Roll No.												

RESIDENCY UNIVERSITY

GAIN MORE KNOWLEDGE
REACH GREATER HEIGHTS

BENGALURU

End - Term Examinations – May / June 2026

Date: 27-05-2026 **Time:** 01:00pm – 04:00pm

School: SOCSE	**Program:** B.Tech CCS	
Course Code : CCS2509	**Course Name:** Malware Analysis	
Semester: VI	**Max Marks**: 100	**Weightage**: 50%

CO - Levels	**CO1**	**CO2**	**CO3**	**CO4**	**CO5**
Marks	**25**	**25**	**25**	**25**	

Instructions:

(i) Read all questions carefully and answer accordingly.

(ii) Do not write anything on the question paper other than roll number.

Part A

Answer ALL the Questions. Each question carries 2marks. **10Q x 2M=20M**

1.	Define 'Malware' and list its primary goals during an attack.	**2 Marks**	**L1**	**CO1**
2.	What is a 'Logic Bomb' and how does it differ from a standard virus?	**2 Marks**	**L1**	**CO1**
3.	Explain the difference between a Worm and a Trojan Horse in terms of self-replication.	**2 Marks**	**L2**	**CO1**
4.	Contrast Static Analysis with Dynamic Analysis. When would you prefer one over the other?	**2 Marks**	**L2**	**CO1**
5.	Using OS security concepts, explain how a piece of malware might attempt to bypass User Account Control (UAC).	**2 Marks**	**L3**	**CO1**
6.	Identify 3 advantages of assembly level debuggers.	**2 Marks**	**L1**	**CO3**
7.	List two primary functions of 'Process Monitor' (ProcMon) during dynamic analysis	**2 Marks**	**L1**	**CO3**

8.	Explain why iNetSim is preferred over a real internet connection during malware analysis.	**2 Marks**	**L2**	**CO3**
9.	Describe how Wireshark helps in identifying a malware's Command and Control (C2) server.	**2 Marks**	**L2**	**CO3**
10.	Review the process of Trace Analysis in brief.	**2 Marks**	**L3**	**CO3**

Part B

Answer the Questions. **Total Marks 80M**

11.	**a.**	Define the role of OS security in malware analysis..	**2**	**L1**	**CO1**
	b.	Describe Malware evolution timeline.	**4**	**L5**	**CO1**
	c.	Write a short note on classification of malware threat levels.	**4**	**L3**	**CO1**
		Or			
12.	**a.**	Define dynamic analysis.	**2**	**L1**	**CO1**
	b.	Describe Role Based Access Control and its importance.	**4**	**L5**	**CO1**
	c.	Interpret the differences between Rootkit, Virus and Botnet.	**4**	**L3**	**CO1**

13.	**a.**	Analyse the importance of cryptographic hashing in static analysis.	**4**	**L4**	**CO2**
	b.	Define the role of malware fingerprinting in static analysis.	**3**	**L1**	**CO2**
	c.	Explain the concept of CFG analysis and state three tools.	**3**	**L3**	**CO2**
		Or			
14.	**a.**	Analyse the importance of decompilation of Malware code.	**4**	**L4**	**CO2**
	b.	Recall the steps of analysing packaged malware files.	**3**	**L1**	**CO2**
	c.	Interpret the key relations between antivirus scanning and threat intelligence.	**3**	**L3**	**CO2**

15.	**a.**	Illustrate any sandbox architecture with a neat labeled diagram.	**5**	**L3**	**CO3**
	b.	List the key disadvantages of using a sandbox.	**2**	**L1**	**CO3**
	c.	Discuss the importance of stack analysis.	**3**	**L2**	**CO3**
		Or			
16.	**a.**	Sketch the components of a packet sniffing tool with proper labels.	**5**	**L3**	**CO3**
	b.	List the importance of using non destructive filters.	**2**	**L1**	**CO3**
	c.	Describe the TCP/IP headers when it transforms data.	**3**	**L2**	**CO3**

17.	**a.**	Explain the concept of a "Credential Stealer" in the context of malware and describe two common ways it can be implemented to bypass standard authentication.	**3**	**L2**	**CO4**
	b.	Define "Process Injection" and list steps of how it is done.	**4**	**L1**	**CO4**
	c.	Demonstrate the steps of Privilege Escalation.	**3**	**L3**	**CO4**
		Or			
18.	**a.**	Differentiate between a "Packed Malware Signature" and a "Metamorphic Malware Signature" in terms of how they appear to a static scanner.	**3**	**L2**	**CO4**
	b.	List the primary components or characteristics that define a "Polymorphic Malware" engine.	**3**	**L1**	**CO4**
	c.	Demonstrate the steps of how Process Replacement takes place..	**4**	**L3**	**CO4**

19.	**a.**	Explain the concept of "Hook Injection" and describe the logical flow it.	**10**	**L2**	**CO4**
	b.	Demonstrate the evolution of Malwares.	**5**	**L3**	**CO1**
	c.	Define malware behaviour and list 3 common IoCs.	**5**	**L1**	**CO4**
		Or			
20.	**a.**	Compare "Process Replacement" (Process Hollowing) with "Process Injection". Explain how each technique manages to execute malicious code within a legitimate process's memory space.	**10**	**L2**	**CO4**
	b.	Interpret the relation between Rootkits and Advanced Persistent Threats.	**5**	**L3**	**CO1**
	c.	Define how polymorphic engines work.	**5**	**L1**	**CO4**

21.	**a.**	Consider the following subroutine
		`section .text`
		`global is_odd`
		
		`is_odd:`
		`  ; Check least significant bit`
		`  test eax, 1  ; AND with 1 (checks LSB)`
		
		`  jz even  ; if zero → even`
		
		`  ; Odd case`
		`  mov eax, 1`
		`  ret`
		
		`even:`
		`  mov eax, 0`
		`  ret`
		
		Illustrate the formal CFG for this given subroutine that checks if a number is odd or even.
			7	**L3**	**CO2**

	b.	Compose the High Level FIRA code for this subroutine.	**8**	**L5**	**CO2**
	c.	Differentiate between Kernel Mode and User Mode debugging.	**5**	**L4**	**CO3**
Or					

22.	**a.**	Consider the following subroutine to calculate the gcd of a number:
		`section .text`
		`global gcd`
		
		`gcd:`
		`  ; Handle case when b == 0`
		`  cmp ebx, 0`
		`  je done`
		
		`gcd_loop:`
		`  mov edx, 0  ; clear high part for division`
		`  div ebx  ; EAX / EBX → quotient in EAX, remainder in EDX`
		
		`  mov eax, ebx  ; a = b`
		`  mov ebx, edx  ; b = remainder`
		
		`  cmp ebx, 0`
		`  jne gcd_loop`
		
		`done:`
		`  ; result already in EAX`
		`  ret`
		
		Illustrate the formal CFG of the given subroutine.
			7	**L3**	**CO2**

	b.	Compose the High Level FIRA code for the given subroutine.	**8**	**L5**	**CO2**
	c.	Differentiate between Source Level and Assembly Level Debuggers..	**5**	**L4**	**CO3**