

Enrollment No./Seat No.:

GUJARAT TECHNOLOGICAL UNIVERSITY
Bachelor of Engineering - SEMESTER - V EXAMINATION - WINTER 2025

Subject Code: 3154803

Date: 21-11-2025

Subject Name: Malware Analysis

Time: 10:30 AM TO 01:00 PM

Total Marks: 70

Instructions

- 1. Attempt all questions.**
- 2. Make suitable assumptions wherever necessary.**
- 3. Figures to the right indicate full marks.**
- 4. Simple and non-programmable scientific calculators are allowed.**

	Marks
Q.1 (a) Define malware and explain its key characteristics.	03
(b) Explain how dynamic analysis differs from static analysis.	04
(c) Demonstrate steps to perform static analysis on a malware sample.	07
Q.2 (a) What is virtualization and why is it used in malware analysis?	03
(b) Illustrate the role of system monitoring tools in malware analysis.	04
(c) Describe step-by-step procedure to set up a safe malware analysis lab using VirtualBox.	07
OR	
(c) Explain configuration of a malware analysis sandbox using VMware Player and outline key security precautions.	07
Q.3 (a) Define PE Header and its role in malware analysis.	03
(b) Discuss the purpose and setup of a safe malware analysis lab.	04
(c) Perform static analysis on a malware sample and describe each stage with tools used.	07
OR	
(a) Write short note on anti-virus scanning and hash matching.	03
(b) Explain persistence mechanisms used by malware.	04
(c) Explain method to identify file obfuscation or packing during static analysis with example and detection tools.	07
Q.4 (a) What is process injection?	03
(b) Describe metamorphic malware with an example.	04
(c) Demonstrate procedure to conduct dynamic analysis using Process Monitor and Wireshark.	07
OR	
(a) Define polymorphic malware.	03

- (b) Explain the function of a backdoor and give an example. 04
- (c) Explain steps to perform registry and file-system monitoring during malware execution with results interpretation. 07
- Q.5** (a) What is the MITRE ATT&CK framework? 03
- (b) How does AI impact modern malware detection? 04
- (c) Apply process-injection detection using Sysinternals tools and explain findings. 07
- OR**
- (a) Define a RAT (Remote Access Trojan)? 03
- (b) Discuss ransomware behavior and mitigation techniques. 04
- (c) Explain and demonstrate persistence mechanisms used by malware to maintain access in Windows systems. 07
