GALGOTIAS
UNIVERSITY

ADMISSION NUMBER

School of Computing Science and Engineering

Bachelor of Technology in Computer Science and Engineering
Semester End Examination - Jun 2024

Duration : 180 Minutes
Max Marks : 100

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) List three common classifications of computer viruses with example. K1(2)

2) An Intrusion Prevention System (IPS) process cycle consists of four stages: Monitoring, Detection, Analysis, and Prevention. If the time taken for each stage is 5 milliseconds, 10 milliseconds, 8 milliseconds, and 7 milliseconds respectively, what is the total processing time for one complete cycle? K2(4)

3) Calculate the percentage of rules triggered by Snort IDS, given 5000 active rules and 200 triggered during network analysis. K2(6)

4) Apply your understanding of IPS types to recommend the most suitable IPS solution for a large enterprise network with diverse endpoints and multiple wireless access points. K3(9)

5) Develop a coherent network security strategy that incorporates both firewalls and Intrusion Detection Systems (IDS) to deliver holistic protection against diverse cyber threats. Explore the collaborative effectiveness of these two security measures and their combined impact on fortifying the overall defense posture against potential attacks. K3(9)

6) Critically evaluate the case studies on research in host-based and network-based intrusion detection systems, considering the relevance of their findings to contemporary cybersecurity challenges. K5(10)

7) A cybersecurity company offers two intrusion detection solutions. Solution A has an accuracy rate of 90% with a false positive rate of 2%, while Solution B has an accuracy rate of 95% with a false positive rate of 1.5%. If an organization receives 1,000 alerts from Solution A and 600 alerts from Solution B, calculate the expected number of false & positive alerts for each solution. K4(12)

8) Evaluate the effectiveness of existing intrusion detection and prevention strategies in addressing evolving cyber threats, and propose recommendations for enhancing IPS capabilities in anticipation of future challenges. K5(15)

9) Given the following metrics: Total incoming network events: 150,000 events per hour, Legitimate network events: 140,000 events per hour, Malicious events: 10,000 events per hour, Detection Rate: 85%, and False Positive Rate: 3%. Determine the Detectable Malicious Events, Total Alerts Generated by IDS,False Positives & True positive also describe the role of True positive to find the accuracy. K5(15)

10) Create a comprehensive network security strategy integrating firewalls, IDS, and other security measures to safeguard against a range of network threats, considering the specific requirements and characteristics of the network environment. K6(18)