Roll No: | | | | | | | | | | | |

PRESIDENCY UNIVERSITY

GAIN MORE KNOWLEDGE
REACH GREATER HEIGHTS

Presidency University Act, 2013 of the Karnataka Act No. 41 of 2013 | Established under Section 2(f) of UGC Act, 1956
Approved by AICTE, New Delhi | Approved By BCI
Bengaluru

Mid Term Examinations - October 2026

Date: 05/10/2026 **Time:** 09:30 AM - 11:00 AM

Course Code: CCS2509 **Course Name:** Malware Analysis

Semester: Fifth Semester **Max. Marks:** 50 **Weightage:** 50%

CO - Levels	CO1	CO2	CO3
Marks	34	46	10

PART A: Answer Following Questions. 10 M

Q.N.	Questions	M	CO	BT
1	Define malware. Give two examples.	2	CO1	BT1
2	What is a bot or botnet? State one malicious use.	2	CO1	BT1
3	What is heuristic analysis in antivirus software?	2	CO2	BT1
4	Mention any two advantages of using a VM for malware analysis.	2	CO2	BT1
5	Differentiate between 32-bit and 64-bit malware.	2	CO2	BT1

PART B : Answer Any 1 Following Questions. 10 M

Q.N.	Questions	M	CO	BT
6	What makes a rootkit particularly difficult to detect and remove?	10	CO1	BT2
7	How does a Trojan differ from a virus or worm in how it spreads?	10	CO1	BT3

PART C: Answer Any 1 Following Questions. 10 M

Q.N.	Questions	M	CO	BT
8	A university employee receives an email containing an attachment named Salary_Increment.exe. Believing it to be a genuine document, the employee opens it. The program secretly installs malicious software, collects login credentials, and sends the stolen information to a remote attacker. Based on this scenario, identify the type of malicious software involved and explain its method of infection, objective, and impact.	10	CO3	BT1
9	Explain the three pillars of OS security. How do they help in protecting systems from malware?	10	CO1	BT1

PART D: Answer Any 1 Following Questions. 10 M

Q.N.	Questions	M	CO	BT
10	Explain the Portable Executable (PE) file format. Describe its major components and explain its importance in static malware analysis.	10	CO2	BT2

11	A cybersecurity analyst receives a suspicious .exe file suspected to contain malware. To prevent the malware from affecting the organization's network, the analyst decides to examine it inside a Virtual Machine (VM). **Question**: Apply malware analysis techniques in a Virtual Machine to safely investigate the suspicious executable. Explain the steps you would follow, including VM isolation, snapshot creation, malware execution, monitoring, network configuration, and evidence collection.	10	CO2	BT4

PART E: Answer Any 1 Following Questions. 10 M				
Q.N.	**Questions**	**M**	**CO**	**BT**
12	Why does x86 malware still run on modern computer systems? Explain the compatibility mechanisms and forensic significance of x86 malware.	10	CO2	BT3
13	Explain how malware evades antivirus detection with a suitable example.	10	CO2	BT2