Reg. No. : | | | | | | | | | | | | |

Question Paper Code:UE109

B.E./B.Tech. DEGREE EXAMINATION, APRIL/MAY 2025

Professional Elective

21ADV109- MALWARE ANALYTICS

Artificial Intelligence and Data Science

(Regulations 2021)

Duration: Three hours | Maximum: 100 Marks

Answer ALL Questions

PART A - (10 x 2 = 20 Marks)

1.	Distinguish between Software attacks and Hardware attacks.	CO1- U
2.	Explain about Security Models	CO1- U
3.	What is the role of control flow analysis in static analysis? How does it help in understanding the execution path of a program?	CO1- U
4.	What are abstract interpretation and write its role in static analysis?	CO1- U
5.	Explain how dynamic fault localization helps to identify the location of defects in a program.	CO1- U
6.	How do dynamic analysis techniques like program slicing and failure-induced execution tracing aid in narrowing down fault location?	CO1- U
7.	What are the examples of Malware in Action?	CO1- U
8.	Define a malware.	CO1- U
9.	What is Android malware?	CO1- U
10.	Name two types of Android malware	CO1- U

PART – B (5 x 16= 80 Marks)

11.	(a)	Explain how malware analysis can help in identifying Indicators of Compromise (IOCs) for enterprise network protection.	CO2- App	(16)
		Or		
	(b)	How would you safely execute and monitor a malware sample in a virtual machine for dynamic analysis?	CO2- App	(16)

12.	(a)	Describe the process of identifying obfuscation in Android malware using static analysis techniques. What are the common methods of obfuscation, and how can static analysis tools help in detecting and analyzing obfuscated code?	CO1- U	(16)
		Or		
	(b)	How does static analysis help in identifying vulnerabilities in Android malware? Discuss the process of detecting security weaknesses such as privilege escalation, improper API usage, and unsafe data handling. What are the key indicators you would look for during static analysis?	CO1- U	(16)
13.	(a)	Apply the techniques of dynamic analysis on a suspected Android malware sample. Explain the tools and methodologies you would use to identify its evasive or polymorphic behaviors and the steps to mitigate the risks associated with such malware	CO2- App	(16)
		Or		
	(b)	Apply dynamic analysis techniques to investigate how Android malware interacts with system resources such as storage, camera, and GPS. Identify potential risks to user privacy and suggest effective countermeasures to reduce exposure to such risks	CO2- App	(16)
14.	(a)	Explain how malware functions on Android devices, including the different types of malware and their methods of execution. Discuss the potential risks they pose to users.	CO1- U	(16)
		Or		
	(b)	Describe the role of Android app permissions in malware functionality. How do malicious apps exploit permissions to perform harmful actions on users' devices?	CO1- U	(16)
15.	(a)	Explain the concept of Android ransomware and how it compromises user data. Discuss the key stages of a ransomware attack on Android devices.	CO1- U	(16)
		Or		
	(b)	Describe the different types of Android spyware and how they can compromise user privacy. What steps should be taken to protect user data?	CO1- U	(16)