Reg. No															

Minor CERTIFICATION EXAMINATION, NOVEMBER 2023

First Semester

18CSC005J - MALWARE ANALYSIS

(For the candidates admitted during the academic year (2020-2021 & 2021-20222))

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: 100**

PART - A (20 × 1 = 20 Marks) — Answer **all** Questions

		Marks	BL	CO
1.	_____is a broad term that refers to different types of malicious programs such as Trojans,viruses, worms, and rootkits. (A) Software (B) Malware (C) Hardware (D) Firmware	1	1	1
2.	_____ presents unwanted advertisements (ads) to the user. (A) Adware (B) Ransomware (C) Botnet (D) Rootkit	1	1	1
3.	_____ holds the system for ransom by locking users out of their computer or by encrypting their files. (A) Adware (B) Down-loader (C) Dropper (D) Ransomware	1	1	1
4.	_____malware is used to steal personal, business, or proprietary information for profit, then the malware can be classified as (A) Cyber ware (B) Steal ware (C) Crimeware (D) Firmware	1	1	1
5.	_____ is a program that takes the executable as input, and it uses compression to obfuscate the executable's content. (A) Compressor (B) Observer (C) Packer (D) Singleton	1	2	1
6.	_____gives information about how to unpack the binary sample. (A) Exeinfo PE (B) Procmon (C) Process Explorer (D) Regshot	1	1	2
7.	The functions that an executable imports from other files called as _____ (A) intern function (B) extern function (C) import function (D) export function	1	1	2
8.	_____ section contains the resources used by the executable such as icons, dialogs, menus and strings. (A) data (B) text (C) rdata (D) rsrc	1	2	2
9.	_____ contains information that specifies when the binary was compiled. (A) PE Header (B) PE Info (C) Binary Header (D) Binary Info	1	1	2
10.	_____technique is useful in comparing a suspect binary with the samples in a repository to identify the samples that are similar. (A) Fuzzy dumping (B) Fuzzy repository (C) Fuzzy hashing (D) Fuzzy storage	1	2	2

11.	_____rules based on textual or binary information contained within the malware specimen. (A) MARA (B) TARA (C) YARA (D) WARA	1	1	3
12.	_____is an open source, multipurpose tool that helps in monitoring system resources. (A) Process Hacker (B) Procmon (C) Procsys (D) Process Explorer	1	1	3
13.	_____is a great technique to understand the behavior of malware and to determine its network and host-based indicators. (A) Static analysis (B) Memory analysis (C) Dynamic analysis (D) Code analysis	1	1	3
14.	A group of 8 bits makes a _____ (A) byte (B) Tera byte (C) Micro byte (D) Mini byte	1	1	3
15.	_____ stores the machine code and data for the computer (A) Flash Memory (B) Secondary Memory (C) ROM (D) RAM	1	1	4
16.	The CPU itself contains a small collection of memory within its chip, called the _____ (A) physical set (B) logical set. (C) chip set. (D) register set.	1	1	4
17.	_____is a program that translates programs written in a programming language. (A) Compiler (B) Interpreter (C) Commutator (D) Component	1	1	5
18.	_____ is a program that translates machine code into a low-level code called assembly code. (A) Decimeter (B) Debugger (C) Decode (D) Delimiter	1	1	5
19.	by GCHQ is a great web application that allows you to carry out all kinds of encoding and decoding process. (A) CyberChef (B) MasterChef (C) WebChef (D) ApplicationChef	1	1	6
20.	Each byte from the plaintext is Xor ed with the encryption key is called as _____ (A) double byte XOR (B) multi byte XOR (C) single byte XOR (D) custom byte XOR	1	1	6

PART - B (5 × 4 = 20 Marks)

Answer **any 5** Questions

		Marks	BL	CO
21.	Write short notes about creeper virus.	4	2	1
22.	Define adware. Give real world examples.	4	2	2
23.	Compare static vs dynamic analysis.	4	2	4
24.	With the help of diagram, show levels of abstraction.	4	1	4
25.	Write short notes on opcode and operand in x86 architecture.	4	2	5
26.	What is general purpose register? Give some examples.	4	1	5
27.	Write briefly about re-basing in OLLYDBG.	4	1	6

PART - C (5 × 12 = 60 Marks)

Answer **all** Questions

		Marks	BL	CO

28.	(a) Discuss in detail types of malware with examples for each.	12	3	1
	(OR)			
	(b) With the help snippet code, how to suspect binary file using virus total API?			
29.	(a) How to extract strings from suspected binary application? Justify using real time example.	12	4	2
	(OR)			
	(b) How to determine file obfuscation? Justify using FLOSS tool.			
30.	(a) Discuss in detail about logging system using Noriben.	12	3	3
	(OR)			
	(b) How to capture network traffic using fake net tool? Explain its role in dynamic analysis.			
31.	(a) Write a C program to demonstrate looping statement. Write its equivalent assembly code.	12	4	4
	(OR)			
	(b) Write a C program to demonstrate conditional statement. Write its equivalent assembly code.			
32.	(a) Discuss in detail the purpose of breakpoints in OLLYDBG tool.	12	3	5
	(OR)			
	(b) How to patch binary files inside debugger? Justify its necessity in reverse engineering.			

* * * * *