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: 06/10/2026 **Time:** 02:00 PM - 03:30 PM

Course Code: CSE3520 **Course Name:** Network Intrusion Detection and Prevention

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

CO - Levels	CO1	CO2	CO3
Marks	48	88	44

PART A: Answer Following Questions. 10 M

Q.N.	Questions	M	CO	BT
1	What is an Intrusion Prevention System (IPS) , Mention any two functions of an IPS.	2	CO1	BT1
2	Differentiate between Network IDS (NIDS) and Protocol-Based IDS (PIDS).	2	CO1	BT2
3	What is credential analysis? How is it different from non-credential analysis?	2	CO2	BT1
4	Differentiate between Misuse Detection and Anomaly Detection.	2	CO3	BT2
5	What are host-based information sources and network-based information sources in IDS?	2	CO3	BT1

PART B : Answer Any 1 Following Questions. 10 M

Q.N.	Questions	M	CO	BT
6	Explain the Intrusion Analysis Model. Describe the different intrusion analysis techniques, types of responses, requirements of a good response, and how responses are mapped to security policies with suitable example.	10	CO2	BT1
7	Explain the architecture of IPS. Describe Network IDS (NIDS), Protocol-Based IDS (PIDS), and Hybrid IDS with their working, main components, advantages, and limitations. Also explain the difference between the response of IDS and IPS.	10	CO2	BT2

PART C: Answer Any 1 Following Questions. 10 M

Q.N.	Questions	M	CO	BT
8	Explain the different types of responses used by an Intrusion Detection and Prevention System. Discuss the requirements of an effective response with suitable examples.	10	CO2	BT2
9	Explain vulnerability analysis, credential analysis, and non-credential analysis in intrusion detection. Describe how each type helps in identifying and preventing security threats.	10	CO3	BT2

PART D: Answer Any 1 Following Questions. 10 M

Q.N.	Questions	M	CO	BT
10	Explain the different information sources used by IDS. Discuss host-based information sources and network-based information sources with suitable examples.	10	CO3	BT2

11	Explain the different information sources used by IDS. Discuss host-based information sources and network-based information sources with suitable examples.	10	CO2	BT3

PART E: Answer Any 1 Following Questions. 10 M				
Q.N.	**Questions**	**M**	**CO**	**BT**
12	Explain the basics of Intrusion Detection and Prevention. Describe IDS and IPS, their main functions, and the difference between them with suitable examples.	10	CO3	BT3
13	Explain the different detection approaches used in IDS: Misuse Detection, Anomaly Detection, Specification-Based Detection, and Hybrid Detection with suitable examples	10	CO3	BT2