Roll No.												

PRESIDENCY UNIVERSITY

BENGALURU

End - Term Examinations – May/June 2026

Date: 18-05-2026 **Time:** 01:00pm – 04:00pm

School: SOCSE	**Program:** B.Tech	
Course Code: CCS2506	**Course Name:** Intrusion Detection and Prevention System	
Semester: VI	**Max Marks**: 100	**Weightage**: 50%

CO - Levels	**CO1**	**CO2**	**CO3**	**CO4**	**CO5**
Marks	**24**	**12**	**14**	**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. **10Q x 2M=20M**

1.	Differentiate between False Positive and False Negative in IDS.	**2 Marks**	**L2**	**CO1**
2.	Identify whether a host-based IDS or a network-based IDS is more suitable for detecting internal threats to data. Justify your answer briefly.	**2 Marks**	**L3**	**CO1**
3.	Define an Intrusion Prevention System (IPS). Mention any 2 preventive actions taken by an IPS.	**2 Marks**	**L1**	**CO2**
4.	Classify the types of intruders.	**2 Marks**	**L2**	**CO3**
5.	Describe the features and functionality of Azure Firewall Premium IDPS.	**2 Marks**	**L2**	**CO3**
6.	Describe the architecture of Zeek (Bro) IDS.	**2 Marks**	**L2**	**CO4**
7.	Explain the three modes of operation of Snort.	**2 Marks**	**L2**	**CO4**
8.	Explain the stages involved in the forensic process.	**2 Marks**	**L2**	**CO5**
9.	Differentiate between policy, standard, and procedure.	**2 Marks**	**L2**	**CO5**
10.	Summarize the importance of chain of custody in digital forensics.	**2 Marks**	**L2**	**CO5**

Part B

Answer the Questions. **Total Marks 80M**

11.	**a.**	Differentiate between Network-based IDS (NIDS) and Host-based IDS (HIDS) in terms of functionality, advantages, and limitations.	**10 Marks**	**L2**	**CO1**
	b.	Analyze different intrusion detection approaches (misuse, anomaly, specification-based, hybrid) and explain their effectiveness in detecting attacks using diagram.	**10 Marks**	**L3**	**CO1**
		Or			
12.	**a.**	Discuss internal and external threats to data in an organization. Explain how host-based IDS and network-based IDS help in detecting these threats.	**10 Marks**	**L2**	**CO1**
	b.	Illustrate the different types of IDS (NIDS, HIDS, PIDS, APIDS, Hybrid IDS) and explain their working in a network environment.	**10 Marks**	**L3**	**CO1**

13.	**a.**	Explain the models for intrusion analysis used in IPS. Describe their components and explain how these models help in detecting and analyzing intrusions.	**10 Marks**	**L2**	**CO2**
	b.	Analyze the differences between credential-based and non-credential-based vulnerability assessments with suitable examples.	**10 Marks**	**L3**	**CO3**
		Or			
14.	**a.**	Explain the analysis schemes used in IPS. Describe the anatomy of intrusion analysis in detail.	**10 Marks**	**L2**	**CO2**
	b.	Analyze how RADIUS and TACACS+ protocols ensure secure authentication, authorization, and accounting.	**10 Marks**	**L3**	**CO3**

15.	**a.**	Illustrate the architecture of Snort IDS and explain each component (sniffer, preprocessor, detection engine, rules, logging) with a neat diagram.	**20 Marks**	**L3**	**CO4**
		Or			
16.	**a.**	Analyze the architecture and working of Zeek (Bro) IDS, explaining how its components contribute to intrusion detection and network monitoring.	**20 Marks**	**L3**	**CO4**

17.	**a.**	Illustrate the steps of creating an IDS/ IPS poliy.	**10 Marks**	**L3**	**CO5**
	b.	Explain the evidence life cycle stages and analyze their importance in maintaining evidence integrity.	**10 Marks**	**L2**	**CO5**
		Or			
18.	**a.**	Demonstrate the application of due care and due diligence in organizational security practices.	**10 Marks**	**L3**	**CO5**
	b.	Explain the different types of laws and standards in IDPS.	**10 Marks**	**L2**	**CO5**