Roll No.												

PRESIDENCY UNIVERSITY

BENGALURU

Mid - Term Examinations – October 2025

Date: 29-10-2025 **Time:** 02.30pm to 04.00pm

School: SOCSE	**Program:** B. Tech Computer Science and Engineering	
Course Code: CSE3145	**Course Name:** Intrusion Detection and Prevention system	
Semester: VII	**Max Marks**:50	**Weightage**:25%

CO - Levels	**CO1**	**CO2**	**CO3**	**CO4**	**CO5**
Marks	**22**	**14**	**14**		

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	Classify the three types of intruders and briefly describe each.	**2 Marks**	**L2**	**CO1**
2	Illustrate how an IPS helps protect against denial-of-service (DoS) attacks.	**2 Marks**	**L3**	**CO2**
3	Apply the concept of intrusion prevention to explain how an IPS stops a hacker from entering a system.	**2 Marks**	**L3**	**CO2**
4	How can combining both credential and non-credential scans improve system safety?	**2 Marks**	**L3**	**CO3**
5	Apply your understanding to show why multi-tier architecture is better for large networks.	**2 Marks**	**L3**	**CO3**

Part B

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

6.	**a.**	Describe the working principle of intrusion analysis by explaining each phase — preprocessing, analysis, response, and refinement — with examples.	**10 Marks**	**L2**	**CO1**
	b.	Explain how internal and external threats can compromise network security and summarize preventive measures to mitigate both.	**10 Marks**	**L2**	**CO1**
		Or			
7.	**a.**	Explain the major pros and cons of IDS and IPS and discuss how they complement each other in protecting an organization.	**10 Marks**	**L2**	**CO1**
	b.	Explain the advantages and limitations of Host-Based and Network-Based information sources in security monitoring.	**10 Marks**	**L2**	**CO1**

8.	**a.**	Apply the working of an Intrusion Prevention System (IPS) to protect an organization from cyberattacks.	**10 Marks**	**L3**	**CO2**
	b.	Apply the concept of multi-tiered architecture to illustrate how sensors, agents, and managers coordinate to detect and prevent a large-scale intrusion in a corporate network.	**10 Marks**	**L3**	**CO3**
		Or			
9.	**a.**	Illustrate how an organization can apply intrusion prevention techniques to reduce both internal and external threats.	**10 Marks**	**L3**	**CO2**
	b.	Analyze how a peer-to-peer architecture could enhance cooperation among firewalls to improve intrusion prevention when no central manager is used.	**10 Marks**	**L3**	**CO3**