GALGOTIAS UNIVERSITY

ADMISSION NUMBER												

School of Computing Science and Engineering

Bachelor of Technology in Computer Science and Engineering
Mid Term Examination - Nov 2023

Duration : 90 Minutes
Max Marks : 50

Sem V - E2UO501B - Intrusion Detection and Prevention System

General Instructions
Answer to the specific question asked
Draw neat, labelled diagrams wherever necessary
Approved data hand books are allowed subject to verification by the Invigilator

1)	A company's intrusion prevention system uses signature-based detection for known attack patterns. It has a database of 10,000 attack signatures. During a network scan, the system identifies 20 matches with these signatures. Determine is the matching rate as a percentage?	K3	(6)
2)	Examine in a network environment to suggest whether a NIPS or a WIPS would be more suitable and explain your choice.	K3	(9)
3)	An organization's intrusion detection system (IDS) claims to have an accuracy rate of 98%, but during a security audit, it is revealed that it missed 40 out of 200 real intrusions in the past year. Calculate the system's true positive rate (sensitivity) and its false negative rate.	K4	(8)
4)	Evaluate the importance of continuous monitoring for the success of an intrusion detection system.	K5	(15)
5)	Develop a policy document outlining the ethical considerations and guidelines for using intrusion detection in an organization.	K6	(12)