VIT

Vellore Institute of Technology

School of Computer Science Engineering

Fall Semester 2024-2025

RE- Continuous Assessment Test – I

Programme Name & Branch: B.TECH – CSE (IS) **Slot : A1, A2**

Course Name & code: Malware Analysis - BCSE321L

Exam Duration: 90 Min. **Maximum Marks: 50**

Q.No.	Question	Max Marks
1.	A security analyst discovers a suspicious executable that appears to have a much smaller file size than expected for its functionality. Upon initial analysis, the file's entropy is unusually high. What might these observations indicate, and how should the analyst proceed with further investigation? What are all the recommended tools that can be utilized for this scenario?	10
2.	An incident response team has been called to investigate a suspected malware infection on a critical server. The team suspects the malware may be employing anti-debugging techniques. What steps should the team take to confirm the presence of malware and analyze its behavior, while mitigating the risks posed by anti-debugging measures?	10
3.	A malware analyst is investigating a piece of malware that appears to be targeting both 32-bit and 64-bit systems. The analyst wants to understand how the malware's behavior differs between these architectures. How can the analyst leverage their knowledge of x86 and x86_64 assembly to compare the malware's functionality across different architectures?	10
4.	A security researcher has discovered a new variant of a known malware family. The researcher wants to understand how this variant differs from previous versions and what new capabilities it might have. How can the researcher use static analysis tools to compare the new variant with known samples?	10
5.	An incident response team has discovered a potential malware sample on a compromised system. The team wants to understand the malware's behavior without risking further infection. What sandboxing techniques can the team employ to safely analyze the sample?	10