Roll No.												

PRESIDENCY UNIVERSITY

BENGALURU

Mid - Term Examinations – MARCH 2026

Date: 10 – 03- 2026 **Time:** 02:00pm – 03:30pm

School: SOCSE	**Program:** B.Tech	
Course Code: CCS2506	**Course Name:** Intrusion Detection and Prevention System	
Semester: VI	**Max Marks**: 50	**Weightage**: 25%

CO - Levels	**CO1**	**CO2**	**CO3**	**CO4**	**CO5**
Marks	**24**	**26**	**-**	**-**	**-**

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. **5Q x 2M=10M**

1	Explain the significance of baseline and threshold behavior in anomaly-based detection systems.	**2 Marks**	**L2**	**CO1**
2	Explain why false positives are a critical challenge in IDS.	**2 Marks**	**L2**	**CO1**
3	Distinguish exploit-facing and vulnerability-facing detection approaches.	**2 Marks**	**L2**	**CO2**
4	Explain why multi-tier architecture is more efficient than single-tier architecture in IDS/IPS.	**2 Marks**	**L2**	**CO2**
5	Differentiate credential-based and non-credential vulnerability assessment in terms of depth of analysis.	**2 Marks**	**L2**	**CO2**

Part B

Answer the Questions. **Total Marks 40M**

6.	**a.**	Illustrate and compare the working mechanisms of HIDS and NIDS using a suitable diagram.	**10 Marks**	**L2**	**CO1**
		Or			
7.	**a.**	Describe the types of IDS based on source and represent their working using an appropriate diagram.	**10 Marks**	**L2**	**CO1**

8.	**a.**	Illustrate the classification of IDS based on detection approaches using a neat diagram.	**10 Marks**	**L2**	**CO1**
		Or			
9.	**a.**	Compare the different IDS detection approaches using suitable parameters.	**10 Marks**	**L2**	**CO1**

10.	**a.**	Explain Diamond Model framework based on structure, purpose, and applicability.	**10 Marks**	**L2**	**CO2**
		Or			
11.	**a.**	Compare single-tier, multi-tier and peer-to-peer IDS/IPS architectures along with their advantages and disadvantages.	**10 Marks**	**L2**	**CO2**

12.	**a.**	Explain the analysis process of rule-based detection and anomaly-based detection with reference to the anatomy of intrusion analysis.	**10 Marks**	**L2**	**CO2**
		Or			
13.	**a.**	Describe the working of protocol-based IDS and discuss its major types with examples of Kerberos, RADIUS, and TACACS+.	**10 Marks**	**L2**	**CO2**