0505N285

Candidate's Seat No :_____

MSc Sem.-2 Examination

410

Cybersecurity & Forensic

May-2025

Time : 2-30 Hours] **[Max. Marks : 70**

Question 1 Answer the following questions:

i. "Static and dynamic analysis represent the two halves of a full perspective—neither is complete alone." Justify the statement with appropriate example. 7Marks

ii. Explain how core components of a CPU component contribute to instruction execution? 7Marks

OR

i. Differentiate between stack and heap memory in terms of allocation, usage, and vulnerabilities. 7Marks

ii. Explain disassemblers and decompilers, their use cases, and differences in output. 7Marks

Question 2 Answer the following questions:

i. What are special-purpose registers? Describe how they influence instruction flow and system state. 7Marks

ii. AX = 1100110011001100 7Marks

BX = 0010101010101010

Solve-

(1) ADD AX BX

(2) SUB AX BX

(3) 00000101 * 00000010

(4) AND AX BX

(5) OR AX BX

(6) XOR AX BX

(7) AND AL 00001111

OR

i. Describe how malware droppers use API functions to execute payloads. Explain with examples. 7Marks

ii. What are MIPS instructions? Describe the three categories of MIPS instructions with suitable examples. 7Marks

Question 3 Answer the following questions:

i. Explain the complete process of analysing suspicious PDF files. 7Marks

ii. While analyzing a packed binary, you discover that after unpacking, it inserts unrelated instructions before every real operation. How this act as both a protective 7Marks

(P.T.O)

and obfuscating mechanism?

OR

i. Explain how reverse engineers interact with malicious websites to assess threats. 7Marks

ii. What is code obfuscation? And explain its types. 7Marks

Questions 4 Answer the following questions:

i. A file is flagged as potentially malicious, and you are asked to analyze its PE structure. How could abnormalities in these sections indicate malware? Explain for each section. 7Marks

ii. What is API hooking? Explain its types. 7Marks

OR

i. What is memory forensics and explain its importance in malware analysis. 7Marks

ii. Security alerts show a system process running suspicious instructions. No new process is created. What kind of technique is this and what are its types? 7Marks

Questions 5: Attempt any Seven out of Twelve. 14Marks

1. What is use of Regshot tool?
2. Draw labelled diagram for memory hierarchy.
3. How is a worm different from a virus?
4. What is the purpose of the .text section in a PE file?
5. What is the role of breakpoints in a debugger?
6. An executable remains inactive for months but is programmed to delete system files on a specific date. Name the malware type and explain its behaviour
7. Which register would likely count the number of loop iterations?
8. What would be your first step if a debugger shows the entry point jumps to an area with unreadable instructions?
9. Explain LIFO in stack with the help of diagram.
10. Explain the function of the CALL and RET instructions.
11. What is the role of the .pdata section in exception handling in PE files?
12. What are JE, JNE, JZ, JNZ instructions?

.....X.....X.....