QP Code: RA21BTECH804 | Reg. No | | | | | | | | | | | AR 21

Gandhi Institute of Engineering and Technology University, Odisha, Gunupur
(GIET University)

B. Tech (Eighth Semester - Regular) Examinations, April – 2025

21BCSPE48001 – Malware Analysis

(CSE)

Time: 3 hrs | Maximum: 70 Marks

Answer ALL questions

(The figures in the right hand margin indicate marks)

PART – A **(2 x 5 = 10 Marks)**

		CO #	Blooms Level
Q.1.	Answer ***ALL*** questions		
a.	Define malware analysis and its primary goals.	CO1	K1
b.	What is the role of sandboxes in malware analysis?	CO2	K2
c.	How does IDA support processor module architecture?	CO3	K2
d.	Explain the purpose of antivirus scanning in malware analysis.	CO4	K4
e.	What are the major threats in the Android operating system?	CO1	K1

PART – B **(15 x 4 = 60 Marks)**

	Answer ***all*** the questions	Marks	CO #	Blooms Level
2. a.	Explain the different types of malware with real-world examples.	8	CO1	K2
b.	What are the techniques used for analyzing packed files?	7	CO1	K1
	(OR)			
c.	How can PEview and Dependency Walker assist in reverse engineering malware? Discuss in detail.	8	CO1	K1
d.	Explain how packet sniffing with Wireshark can be used to detect malware.	7	CO1	K2
3.a.	Explain in brief how reverse engineering helps in malware analysis.	8	CO2	K2
b.	Explain the x86 architecture and its significance in recognizing C code constructs in assembly.	7	CO2	K2
	(OR)			
c.	Describe the process of recognizing data structures in disassembly.	8	CO2	K2
d.	Discuss the role of IDA Pro in advanced malware reverse engineering.	7	CO2	K2
4.a.	How can C++ reverse engineering techniques help in malware analysis?	8	CO3	K1
b.	Describe the process of setting up a virtual machine for malware analysis.	7	CO3	K2
	(OR)			
c.	Explain how function calls and cross-references help in reverse engineering malware.	8	CO3	K2
d.	Discuss the role of process monitoring tools in malware analysis.	7	CO3	K2
5.a.	Describe how IDA scripting can be used to automate malware analysis.	8	CO4	K2
b.	Explain the role of malware threats, hoaxes, and taxonomy in cybersecurity	7	CO4	K2
	(OR)			
c.	Discuss how plug-ins can extend IDA's functionality in malware analysis.	8	CO4	K2
d.	Compare various open-source tools available for malware analysis.	7	CO4	K2

--- End of Paper ---