Roll No											

PRESIDENCY UNIVERSITY
BENGALURU

SCHOOL OF ENGINEERING
END TERM EXAMINATION - JUN 2023

Semester : Semester VI - 2020
Course Code : CSE3145
Course Name : Sem VI - CSE3145 - Intrusion Detection and Prevention System
Program : CCS

Date : 14-JUN-2023
Time : 9.30AM - 12.30PM
Max Marks : 100
Weightage : 50%

Instructions:
(i) Read all questions carefully and answer accordingly.
(ii) Question paper consists of 3 parts.
(iii) Scientific and non-programmable calculator are permitted.
(iv) Do not write any information on the question paper other than Roll Number.

PART A

ANSWER ALL THE QUESTIONS **(10 X 2 = 20M)**

1. State the advantages of using intrusion analysis for security professionals.
(CO1) [Knowledge]

2. Define the diamond model of intrusion analysis used in an organization.
(CO1) [Knowledge]

3. Define the role of Incident Response Team.
(CO4) [Knowledge]

4. List the different modes of Snort tool.
(CO3) [Knowledge]

5. List the different parameters available for Profile based Intrusion Detection System.
(CO4) [Knowledge]

6. Define honeypot system.
(CO2) [Knowledge]

7. Describe Intruder Artifacts.
(CO2) [Knowledge]

8. Relate Intrusion and Intruder in IDPS.
(CO3) [Knowledge]

9. List the different features of SNORT tool.
(CO3) [Knowledge]

10. List the features provided by ISO/IEC 18043:2006 standard.

(CO4) [Knowledge]

PART B

ANSWER ALL THE QUESTIONS **(5 X 10 = 50M)**

11. Distinguish between Internal and External Threat.

(CO1) [Comprehension]

12. Review the Importance of Incident Response Plan to an organization and specify the documentation detail.

(CO2) [Comprehension]

13. Discuss the Importance of WIPS and explain the different types of threats that can be prevented by a good WIPS.

(CO4) [Comprehension]

14. Explain Bro Intrusion Detection and Prevention System with proper diagram.

(CO3) [Comprehension]

15. Distinguish between Intrusion Detection System and Intrusion Prevention System with proper examples.

(CO3) [Comprehension]

PART C

ANSWER ALL THE QUESTIONS **(2 X 15 = 30M)**

16. Illustrate Prelude Intrusion Detection and Prevention System with a neat architectural diagram.

(CO2) [Application]

17. A) Explain the list of attacks detected by the Snort tool with proper examples.
B) Analyze the benefits of using Snort for security professional.

(CO4) [Application]