GALGOTIAS UNIVERSITY

ADMISSION NUMBER												

School of Computing Science and Engineering

Bachelor of Technology in Computer Science and Engineering
Mid Term Examination - May 2024

Duration : 90 Minutes
Max Marks : 50

Sem VI - R1UC614C - Intrusion Detection and Prevention

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)	Compare and contrast the distinguishing features of a network-based IDS and a host-based IDS.	K2	(2)
2)	List and provide concise explanations of the three primary approaches to intrusion detection.	K1	(3)
3)	Assess the relative significance of Wireless IPS (WIPS) and Network Behavior Analysis (NBA)-based Intrusion Prevention Systems (IPS).	K2	(4)
4)	Compare and contrast the characteristics of Host-based Intrusion Detection Systems (HIDS) and Network-based Intrusion Detection Systems (NIDS). How do they differ in their approach to detecting intrusions?	K2	(6)
5)	A company's intrusion prevention system uses signature-based detection for known attack patterns. It has a database of 5,000 attack signatures. During a network scan, the system identifies 10 matches with these signatures. Determine is the matching rate as a percentage and describe network scan process?	K3	(6)
6)	Examine in a network environment to suggest whether a HIPS or a NIPS would be more suitable and explain your choice.	K3	(9)
7)	An organization's intrusion detection system (IDS) claims to have an accuracy rate of 90%, but during a security audit, it is revealed that it missed 30 out of 100 real intrusions in the past year. Calculate the system's true positive rate (sensitivity) and its false negative rate.	K4	(8)
8)	Analyze the methodologies used in the case studies on research in host-based and network-based intrusion detection systems. Discuss their contributions to the field of cybersecurity.	K4	(12)
	OR		
	Describe ROI in detail and find the Return on investment(ROI) for the first year of an organization, which invests in a new intrusion detection system that costs $20,000 to implement, $8,000 annually for maintenance and the system helps prevent an estimated $150,000 in potential damages each year.	K4	(12)