REG.NO.:

SLOT: C1

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

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

Programme Name & Branch	**: B.Tech. and Computer Science and Engineering**
Course Code and Course Name	**: BCSE321L and Malware Analysis**
Faculty Name(s)	**: Dr. JAYAKUMAR S and Dr. KATHIRAVAN S**
Class Number(s)	**: VL2025260101464 and VL2025260101463**
Date of Examination	**: 19.08.2025**
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:

CO 1. Possess the skills to carry out static and dynamic malware analysis on various malware samples.

CO 3. Apply techniques and concepts to unpack, extract, and decrypt malware.

Q. No	Question	M	CO	BL
1.	Describe the intent behind threat actors' use of malware, explain the typical methods of malware distribution, and outline the common types of malware based on their targeting approaches.	10	CO1	BL1
2.	As a cybersecurity analyst investigating a suspicious executable using BinText, which key features would you use to extract readable strings, and how would you interpret potentially suspicious content? Additionally, what are the main strengths and limitations of BinText when used for static malware analysis?	10	CO1	BL3
3.	As a malware analyst investigating a suspicious DLL—flagged during analysis of unexplained application crashes—using FileAlyzer, which specific features would you employ to determine whether the file exhibits malicious characteristics and which static artefacts or behavioural indicators would most strongly support that assessment?	10	CO1	BL3
4.	Discuss in detail how the key features of PEiD can be used in malware analysis to identify packers, cryptors, or compilers within a suspicious executable. Explain the significance of these detections and how they inform and support the broader malware investigation process.	10	CO3	BL2
5.	As part of a cybersecurity team in a start-up, how would you compare the advantages and disadvantages of using local versus cloud-based (online) malware sandboxing environments, and what key factors should be considered when selecting the most appropriate sandboxing strategy for the organisation?	10	CO3	BL1

****