Roll No. : ....

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

SEMC–417

M.Sc. (IVth Semester) Examination, 2022

CYBER SECURITY

Paper – MCSEC–401

(Malware Analysis)

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

Note :– 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 is patching binaries ?

   (ii) Give *two* examples of different file format.

(iii) Explain Viruses.

(iv) What is cover analysis ?

(v) Write *two* differences between viruses and worm.

(vi) Give the information of static and dynamic analysis of malware.

(vii) Explain trojan horse.

(viii) Give *one* example of how to encounter malware.

(ix) What is data encoding ?

(x) What is Network Mapper used for ?

Section–B

Unit–I

2. Explain in brief about Malware.

3. What is reverse engineering ?

4. Explain in brief about IDA.

Unit–II

5. Write in detail *two* functions of virtual machine.

6. Mention the concepts of debugging tools.

7. Discuss in brief about the concept of win AI.

Unit–III

8. Elaborate the concept of reverse engineering using GDB and IDA.

9. Give introduction of kernal OS.

10. What do you mean by hooking ?

Section–C

Unit–I

11. Elaborate the patching concept.

12. Write about *five* different types of malware.

Unit–II

13. What are the concepts of dynamic analysis for analyzing malware ?

14. Explain in brief the concept of anti-analysis. (Anti-disassembly)

Unit–III

15. Discuss in detail Rootkit anti-forensic tool.

16. Where and how can we use kernel debugging ?