REG.NO.:

VIT

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING

SLOT: A1

CONTINUOUS ASSESSMENT TEST - II
FALL SEMESTER 2024-2025

Programme Name & Branch	:	**B.TECH – CSE (IS)**		
Course Code and Course Name	:	**BCSE321L - Malware Analysis**		
Faculty Name(s)	:	**Dr. Jayakumar S, Dr. Kathiravan S**		
Class Number(s)	:	**VL2024250101454, VL2024250101457**		
Date of Examination	:	**13-Oct-2024**		
Exam Duration	:	**90 minutes**	**Maximum Marks: 50**	

General instruction(s):

- Answer All Questions
- M - Max mark; CO – Course Outcome; BL – Blooms Taxonomy Level (1 – Remember, 2 – Understand, 3 – Apply, 4 – Analyse, 5 – Evaluate, 6 – Create)
- Course Outcomes
  - CO2 - Understand the executable formats, Windows internals, and APIs.
  - CO3 - Apply techniques and concepts to unpack, extract, and decrypt malware.
  - CO4 - Comprehend reverse-engineering of malware and anti-malware analysis techniques.

Q. No	Question	M	CO	BL
1.	You have encountered a suspected metamorphic malware file that changes its code structure with each execution, making traditional signature-based detection ineffective. How would you use a combination of static and dynamic analysis techniques to analyze this metamorphic malware? What challenges might you face, and how would you overcome them?	10	CO2	B 3
2.	Your organization has detected anomalous behavior suggesting a fileless malware attack. There are no suspicious files on disk, but systems are exhibiting unusual network activity and process behavior. How would you use dynamic analysis tools, particularly those from Sysinternals, to detect and analyze this fileless malware? What specific indicators would you look for, and how would you differentiate this from normal system behavior?	10	CO2	B 3
3.	You have identified a piece of malware that requires a password to execute its payload. The password isn't hardcoded in the binary. How would you go about identifying this password?	10	CO4	B 4
4.	You are examining an Android APK file suspected of being malicious. During static analysis, you notice heavy obfuscation and an unusually large number of permissions being requested. What steps would you take to determine if this is indeed a malicious app, and what type of malware might it be?	10	CO4	B 4
5.	A cybersecurity firm has detected a potential watering hole attack targeting websites frequently visited by employees in the aerospace industry. They've asked you to analyze one of the suspected compromised sites. Describe your approach to investigating this potential watering hole attack. What specific indicators would you look for, and how would you determine if the site has been compromised to serve targeted malware to specific visitors?	10	CO3	B 5

****