Reg. No.															

B.Tech. DEGREE EXAMINATION, MAY 2024
Sixth Semester

18CSE472T – MALWARE ANALYSIS
(For the candidates admitted during the academic year 2018-2019 to 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 type of payload that can spread without user intervention. (A) Worm (B) Virus (C) Trojan (D) Fake defender	1	2	1	1
2. What is the output for following command? File sample exe (A) Show the nature of file (B) Show the file size (C) Shows the file stamp (D) Shows the file security	1	1	1	1
3. The program that takes the executable as input and uses compression to obfuscate content is _____. (A) Cryptor's (B) Encoders (C) Packers (D) Floss	1	2	1	1
4. _____ uses a debugger to examine the internal state of a running malicious executable (A) Basic static analysis (B) Basic dynamic analysis (C) Advanced static analysis (D) Advanced dynamic analysis	1	2	1	3
5. _____ is an open source, multipurpose tool that helps in monitoring system resources (A) Process hacker (B) Regshot (C) Regedit (D) CFF explorer	1	1	2	1
6. _____ clears all the events in process monitor tool. (A) Ctrl + X (B) Ctrl + C (C) Ctrl + E (D) Ctrl + W	1	1	2	1
7. _____ is a security mechanism for running untrusted program in a safe environment without fear of harming real systems. (A) Process monitor (B) Sand box (C) Process explorer (D) Regshot	1	1	2	1
8. _____ displays configurable columns containing information about individual events (A) Regshot (B) Procmon (C) Fakenet (D) IDA	1	2	2	1

9. A _____ is a program that translated machine code back to assembly code. 1 2 4 1
   (A) Assembler (B) Interpreter
   (C) Disassembler (D) Compiler

10. IDA stands for _____. 1 2 3 4
   (A) Interactive disassembler (B) Interface disassembler
   (C) Inductive disassembler (D) Imperative disassembler

11. The microcode level is also known as _____. 1 2 3 4
   (A) Firmware (B) Software
   (C) Wrapper (D) Assembler

12. The way of hiding implementation details in a code is called as 1 2 3 1
   (A) Encapsulation (B) Polymorphism
   (C) Abstraction (D) Typecast

13. _____ is used to examine an intermediate object file 1 1 3 1
   (A) NM (B) NMAP
   (C) NETCAT (D) NETVIEW

14. _____ is capable of displaying a wide range of information related to windows PE files 1 2 3 1
   (A) Dunkbin (B) Dumpbin
   (C) Deskbin (D) Cyclebin

15. Programmers typically group executable statements into units called _____. 1 1 2 1
   (A) Segments (B) Functions
   (C) Loops (D) Header

16. _____ allows the user to group comments for display at the top of a functions disassembly listing 1 1 3 1
   (A) Feedback comments (B) Regular comments
   (C) Function comments (D) Segment comments

17. _____ researches properties of software that can be investigated by the inspection of application and its source code 1 1 6 1
   (A) Static analysis (B) Behavioral analysis
   (C) Dynamic analysis (D) Functional analysis

18. DVM in android stands for _____. 1 2 6 1
   (A) Dilvik Virtual Machine (B) Delvik Virtual Machine
   (C) Dalvik Virtual Machine (D) Dalvuk Virtual Machine

19. _____ attempted to send premium rate SMS messages to predetermined numbers. 1 1 6 1
   (A) Base bridge (B) Mass bridge
   (C) Zsone (D) Zhash

20. _____ was viewed as spyware and the official name would show as SMS spy 1 2 6 1
   (A) Trojan spy (B) Gambler SMS
   (C) Hippo SMS (D) Love trap

PART – B (5 × 4 = 20 Marks)
Answer **ANY FIVE** Questions

		Marks	BL	CO	PO
21.	Write a note on file dependencies and imports.	4	3	1	1
22.	What are the various steps in dynamic analysis?	4	3	2	1
23.	Distinguish between high level and interpreted language with examples.	4	3	3	2
24.	How to import new structures in IDApro tool?	4	3	3	3
25.	Write short notes on obj dump with an example.	4	3	2	2
26.	Discuss ADB push and pull command with an example.	4	3	6	3
27.	How to find certificate information in APK file?	4	3	6	3

PART – C (5 × 12 = 60 Marks)
Answer **ALL** Questions

		Marks	BL	CO	PO
28. a.i.	How to extract strings using tools?	6	3	1	1
ii.	How to decode encrypted strings using FLOSS?	6	3	1	1
	(OR)				
b.	Obfuscation is used by malware authors to protect the inner workings of malware from security researchers, malware analyst and reverse engineers. Summarize the various ways of determining file obfuscation.	12	4	1	3
29. a.	Explain the structure of virtual machine and sandboxing approach in dynamic analysis.	12	3	2	1
	(OR)				
b.	Discuss in detail about faking a network and registry snapshot with necessary tool.	12	4	4	1
30. a.	Construct a C++ application using arithmetic operators. Write an equivalent assembly code for the same.	12	4	4	1
	(OR)				
b.	How reverse engineering is done using disassembler? Discuss in detail.	12	4	4	3
31. a.	Explain in detail about Names and Naming in IDApro tool.	12	4	5	1
	(OR)				
b.	Compare and contrast exports and imports window using example.	12	3	3	1
32. a.	How dynamic analysis is done for android malware? Given an example.	12	4	6	3
	(OR)				
b.	Write the procedure for performing static analysis in android malware. Justify with an example.	12	4	6	3

* * * * *