VIT
Vellore Institute of Technology

REG.NO.:

SLOT: C2

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING
CONTINUOUS ASSESSMENT TEST - II
FALL SEMESTER 2025-2026

Programme Name & Branch	: B.TECH – CSE (IS)
Course Code and Course Name	: Malware Analysis - BCSE321L
Faculty Name(s)	: Dr. Jayakumar S, Dr. Kathiravan S
Class Number(s)	: VL2025260101468, VL2025260101466
Exam Duration	: 90 minutes

Maximum Marks: 50

Q.No	Question	Max Marks	CO	BL
1.	You are part of a development team working on a low-level device driver for a custom hardware component. During testing, the system crashes intermittently without providing clear logs. Your team must decide whether to use kernel-mode or user-mode debugging to diagnose the issue. Which debugging mode is more appropriate in this scenario? Justify your answer by comparing kernel-mode and user-mode debugging in terms of access level, system stability, and associated risks.	10	CO 2	BL 4
2.	A company provides you with a suspicious file and asks you to run it in a malware sandbox for dynamic analysis. Describe how you would monitor the behavior of the file inside the sandbox and highlight the indicators that would confirm the file as malicious.	10	CO 3	BL 3
3.	During a forensic investigation of a compromised server, you discover an unfamiliar binary that appears to subvert authentication routines. Describe the systematic steps you would undertake to emulate and analyse the authentication bypass within a controlled environment, in order to understand the malware's behaviour. How might this process contribute to strengthening defensive measures against similar attacks in the future?	10	CO 3	BL 4
4.	A university's research laboratory has detected a network worm propagating by exploiting weak authentication mechanisms across internal systems. As a member of the malware analysis team, outline a systematic approach to reverse-engineer the worm's propagation logic within a controlled sandbox environment. Your response should detail the tools, techniques, and safety protocols involved in reconstructing its behaviour. Critically assess how the insights gained from this analysis could inform the design of robust countermeasures, including authentication hardening and network segmentation strategies.	10	CO 4	BL 3
5.	A financial company's employees report that opening a seemingly harmless PDF invoice triggers abnormal system behavior. Initial checks reveal the PDF has an unusually large number of embedded objects and compressed streams. As a malware analyst, explain how you would dissect the document structure to reveal hidden malicious code, and which vulnerabilities attackers are likely exploiting.	10	CO 4	BL 4

****