M.Sc IT Sem-III

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. Explain types of malware.
b. What are packed and obfuscated program? Explain packing of files and how to detect it.
c. How to use VMware machine for malware analysis?
d. Explain the use of malware Sandboxes. Also state its drawback.

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

a. What are the features of IDA Pro to enhance disassembly?
b. Explain function call convention.
c. What are DLLs? How malware authors use dlls?
d. Write a short note on Using a debugger.

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

a. What is tracing? Explain features of tracing supported by OllyDbg.
b. Explain important commands of WinDbg.
c. What is a backdoor? What are the functions performed by backdoor?
d. Write a short note on Hook Injection.

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

a. Explain different ways to identify the use of standard cryptographic functions and content.
b. How to safely investigate an attacker online?
c. Explain Anti-disassembly.
d. What are the anti-debugging techniques of malware to detect debugger behavior?

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

a. Explain Red pill anti-VM and No pill techniques.
b. What are the tips and tricks for common packers?
c. Write a short note on Virtual vs. Non-Virtual function.
d. Give the example of why malware might need to be compiled for x64 architecture. Also state the differences between Windows 64-bit and 32-bit architecture.
