Paper / Subject Code: 90924 / Information Tech.: Malware Analysis (R-2020)

(Time: $2\frac{1}{2}$ hours)

[Total Marks: 60]

N. B.: (1) All questions are compulsory.
(2) Make suitable assumptions wherever necessary and state the assumptions made.
(3) Answers to the same question must be written together.
(4) Numbers to the right indicate marks.
(5) Draw neat labeled diagrams wherever necessary.
(6) Use of Non-programmable calculator is allowed.

1. Attempt *any two* of the following: 12

a. State the different types of Malware Analysis Techniques.

b. Write a short note on i) ApateDNS ii) Netcat .

c. What is Sandboxes? What is purpose of Sandboxes is used for analyzing the malware? Explain with an Example.

d. What is Register? Explain the four types of Registers.

2. Attempt *any two* of the following: 12

a. What is use of Graph option of IDA Pro?

b. Explain the three most common calling conventions of C compiler used in the stack operation during function call.

c. What are the different function of Microsoft are used for accessing the file system?

d. What is Dynamic link libraries (DLLs)? How malware authors used DLL for infecting the system?

3. Attempt *any two* of the following: 12

a. Explain the OllyDbg Interface.

b. Write a short note on i) Remote Administration Tool (RAT) ii) botnet.

c. How malware uses Microsoft's Graphical Identification and Authentication (GINA) interception techniques for stealing the user credentials ?

d. Write a short note on Hook Injection.

4. Attempt *any two* of the following: 12

a. Explain the Brute-Forcing XOR Encoding.

b. Write a short notes on Base64 encoding.

c. How Snort is used for intrusion detection? Explain with an example.

d. State the Windows API functions are used for anti-debugging.

5. Attempt *any two* of the following: 12

a. Write a short note on Red Pill Anti-VM Technique.

b. What are indicators of a Packed Program?

c. Explain the difference between the Virtual and Nonvirtual Function.

d. Why malware might need to be compiled for the x64 architecture? Justify with an example.