| Reg. No. | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

## B.Tech/ M.Tech (Integrated) DEGREE EXAMINATION, MAY 2024

Sixth Semester

21CSC310J – MALWARE ANALYSIS

*(For the candidates admitted from the academic year 2022-2023 onwards)*

**Note:**

(i) **Part - A** should be answered in OMR sheet within first 40 minutes and OMR sheet should be handed over to hall invigilator at the end of 40th minute.

(ii) **Part - B** and **Part - C** should be answered in answer booklet.

Time: 3 Hours — Max. Marks: 75

### PART – A (20 × 1 = 20Marks)

Answer **ALL** Questions — Marks BL CO PO

1. Malware that presents unwanted advertisement to the user is ______. — 1 1 1 2
   (A) Adware (B) Botnet
   (C) Spyware (D) Scareware

2. Malware that holds the system for ransom by locking user's is ______. — 1 1 1 2
   (A) Rootkit (B) Ransomware
   (C) Rat (D) Dropper

3. ______ involves disassembling the suspect binary and looking at the code to understand program behavior. — 1 2 2 2
   (A) Dynamic analysis (B) Memory analysis
   (C) Behavioral analysis (D) Static analysis

4. sudoapt-get install upx command is used for — 1 1 1 2
   (A) Updation (B) Upgrade
   (C) Encryption (D) Packaging

5. The file command in Linux returns _______. — 1 1 1 2
   (A) Size of file (B) Nature of file
   (C) Time stamp of file (D) Complier name

6. ______ used to determine whether the sample has been previously detected by search online. — 1 2 2 4
   (A) File search (B) File find
   (C) File hash (D) File get

7. _______ is a popular web based malware scanning service. — 1 1 2 4
   (A) Virus total (B) Virus share
   (C) The zoo (D) Clarivate

8. FLOSS stands for ______. — 1 1 2 4
   (A) File login operating system service (B) File loss obfuscated string solver
   (C) Fireeye labs obfuscated string solver (D) File labs obfuscated string solver

9. ______ contains executable code. 1 1 2 4

(A) .TEXT (B) .DATA

(C) .RDATA (D) .IDATA

10. PE stands for ______. 1 1 2 4

(A) Program editable (B) Portable executable

(C) Program executable (D) Preference executable

11. _____ is a great method to compare files for similarity between the samples. 1 2 3 8

(A) Fuzzy searching (B) Fuzzy comparing

(C) SS fuzzy (D) Fuzzy hashing

12. ______ includes monitoring the real-time file system activity during malware execution. 1 2 3 8

(A) Process monitoring (B) File system monitoring

(C) Registry monitoring (D) Network monitoring

13. In process monitor, Ctrl + E key used for ______. 1 1 3 8

(A) Save all the events (B) Backup all the events

(C) Restore all the events (D) Clear all the events

14. NORIBEN is a _______. 1 1 3 8

(A) Programming tool (B) Sandboxing tool

(C) Debugging tool (D) Disassembly tool

15. ______ stores the code and data for the computer. 1 1 3 8

(A) ROM (B) RAM

(C) EPROM (D) DRAM

16. Network data uses _______. 1 1 4 4

(A) Bit format (B) Byte format

(C) Big-Endian format (D) Little-endian format

17. An attacker can achieve persistent by modifying the registry entries used by ______. 1 2 5 2

(A) Startup (B) Winlogon

(C) Services (D) Updates

18. ______ is a program that runs in the background without any user interface such as event logging. 1 2 4 4

(A) Startup (B) Update

(C) Regedit (D) Service

19. A service can also be created using management tools such as ______. 1 1 4 4

(A) Power shell (B) Winshell

(C) Shell script (D) Python shell

20. ______ isolates the operating system from different hardware platforms. 1 1 4 4

(A) NTOSKRNL (B) WIN32K

(C) HAL (D) NTDLL

## PART – B (5 × 8 = 40 Marks)
Answer **ALL** Questions

| | | | Marks | BL | CO | PO |
|---|---|---|---|---|---|---|
| 21. | a. | Discuss in detail different types of malware and its impact. | 8 | 3 | 1 | 2 |
| | | **(OR)** | | | | |
| | b. | Write in detail the countermeasures to be taken for avoiding ransomware attacks in any system. | 8 | 3 | 1 | 2 |
| 22. | a. | How to simulate networking services using INetSim? | 8 | 3 | 2 | 4 |
| | | **(OR)** | | | | |
| | b. | Compare and contrast INetSim Vs Fakenet tool under dynamic analysis. | 8 | 3 | 2 | 4 |
| 23. | a. | Write a C program using global and local variables. Write its equivalent assembly code. | 8 | 3 | 3 | 8 |
| | | **(OR)** | | | | |
| | b. | Write a C program to implement 1-D array. Write its equivalent assembly code. | 8 | 3 | 3 | 8 |
| 24. | a. | Explain in detail memory map using OllyDbg interface. | 8 | 3 | 4 | 4 |
| | | **(OR)** | | | | |
| | b. | How to show threads and stacks in OllyDbg interface? | 8 | 3 | 1 | 4 |
| 25. | a. | With the help of a neat diagram, explain event and message flow in windows with and without hook injection. | 8 | 3 | 5 | 2 |
| | | **(OR)** | | | | |
| | b. | Discuss in detail about keystroke Logging and its types. | 8 | 3 | 5 | 2 |

## PART – C (1 × 15 = 15 Marks)
Answer **ANY ONE** Question

| | | Marks | BL | CO | PO |
|---|---|---|---|---|---|
| 26. | How to perform bindshell using NASM in Linux 64 bit shell code? Justify with snippet code. | 15 | 4 | 3 | 8 |
| 27. | You are working as malware analyst in organization under cyber wing. The task given is to analyze different types of malware payload. Justify with example for carrying out static and dynamic analysis with the various types of payloads. | 15 | 4 | 3 | 8 |

* * * * *