REG.NO.: 21BCB0[illegible]

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

School of Computer Science and Engineering
CONTINUOUS ASSESSMENT TEST - II
WINTER SEMESTER 2024-2025

SLOT: D2

---

rogramme Name & Branch : B.Tech & CSE
ourse Code and Course Name : BCSE321L and Malware Analysis
aculty Name : Kathiravan S
lass Number : VL2024250501660
ate of Examination : 19.03.2025
xam Duration : 90 minutes **Maximum Marks: 50**

eneral 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.
  CO4: Comprehend reverse-engineering of malware and anti-malware analysis techniques.

Q. No	Question	M	CO	BL
1.	You are tasked with analysing malware suspected of operating at both the user and kernel levels, manipulating system processes and kernel memory. How would you approach debugging this malware? Compare the advantages and limitations of kernel-mode and user-mode debugging, and outline the tools and techniques you would use for each.	10	1	4
2.	As a threat intelligence analyst, you have identified a potentially malicious DLL responsible for unauthorized access and suspicious network activity. How would you analyse this DLL in a sandbox environment? Outline the steps, tools, and techniques you would use to monitor its behaviour on both the system and the network.	10	1	3
3.	You are analysing malware suspected of stealing passwords. Upon discovering encrypted password storage, how would you go about extracting and decrypting the passwords? Outline the tools and techniques you would use to assess the malware's impact.	10	3	4
4.	You have encountered a suspicious binary, "winlottery.exe," which establishes encrypted communication with a remote server. You suspect that the encryption key is dynamically generated by an obfuscated function at runtime. Using OllyDbg, how would you reverse-engineer the executable to locate the function responsible for generating the encryption key and extract it, without access to the source code?	10	4	4
5.	You are tasked with assessing the security of a PDF document suspected of containing exploits. How would you identify vulnerabilities within the document, and which tools and techniques would you use to detect potential malicious scripts or payloads?	10	1	4