection.	**03**
	(b)	How does malware establish persistence? Analyze the Pegasus malware persistence in detail and write down the type of information being targeted with CVE details.	**04**
	(c)	Differentiate static and dynamic analysis. Why does malware analyst need to perform dynamic analysis?	**07**
Q.5	**(a)**	Explain the analysis of malicious Windows programs.	**03**
	(b)	Explain android malware characterization in brief.	**04**
	(c)	Give the name of two different tools that you would use as a malware analyst which is being used in different phases of malware analysis. Explain these tools with features and characteristics.	**07**

OR

Q.5	**(a)**	Why Emotet malware is considered as most dangerous malware in the World?	**03**
	(b)	Which attack vectors were applied by the hackers to deliver the Emotet malware? Explain in brief.	**04**
	(c)	Define polymorphic malware and metamorphic malware. Differentiate both with suitable example.	**07**

****