32. a. How to perform logging based vulnerability in android platform? Justify with a suitable example. 12 4 6 1

(OR)

b. Write in detail about analyzing android malware. Justify with necessary examples. 12 3 6 1

* * * * *

Reg. No.														

B.Tech. DEGREE EXAMINATION, JUNE 2023

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) Marks BL CO PO

Answer **ALL** Questions

1. The malicious programs which include key loggers, spyware, sniffers and form grabbers called as 1 1 1 1
   (A) Information stealer (B) Ransom ware
   (C) Adware (D) Botnet

2. Malware designed to download or install additional malware components called as _____. 1 1 1 1
   (A) Downloader (B) Spyware
   (C) Adware (D) Key logger

3. _____ covers the tools and techniques to extract useful information from the malware binary using this approach. 1 2 1 2
   (A) Static analysis (B) Dynamic analysis
   (C) Hybrid analysis (D) Memory analysis

4. The windows executable files are also called as _____. 1 1 1 1
   (A) PE files (B) Pdf files
   (C) Doc files (D) Cpp files

5. _____ tool that allows an examiner to inspects each byte of the file. 1 1 2 1
   (A) Hex editor (B) Text editor
   (C) C editor (D) Java editor

6. _____ can be used to determine whether the sample has been previously detected by searching online or database of AV scanner. 1 2 1 1
   (A) File hash (B) File name
   (C) File size (D) File time stamp

7. To extract strings from a suspect binary the following command is used 1 1 1 2
   (A) Strings - a log.exe (B) Strings - b log.exe
   (C) Strings - c log.exe (D) Strings - e log.exe

8. _____ applies filter on the malware executable name and clear all events just before running it. 1 2 1 1
   (A) Procmon (B) Process explorer
   (C) Regshot (D) Wireshark

9.	_____ listen on a single TCP port in windows. (A) Ncat.exe (B) Nc.exe (C) Nc.cet (D) netcat.exe	1	1	1	1
10.	_____ is included in Kali Linux to simulate the internet. (A) Glomsim (B) Inetsim (C) Mobile sim (D) Internet sim	1	1	2	1
11.	Which tool can be used to compare registry keys when they are changed or modifier? (A) Regshot (B) Procomn (C) Process explorer (D) Fake net	1	1	2	2
12.	Expand ASLR. (A) Address Space Layout Resolution (B) Address Space Layout Recommendation (C) Address Space Layout Randomization (D) Address Space Layout Resize	1	1	3	1
13.	In coloring the services are represented using _____. (A) Pink (B) Blue (C) Green (D) Red	1	1	3	1
14.	Expand FLIRT. (A) Fast Library Identification and Recognition Technology (B) Fast Library Identity Recognition Technology (C) Fast Library Information Recognition Technology (D) Fast Library Incident Recognition technology	1	1	3	1
15.	List the two modes in IDA protocol. (A) Graph and code mode (B) Graph and text mode (C) Graph and display mode (D) Graph and tree mode	1	1	4	2
16.	Names window contains _____. (A) Functions, strings (B) Name code, data code (C) Functions, name code, named data, strings (D) Data, strings	1	1	5	1
17.	Parameters pushed onto stack inside _____. (A) Function call (B) Value call (C) Data call (D) Window call	1	1	5	2
18.	Going to shell mode of android device using _____. (A) sudo adb (B) root adb (C) shell adb (D) adb shell	1	1	6	1
19.	The command used to show current running processes is _____. (A) ps (B) ls (C) pc (D) lc	1	1	6	1

20.	Which command is used to transfer files from android device to sdcard? (A) sudo push (B) sudo pull (C) adb push (D) adb pull	1	1	6	2

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

		Marks	BL	CO	PO
21.	How to classify malware using section hash? Justify with example.	4	3	1	2
22.	How to simulate internet services for dynamic analysis? Justify with an example.	4	3	1	2
23.	With the help of a diagram, explain the various levels of abstraction.	4	3	1	4
24.	Write short notes on opeodes and endianes with examples.	4	3	2	2
25.	How push and pop operations are done in a stack? Justify with an example.	4	4	3	2
26.	How to configure emulated devise within AUD? Justify with an example.	4	4	5	2
27.	Write short notes on devices view. Justify with an example.	4	3	6	1

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

		Marks	BL	CO	PO
28. a.i.	Discuss in detail the methods used as a finger print for malware analysis.	6	3	1	1
ii.	In malware analysis, what are all the methods for identifying file types?	6	3	1	2
	(OR)				
b.	Explain in detail the important PE sections giving suitable examples.	12	3	1	4
29. a.	Discuss in detail the various logging system activities using Noriben.	12	4	2	2
	(OR)				
b.	Explain in detail the simulating services with Inetsim. Justify by giving an examples.	12	4	2	2
30. a.	Write a C++ application to dcmonstrate conditional statement. Convert the code to assembly language and explain the same with global and local variables.	12	4	3	2
	(OR)				
b.	Explain in detail Rep instructions for manipulating data buffers.	12	3	4	1
31. a.	Write in detail about named constants in IDA pro.	12	3	5	1
	(OR)				
b.	How to modify execution with a debugger? Justify with an example.	12	4	5	2