U/K/TY

Reg. No: 22BCJ0189

Final Assessment Test – November 2025

VIT
Vellore Institute of Technology

Course: BCSE321L - Malware Analysis

Class NBR(s): 1463/1464

Slot: C1

Time: Three Hours

Max. Marks: 100

- KEEPING MOBILE PHONE/ANY ELECTRONIC GADGETS, EVEN IN 'OFF' POSITION IS TREATED AS EXAM MALPRACTICE
- DON'T WRITE ANYTHING ON THE QUESTION PAPER

COs	CO Statements
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.
CO3	Apply techniques and concepts to unpack, extract, and decrypt malware.
CO4	Comprehend reverse-engineering of malware and anti-malware analysis techniques.
CO5	Achieve proficiency with industry-standard malware analysis tools.

BL – Blooms Taxonomy Level (1 – Remember, 2 – Understand, 3 – Apply, 4 – Analyse, 5 – Evaluate, 6 – Create)

Answer ALL Questions

(10 X 10 = 100 Marks)

1.	A suspicious executable has been observed spawning multiple child processes and modifying registry keys associated with persistence. Using Process Monitor and Process Explorer, outline a detailed step-by-step approach to investigating this behaviour. Your response should include identification of the parent process and its integrity level, tracing relevant registry modifications with appropriate filters, and determining whether any injected threads or DLLs are present in the child processes. Justify your choice of specific features or views within each tool throughout the investigation.	CO1	BL5
2.	Using OllyDbg, explain methods for identifying and bypassing a basic software-protection mechanism, such as a hard-coded serial-key check. Your answer should outline the key steps, specify the relevant features of OllyDbg, and describe considerations for safe and responsible analysis.	CO1	BL4
3.	Malware authors frequently exploit different levels of abstraction within computing systems to evade detection and complicate analysis. Discuss malware operation across at least three distinct abstraction layers, providing one concrete example for each selected layer. Explain the influence of these design choices on detection strategies and the limitations they impose on both static and dynamic analysis tools.	CO1	BL4
4.	Malware analysts frequently rely on file signature analysis to identify and classify malicious binaries. Explain the use of file signatures in detecting file type spoofing and polymorphic malware. Justify your answer with examples involving mismatched headers and modified Portable Executable (PE) structures, and discuss the limitations of signature-based detection within contemporary threat landscapes.	CO1	BL4

5.	Compare and contrast kernel-mode and user-mode debugging in terms of their operational scope, typical use cases, and associated risks. Provide an example where kernel-mode debugging is essential and another where user-mode debugging is more appropriate.	CO2	BL4
6.	Explain the ways in which malicious dynamic-link libraries (DLLs) may be used to achieve code execution or persistence in a Windows environment. Discuss two common DLL-based techniques employed by malware, and outline methods an analyst might employ to detect or investigate such behaviour.	CO2	BL4
7.	You are tasked with analysing a suspicious Android Package Kit (APK) file suspected of containing Trojan functionality. Outline the key steps required to identify embedded malicious behaviours, incorporating both static and dynamic analysis techniques. Additionally, explain the differences between these steps and conventional virus analysis processes performed on Windows platforms.	CO4	BL4
8.	You are investigating a website suspected of hosting phishing content. Describe the key indicators that may suggest malicious intent, and explain the ways in which tools such as browser developer consoles, network monitors, and threat intelligence platforms assist in confirming the site's behaviour.	CO3	BL4
9.a)	Briefly explain the impact of opaque predicates on the static disassembly of malicious code. Provide an example of an opaque predicate and describe its effect on disassembly tools.	CO4	BL2
	OR		
9.b)	What is shellcode, and why is it often encoded or obfuscated in malicious payloads? Briefly describe a method for detecting or analysing shellcode in a suspicious binary.	CO4	BL2
10.a)	Explain the concepts of sandboxing and code signing in iOS security. Discuss in detail the mechanisms by which each protects the operating system, and illustrate your answer with relevant examples demonstrating the restriction of malicious applications or unauthorised code.	CO5	BL2
	OR		
10.b)	Describe the common types of malware found on handheld devices. Additionally, explain three common methods that attackers use to exploit handheld devices and briefly outline a simple technique for analysing malware on a smartphone.	CO5	BL2

⇔⇔⇔ U/K/TY ⇔⇔⇔