Roll No. : .....

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

SCYS–324

M.Sc. (Computer Science) (IIIrd Semester) Examination, 2021

CYBER SECURITY

Paper - MCSEC-301

(Intrusion Detection and Prevention System)

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

Note :– The question paper contains three Sections.

Section–A **(Marks : 1 × 10 = 10)**

Note :– Answer all *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 each

1. (i) What is an Intrusion Prevention System (IPS) ?

   (ii) What are the types of IDS ?

(iii) What do you mean by Anomaly Detection ?

(iv) What is a Gateway ?

(v) What is a Man-in the-Middle Attach ?

(vi) What is a Threat Briefing ?

(vii) What is a threat agent example ?

(viii) Define Return on Investment (ROI).

(ix) What is Cyber Crime ?

(x) What is Legal Issues ?

Section–B 3 each

Unit–I

2. What do intrusion detection system detect in terms of misuse detection ?

3. Differentiate between detection and prevention systems.

4. Explain Hybrid detection methods with example.

Unit–II

5. What is the difference between Threat Brief and Quantifying Risk ?

6. How does intrusion detection in security work ? Give example.

7. Explain bro intrusion detection with an example.

Unit–III

8. What are the legal issues in Cyber Security ?

9. Define Cyber Forensics.

10. Is government organizations working for IDS ? If yes, then explain its objectives.

Section–C 5 each

Unit–I

11. Explain the architectures in detail :

(a) Centralized

(b) Distributed

12. What is Intruder in Cyber Security ? Explain two main types of intrusion detection systems.

Unit–II

13. In intrusion detection explain its tool selection and acquisition process.

14. How does short IPS work and also explain what attacks can short detect ?

Unit–III

15. What is Criminal Prosecutions ? And also explain the role of prosecutions.

16. Explain these terms in detail :

    (a) Organizations

    (b) Standardizations