Roll No.												

PRESIDENCY UNIVERSITY

BENGALURU

End - Term Examinations – December 2025

Date: 18 – 12- 2025 **Time:** 01:00pm – 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**: 100	**Weightage**: 50%

CO - Levels	**CO1**	**CO2**	**CO3**	**CO4**	**CO5**
Marks	**24**	**14**	**12**	**26**	**24**

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.	Define Intrusion Detection System (IDS).	**2 Marks**	**L1**	**CO1**
2.	List any three features or capabilities of an IDS.	**2 Marks**	**L1**	**CO1**
3.	Identify the situation where a multi-tiered architecture is preferable over a single-tiered one.	**2 Marks**	**L3**	**CO2**
4.	Demonstrate the use of signature-based detection in preventing a SQL injection attack.	**2 Marks**	**L3**	**CO3**
5.	Apply the policy-based approach of IPS to control unauthorized access in an enterprise network.	**2 Marks**	**L3**	**CO2**
6.	Apply the concept of Dynamic Threat Update (DTU) to explain how AirMagnet maintains up-to-date security posture.	**2 Marks**	**L3**	**CO4**
7.	What is the purpose of the Event Engine in Zeek?	**2 Marks**	**L1**	**CO4**
8.	Apply the principle of 24/7 network monitoring using IBM's IDPS Management tool.	**2 Marks**	**L3**	**CO4**
9.	Apply the concept of evidence acquisition to explain how forensic experts ensure data integrity.	**2 Marks**	**L3**	**CO5**
10.	Illustrate how IDS log analysis can help reconstruct a cyberattack timeline.	**2 Marks**	**L3**	**CO5**

Part B

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

11.	**a.**	Discuss the three classes of intruders and provide real-world examples for each.	**10 Marks**	**L2**	**CO1**
	b.	Explain with examples the difference between internal and external threats.	**10 Marks**	**L2**	**CO1**
		Or			
12.	**a.**	Explain the role of preprocessing and analysis in IDS/IPS functioning.	**10 Marks**	**L2**	**CO1**
	b.	Differentiate between rule-based detection and profile-based (anomaly) detection	**10 Marks**	**L2**	**CO1**

13.	**a.**	Demonstrate how signature-based and anomaly-based detection can work together to minimize false positives.	**10 Marks**	**L3**	**CO2**
	b.	Use vulnerability assessment results to prepare an appropriate intrusion response plan for an organization.	**10 Marks**	**L3**	**CO3**
		Or			
14.	**a.**	Construct a hybrid intrusion detection setup integrating both protocol-based IDs and modern identity frameworks.	**10 Marks**	**L3**	**CO2**
	b.	Apply the Diamond Model of Intrusion Analysis to a ransomware attack and identify each element (adversary, capability, infrastructure, victim).	**10 Marks**	**L3**	**CO3**

15.	**a.**	Demonstrate how Snort can be applied in *Sniffer, Logging,* and *NIDS* modes to protect a campus network.	**10 Marks**	**L3**	**CO4**
	b.	Use NSFocus NGIPS sandboxing to simulate blocking of malicious traffic while maintaining service availability.	**10 Marks**	**L3**	**CO4**
		Or			
16.	**a.**	Illustrate how to execute multiple VLAN configurations in Snort to handle separate subnets using different rule sets.	**10 Marks**	**L3**	**CO4**
	b.	Apply the Zeek scripting interpreter to define a custom policy that logs all FTP connections.	**10 Marks**	**L3**	**CO4**

17.	**a.**	Demonstrate the step-by-step forensic procedure to collect, preserve, and analyze IDS log files for a network breach.	**10 Marks**	**L3**	**CO5**
	b.	Demonstrate how packet capture tools (like Wireshark or Snort) can be used for forensic reconstruction of a cyber incident.	**10 Marks**	**L3**	**CO5**
		Or			
18.	**a.**	Show how business and investigative records can be used together to strengthen digital forensic findings.	**10 Marks**	**L3**	**CO5**
	b.	Apply training and awareness procedures to ensure that employees adhere to IDS/IPS policy requirements.	**10 Marks**	**L3**	**CO5**