Roll No											

PRESIDENCY UNIVERSITY
BENGALURU

SET-A

SCHOOL OF ENGINEERING
END TERM EXAMINATION – MAY/JUNE 2024

Semester : VI- B.Tech CSE-2021
Course Code : CSE3145
Course Name : Intrusion Detection And Prevention Systems
Program : B.Tech

Date : JUNE 12-2024
Time : 1:00 PM - 4:00 PM
Max Marks :100
Weightage : 50%

Note:
1. **Answer ALL 5 FULL Questions.**
2. **Each Full Question carries 20 Marks**
3. **Scientific and non-programmable calculator are permitted.**
4. **Do not write any information on the question paper other than Roll Number.**

1.a.	Explain zero-day attack, and how does it affect IDS/IPS. **[Knowledge]**	**(CO1)**	**(04 Marks)**
1.b.	Explain the risks associated with social engineering attacks. **[Comprehension]**	**(CO1)**	**(06 Marks)**
1.c.	Explain the complete working of Wireless Intrusion Prevention System. **[Application]**	**(CO1)**	**(10 Marks)**
	or		
2.a.	Explain the three classes of Intruders. **[Knowledge]**	**(CO1)**	**(04 Marks)**
2.b.	Explain the Host-Based IDS with diagram. **[Comprehension]**	**(CO1)**	**(06 Marks)**
2.c.	Elaborate the steps taken by system administrator to support investigation and prosecution. **[Application]**	**(CO1)**	**(10 Marks)**
3.a.	Explain how credential based vulnerability assessment is performed. **[Knowledge]**	**(CO2)**	**(04 Marks)**
3.b.	Explain the anatomy of Intrusion Analysis **[Comprehension]** a) Pre-processing b) Refinement	**(CO2)**	**(06 Marks)**
3.c.	Explain the three general techniques used in Anomaly based Methodology for detecting the attack in the network. **[Application]**	**(CO2)**	**(10 Marks)**
	or		
4.a.	Elaborate the working of WIPS. **[Knowledge]**	**(CO2)**	**(04 Marks)**
4.b.	Explain the three-tiered architecture for IDPS. **[Comprehension]**	**(CO2)**	**(06 Marks)**
4.c.	Explain in detail BRO IDPS with proper diagram. **[Application]**	**(CO2)**	**(10 Marks)**

5.a.	Identify the factors that should be considered in the tool selection and acquisition process for an Intrusion Detection System (IDS)? **[Knowledge]**	**(CO3)**	**(04 Marks)**
5.b.	Compare and contrast Air Magnet Enterprise with Cisco Secure IPS. **[Comprehension]**	**(CO3)**	**(06 Marks)**
5.c.	Explain the importance of maintaining detailed logs and records by IDPS for legal and evidentiary purposes. How can these logs support forensic investigations and legal actions? **[Application]**	**(CO3)**	**(10 Marks)**
	or		
6.a.	Describe how evidentiary issues can impact the effectiveness of Intrusion Detection and Prevention Systems during criminal prosecutions. **[Knowledge]**	**(CO3)**	**(04 Marks)**
6.b.	Explain the primary capabilities of Prelude Intrusion Detection System. How does its hybrid architecture contribute to comprehensive threat detection and correlation? **[Comprehension]**	**(CO3)**	**(06 Marks)**
6.c.	Discuss the significance of legal standards in the implementation of Intrusion Detection and Prevention Systems (IDPS). How do these standards influence the effectiveness, compliance, and overall security posture of organizations? **[Application]**	**(CO3)**	**(10 Marks)**
7.a	Describe the key techniques used for intrusion detection in a network environment? **[Knowledge]**	**(CO4)**	**(04 Marks)**
7.b.	Describe the architecture models typically used for Intrusion Prevention Systems. **[Comprehension]**	**(CO4)**	**(06 Marks)**
7.c	Discuss the need for Intrusion Detection Systems (IDS) in the context of modern cyber security threat What are the different types of IDS, and how do they contribute to a multi-layered security strategy? Provide examples of scenarios where IDS is crucial. **[Application]**	**(CO4)**	**(10 Marks)**
	or		
8.a	Compare Meraki MX Advanced Security Edition with Dark trace Enterprise Immune System. **[Knowledge]**	**(CO4)**	**(04 Marks)**
8.b.	Distinguish between network-based IDS and host-based IDS in terms of visibility? **[Comprehension]**	**(CO4)**	**(06 Marks)**
8c.	Discuss a comprehensive model for intrusion analysis. Include the stages of detection, analysis, and response, and explain how each stage contributes to the overall effectiveness of an intrusion detection/prevention strategy. **[Application]**		
9.a	Define the primary goals of an IPS when handling detected intrusions? **[Knowledge]**	**(CO3)**	**(04 Marks)**
9.b	Explain Non-Credential based Vulnerability Assessment. **[Comprehension]**	**(CO3)**	**(06 Marks)**
9.c	Critically analyze the misuse detection approach in IDS. How does it operate, and what are the key benefits and limitations? Illustrate your answer with examples of specific attack signatures that misuses detection might identify. **[Application]**	**(CO3)**	**(10 Marks)**
	Or		

10.a	Review the advantages IPS offers over IDS that makes it a crucial component of a security approach? **[Knowledge]**	**(CO4)**	**(04 Marks)**
10.b	Explain primary purpose of network traffic filtering. **[Comprehension]**	**(CO4)**	**(06 Marks)**
10.c	Explain the importance of logging and monitoring for detecting and preventing intrusions. Support your answer with example. **[Application]**	**(CO4)**	**(10 Marks)**