REG.NO.: 21BCI0046

VIT

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
WINTER SEMESTER 2024-2025

SLOT: D2

Programme Name & Branch : **B.Tech & CSE**
Course Code and Course Name : **BCSE321L and Malware Analysis**
Faculty Name : **Kathiravan S**
Class Number : **VL2024250501660**
Date of Examination : **30.01.2025**
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
  CO1: Possess the skills to carry out static and dynamic malware analysis on various malware samples.
  CO2: Understand the executable formats, Windows internals, and APIs

Q. No	Question	M	CO	BL
1.	How would you classify a polymorphic malware strain used to create a large scale botnet in terms of taxonomy? Discuss the potential risks posed by such a botnet and suggest strategies to disrupt or dismantle it.	10	1	2
2.	How can a manufacturing company's software department use its knowledge of the Portable Executable (PE) file format to quickly assess the potential threat posed by an executable file suspected of being malware?	10	1	2
3.	How can a cybersecurity incident response team use ProcMon and ProcExplorer to track and analyse malware behaviour? Discuss the key indicators of compromise (IOCs) identified through process monitoring and exploration.	10	2	2
4.	In a start-up e-commerce company, a cybersecurity team was analysing the efficacy of local and online malware sandboxing methods. As a member of the team, compare and analyse the benefits and drawbacks of using an online sandbox service versus a local sandbox environment for executing malware samples. How should the team choose the best sandboxing strategy for this e-commerce company?	10	2	4
5.	Consider a scenario in which your web application is infected by packed and obfuscated malware. Discuss the key features of the PEiD tool, along with the merits and demerits of using this tool to analyse packed and obfuscated malware.	10	1	3