Roll No.												

PRESIDENCY UNIVERSITY

BENGALURU

School of Computer Science and Engineering

Mid - Term Examinations - October 2025

Semester: V	**Date**: 09-10-2025
Course Code: CCS2506	**Time**: 02:00pm – 03:30pm
Course Name: Intrusion Detection & Prevention System	**Max Marks**: 50
Program: ISE, CAI, CCS	**Weightage**: 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.		**2Mx5Q=10M**		
1	What is meant by Asymmetric Routing	**2 Marks**	**L1**	**CO1**
2	List down the Cons of IDPS	**2 Marks**	**L1**	**CO1**
3	What is meant by NIDS techniques	**2 Marks**	**L1**	**CO1**
4	List the benefit of Non- Credential Vulnerability Scan	**2 Marks**	**L1**	**CO2**
5	Write the short note about dangers of Honeypots	**2 Marks**	**L1**	**CO2**

Part B

Answer ALL Questions. Each question carries 10 marks.			**4QX10M=40M**		
6	**a.**	Discuss the Profile Based Detection	**5 Marks**	**L2**	**CO1**
	b.	Discuss the variety of security capabilities of IDPS technologies	**5 Marks**	**L2**	**CO1**
		or			
7	**a.**	Explain the Host based IDPS with diagram	**5 Marks**	**L2**	**CO1**
	b.	Explain the Network based IDPS with diagram	**5 Marks**	**L2**	**CO1**

8	**a.**	Assume that You are working as a data science Engineer at KPN company in Dubai that provides an online payment platform. As your team is tasked with building a fraud detection system that can identify suspicious transactions. The goal is to flag any	**10 Marks**	**L3**	**CO1**

		transaction that deviates significantly from normal activity, indicating potential fraud, Question: a. Identify , which Methodology Architecture will be suitable to find the fraud detection b. Draw the Methodology Architecture C.What are steps would you take to implement for this scenario			
		or			
9	**a.**	A OCCR company in Bangalore , has recently installed a new antivirus solution that primarily to identify and block malware. Assume that your working in security team, security team notices that while the antivirus software catches most known threats, it misses some new variants of malware. Question: a. Identify , which Methodology Architecture will be suitable to find the malware b. Draw the Methodology Architecture c. What are steps would you take to implement for this scenario	**10 Marks**	**L3**	**CO1**

10	**a.**	Discuss the Diamond Model of Intrusion with Diagram	**5 Marks**	**L2**	**CO2**
	b.	Explain the components in an IDPS	**5 Marks**	**L2**	**CO2**
		or			
11	**a.**	Discuss the WIPS work and how the Threats Can WIPS defend Against	**5 Marks**	**L2**	**CO2**
	b.	Discuss the Diamond model benefit and feature	**5 Marks**	**L2**	**CO2**

12	**a.**	Explain the Honeypot with diagram	**5 Marks**	**L3**	**CO2**
	b.	Discuss the Credential Vulnerability Scan	**5 Marks**	**L2**	**CO2**
		or			
13	**a.**	Compare the types of architecture model for IDPS	**5 Marks**	**L3**	**CO2**
	b.	Explain the types of Honeypot in detail with examples	**5 Marks**	**L2**	**CO2**