| | | | | | | |
|---|---|---|---|---|---|---|
| 28. a. | Describe the recursive descent disassembly algorithms in detail. | 10 | 1 | 3 | 1 |
| | **(OR)** | | | | |
| b. | Categorize the various disassembly tools. | 10 | 2 | 3 | 1 |
| 29. a. | Categorize various infamous patch program menus. | 10 | 2 | 4 | 1 |
| | **(OR)** | | | | |
| b. | Develop a script to enhance additional features in *IDA* using variables, expressions, statements, functions, objects of *IDC* scripting language. | 10 | 3 | 5 | 4 |
| 30. a. | Analyse the android Trojan "Usbcleaver". | 10 | 2 | 6 | 1 |
| | **(OR)** | | | | |
| b. | Categorize the various open source tools available in Native analysis and reverse engineering. | 10 | 2 | 6 | 1 |

* * * * *



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

**B.Tech. DEGREE EXAMINATION, MAY 2022**

Sixth & Seventh Semester

18CSE472T – MALWARE ANALYSIS

*(For the candidates admitted from the academic year 2018-2019 to 2019-2020)*

**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** should be answered in answer booklet.

Time: 2½ Hours Max. Marks: 75

**PART – A (25 × 1 = 25 Marks)**

Answer **ALL** Questions

| | | Marks | BL | CO | PO |
|---|---|---|---|---|---|
| 1. | Identify the signature used to detect malicious code by monitoring network traffic<br>(A) Network signature (B) Host based signature<br>(C) Remote signature (D) Malicious signature | 1 | 1 | 1 | 1 |
| 2. | Relate the analysis which involves examining the malware without using it<br>(A) Static analysis (B) Dynamic analysis<br>(C) Behavioural analysis (D) Advanced analysis | 1 | 1 | 1 | 1 |
| 3. | What examines the executable file without viewing the actual instructions?<br>(A) Basic static analysis (B) Basic dynamic analysis<br>(C) Behavioural analysis (D) Advanced analysis | 1 | 1 | 1 | 1 |
| 4. | The analysis that consists of reverse engineering in the malware's internals by loading the executable into a disassembler and looking at the program instructions to discover what the program does is<br>(A) Basic static analysis (B) Basic dynamic analysis<br>(C) Advanced static analysis (D) Advanced dynamic analysis | 1 | 1 | 1 | 1 |
| 5. | Identify the malware that installs itself onto a computer to allow the attacker access is<br>(A) Backdoor malware (B) Botnet malware<br>(C) Downloader (D) Root kit | 1 | 1 | 1 | 1 |
| 6. | Relate the security mechanism for running untrusted programs in a safe environment without the fear of harming real systems is<br>(A) Sand box (B) Mind box<br>(C) Flip box (D) Mind map | 1 | 2 | 2 | 2 |
| 7. | Identify the advanced monitoring tool for windows that provides a way to monitor certain registry, file system, network process and thread activity.<br>(A) Proexe (B) Procmon<br>(C) Viewpro (D) Viewmon | 1 | 1 | 2 | 2 |

8. Which is an extremely powerful task manager that should be running, when you are performing dynamic analysis — 1 1 2 1
   (A) Process monitor (B) View processor
   (C) Process explorer (D) View explorer

9. Select the tool which provides the quickest way to see DNS requests made by malware — 1 1 2 1
   (A) ApateDNS (B) Netcat
   (C) Procmon (D) Viewmon

10. Which is an open source sniffer, a packet capture tool that intercepts and logs network traffic? — 1 1 2 1
   (A) Net cat (B) Wireshark
   (C) Apate DNS (D) Procomon

11. Which of the below display information from object files? — 1 1 3 1
   (A) objdump (B) otool
   (C) nm (D) PEiD

12. Which tool is used to examine an intermediate object file? — 1 1 3 1
   (A) objdump (B) otool
   (C) nm (D) PEiD

13. Relate the tool that is used to identify the compiler used to build a particular windows portable executable binary and to identify any tools used to obfuscate a windows portable executable binary — 1 3 3 1
   (A) objdump (B) otool
   (C) nm (D) PEiD

14. Select the most prominent examples of recursive descent disassembler — 1 1 3 1
   (A) IDA Pro (B) SAND BOX
   (C) PEiD (D) otool

15. The linear sweep disassembly algorithm takes a very _____ approach to locating instructions to disassemble — 1 1 3 1
   (A) Straight forward (B) Backward
   (C) Bottom-up (D) Top-down

16. In IDA's batch mode which causes IDA to delete any existing database associated with the file specified on the command line is — 1 1 4 1
   (A) " A" (B) "–C"
   (C) " S" (D) "–B"

17. Relate the configuration file which allows IDA to create hotkey specification is — 1 1 4 1
   (A) ida.cfg (B) idagui.cfg
   (C) idatui.cfg (D) idamain.cfg

18. The set of techniques employed by IDA to identify sequences of code as library code is said to be — 1 1 4 1
   (A) "IDC" (B) "FLIRT"
   (C) "ADA" (D) "SHARK"



19. Recognize the output file that describes the overall layout of a binary, including information about the sections that make up the binary and the location of symbols within each section — 1 1 4 1
   (A) .map (B) .asm
   (C) .inc (D) .lst

20. Relate the directory that contains a number of subdirectories, which in turn contain the link libraries required to build various IDA modules — 1 1 5 1
   (A) ldr directory (B) module directory
   (C) etc directory (D) lib directory

21. Relate the malware that attempted to send premium rate SMS messages without the users consent to a hardcoded phone number — 1 3 6 1
   (A) Fake player (B) DroidSMS
   (C) FakeInst (D) TapSnake

22. Recognize the image file the emulator uses to write runtime user-data for a unique user — 1 1 6 1
   (A) sdcard.img (B) userdata-qemu.img
   (C) temp.img (D) avd.img

23. Identify the tool which uses a generic web server to host files — 1 1 6 1
   (A) FakeDNS (B) FakeHTTP
   (C) AVS logical (D) Proxy server

24. Identify the tool which is used to capture all the net flow traffic passing through the machine — 1 1 6 1
   (A) HTTP (B) Heap
   (C) Wire shark (D) Promax

25. Recognize the tool that profiles the application showing the objects and methods called during application operation. — 1 1 6 1
   (A) Update heap (B) Dump HPROF
   (C) Start method profiling (D) Update threads

**PART – B (5 × 10 = 50 Marks)** — Marks BL CO PO
Answer **ALL** Questions

26. a.i. Describe how the hashing helps in Malware analysis. — 5 1 1 1

   ii. List the types of Malware. — 5 1 1 1

**(OR)**

   b. Relate how dependency walker explores the dynamically linked functions. — 10 3 1 1

27. a. Relate how dynamic analysis of Malware can be performed using Sandbox technology. — 10 3 2 2

**(OR)**

   b. Sketch the architecture of X86 and explain in detail. — 10 2 2 1