Reg. No.															

B.Tech. DEGREE EXAMINATION, NOVEMBER 2023

Seventh Semester

18CSE472T – MALWARE ANALYSIS

(For the candidates admitted from the academic year 2020-2021 & 2021-2022)

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 & Part - C** should be answered in answer booklet.

Time: 3 hours | Max. Marks: 100

PART – A (20 × 1 = 20 Marks)

Answer **ALL** Questions

	Marks	BL	CO	PO
1. _____ is a code that performs malicious actions, it can take the form of an executable, script, code or any other software. (A) Malware (B) Application (C) Encryptor (D) Decryptor	1	2	1	1
2. _____ presents unwanted advisement to the user. (A) Adware (B) Spyware (C) Ransom ware (D) Botnet	1	1	1	2
3. _____ scans the network looking for vulnerable systems upon successful exploitation. (A) Botnet (B) Backdoor (C) Spyware (D) Rootkit	1	2	1	1
4. _____ determines the tools and techniques for behavioural analysis. (A) Static (B) Dynamic (C) Memory (D) Code	1	1	2	2
5. _____ technique focus on understanding inner working of a binary. (A) Code analysis (B) Memory analysis (C) Dynamic analysis (D) Hybrid analysis	1	2	3	2
6. _____ is a crucial part of Microsoft windows made to launch functionalities based on windows DLL. (A) Rundll32.exe (B) rundll64.exe (C) Run32.exe (D) run64.exe	1	2	2	1
7. Process name, operations and details are related to (A) Files (B) Pages (C) Filters (D) Executable binary	1	1	2	2
8. _____ in memory, available to all functions. (A) Global (B) Local (C) Objects (D) Pointers	1	1	3	1

9. cmp, test, jz, jnz are examples of _____. 1 1 4 1
   (A) Branching (B) Conditional
   (C) Selection (D) Structures

10. add, sub, idiv are examples of _____. 1 1 3 1
   (A) Arithmetic (B) Branching
   (C) Selection (D) Conditional

11. The blue arrow indicates _____. 1 1 4 4
   (A) Unconditional jump (B) Conditional jump
   (C) Looping (D) Recursion

12. Which color represents compiler generated code? 1 1 4 4
   (A) Black (B) Red
   (C) Blue (D) Green

13. The assembly-level debugger's also called as _____. 1 1 3 1
   (A) High-level debuggers (B) Medium-level debuggers
   (C) Low-level debuggers (D) Code-level debuggers

14. _____ allows to significantly decrease the amount of instructions to analyze wrong functionalities 1 2 5 2
   (A) Step-in (B) Step-over
   (C) Step-out (D) Step-gain

15. _____ used to pause execution and allow the examine programs state 1 1 3 2
   (A) Check point (B) View point
   (C) Turning point (D) Breakpoint

16. _____ principle way that a debugger gains control of a running program. 1 2 5 1
   (A) Exception (B) Exemption
   (C) Encoder (D) Encryption

17. _____ was the first ransomware discovered for the android OS. 1 1 6 1
   (A) Defender (B) Drsheep
   (C) Luckycat (D) Bmaster

18. _____ was the very first boot kit created for the android OS. 1 1 6 1
   (A) Droid pack (B) Old boot
   (C) Droid bot (D) Torec

19. _____ is a popular reverse engineering tool that contains part of repository code. 1 2 6 4
   (A) Androguard (B) Ugaurd
   (C) Proguard (D) Mgaurd

20. _____ most established and known multiscanner's for .apk files 1 1 6 2
   (A) Virusshare (B) Virusget
   (C) Virustotal (D) Virusmart

PART – B (5 × 4 = 20 Marks)

Answer **ANY FIVE** Questions

	Marks	BL	CO	PO
21. How to detect packer's with PEiD tool? Justify with example.	4	3	1	1
22. Compare static Vs dynamic linking with example for each.	4	3	1	1
23. Give some examples of import and export functions form malware binary file.	4	3	1	2
24. How to run malware inside sandboxing environment?	4	4	2	2
25. What is IDA data displays? Justify with an examples.	4	3	4	1
26. How to write plugin user interface inside IDA pro?	4	4	5	2
27. How to create JAR file for signing into android application.	4	3	6	1

PART – C (5 × 12 = 60 Marks)

Answer **ALL** Questions

	Marks	BL	CO	PO
28. a.i. How to examine PE files with PE view? Justify with an example.	6	3	1	1
ii. How to unpack executables? Justify with an example.	6	4	1	2
(OR)				
b. Discuss in detail the general rules for malware analysis.	12	3	2	2
29. a. Explain in detail the structure of virtual machine for building sandboxing environment using suitable diagram.	12	3	2	1
(OR)				
b. Discuss in detail the basic tools used for dynamic analysis. Give examples for each tool with its purpose.	12	3	2	2
30. a. Write in detail the process of reverse engineering and patching new executables inside the disassembler.	12	4	5	4
(OR)				
b.i. Write brief notes on virtual functions and utables.	6	3	3	2
ii. Explain in detail the object life cycle with examples.	6	3	3	1
31. a. Discuss in detail augmenting functions and pre-defined comments inside IDA pro disassembler.	12	3	4	1
(OR)				
b. Explain in detail customizing IDA's for analyzing malicious binary file.	12	3	5	2

32. a.	Write in detail about application storage and data collections inside android application.	12	3	6	1
	(OR)				
b.i.	Enlist the capabilities and limitations of Emulators.	6	3	6	1
ii.	Discuss in detail processor emulation giving suitable example.	6	3	6	1

* * * * *