Roll No. : .....

Total No. of Questions : **16**] [Total No. of Printed Pages : **3**

SEMC–419

M.Sc. (IVth Semester) Examination, 2022

CYBER SECURITY

Paper – MCSEC–403

(Intrusion Detection and Prevention System)

Time : 1½ Hours] [*Maximum Marks : **40***

The Question paper contains three Sections.

Section–A **(Marks : 1 × 10 = 10)**

Note :– Answer all the *ten* questions (Answer limit **50** words). Each question carries **1** mark.

Section–B **(Marks : 3 × 5 = 15)**

Note :– Answer any *five* questions by selecting at least *one* question from each Unit (Answer limit **200** words). Each question carries **3** marks.

Section–C **(Marks : 5 × 3 = 15)**

Note :– Answer any *three* questions by selecting *one* question from each Unit (Answer limit **500** words). Each question carries **5** marks.

Section–A

1. (i) What are external data threats ?

   (ii) What is host-based systems ?

(iii) What is IDS ?

(iv) What is Snort ?

(v) What do you understand by Snort Alert Moe ?

(vi) What is the credential analysis ?

(vii) Basic structure of Snort rules.

(viii) Full form of CIDR.

(ix) Explain the offset keyword.

(x) What is ACID ?

Section–B

Unit–I

2. What are external and internal threats of cyber security ?

3. Explain Intrusion prevention system.

4. What is Host-based IPS ?

Unit–II

5. Explain Snort command line options.

6. Differences between credentials analysis and non-credential analysis.

7. Explain packet sniffer mode and NIDS mode.

Unit–III

8. What do you understand by SnortSnarf ?

9. Describe agent development for intrusion detection.

10. Define the XML output module.

Section–C

Unit–I

11. What are IDS ? Explain its different types in detail.

12. Give difference between IPS and IDS.

Unit–II

13. Explain running snort on multiple network interfaces.

14. Elaborate upon the working of snort by describing the role of its main IDS components.

Unit–III

15. Explain architecture modes of IDs and IPs.

16. Write short notes on the following :

    (a) The class type keyword

    (b) The content keyword