41 **1104E130** Candidate's Seat No :_____

IM.B.A. (CSM) Sem.-6 Examination

CSM-BBA-CC-309 E (EA)

Funda. of Rev. Engg. & Malware Analysis

Time : 2-30 Hours] **April-2025** **[Max. Marks : 70**

Question 1 Answer the following questions:

i. Differentiate between x86 and x64 architectures in terms of register sets, memory addressing, and instruction execution. 7Marks

ii. What are control flow statements, and why are they crucial in reverse engineering? 7Marks

OR

i. Explain User-Defined Data Structures and its types in detail 7Marks

ii. Explain the concept of instruction execution cycle in context of CPU components. 7Marks

Question 2 Answer the following questions:

i. How do dummy code insertion and instruction flow transformation affect control flow analysis? 7Marks

ii. Suppose a new malware variant contains thousands of lines of 'dead' code, encrypted metadata, and suspicious jump patterns. How these act as both a protective and obfuscating mechanism? 7Marks

OR

i. Explain how metadata and unused code removal act as both a protective and obfuscating mechanism. 7Marks

ii. An unknown executable produces no readable output, contains no strings, and has encrypted or compressed sections. What signs would indicate that the file is packed, and how would you go about unpacking it for deeper analysis? 7Marks

Question 3 Answer the following questions:

i. What are bitwise operations in assembly? Explain AND, OR, and XOR operations with binary examples. 7Marks

ii. How do disassembly, debugging, and pattern recognition facilitate the understanding of malicious functionalities? 7Marks

OR

i. Illustrate the use of CALL and RET instructions in subroutine execution and how malware can hijack this structure? 7Marks

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

Questions 4 Answer the following questions:

i. Explain how malware uses the .rsrc and .idata sections of a PE file for concealment and payload delivery. 7Marks

ii. Explain how a Portable Executable (PE) file is structured and how PE Header analysis can assist in identifying a malicious executable? 7Marks

OR

(P.T.O)

E130-2

i. Explain the role of network behavior analysis in detecting command-and-control (C2) communication. 7Marks

ii. Describe the steps, advantages, and challenges of performing dynamic malware analysis in a controlled environment. 7Marks

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

1. What is packing in the context of obfuscation, and how can packed malware be detected?
2. "ISA is not the code, but the code's language" Justify the statement.
3. What is the role of the .pdata section in exception handling in PE files?
4. Explain the purpose of the .rdata section in PE files.
5. What is the function of EBP registers?
6. What are JE, JNE, JZ, JNZ instructions?
7. Define size directives in assembly language.
8. What is a conditional jump instruction?
9. What information is stored in the .idata section of a PE file?
10. What is the difference between index and pointer registers?
11. Explain how logic bombs can be triggered via non-obvious system events.
12. Explain how bitwise XOR can be used to nullify or swap variables.

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

1104E130 -3 Candidate's Seat No :_____

IM.B.A. (CSM) Sem.-6 Examination

CSM-BBA-CC-309

EB-Security Incident Response

Time : 2-30 Hours] **April-2025** **[Max. Marks : 70**

Question 1 Answer the following questions:

i. What is the importance of having a structured security incident response plan in an organization? 7Marks

ii. What are the lessons learned from recent major cybersecurity incidents, and how can organizations apply them to improve security? 7Marks

OR

i. What are the challenges faced by security teams in responding to incidents, and how can they be overcome? 7Marks

ii. How do organizations ensure compliance with legal and regulatory requirements in incident response? 7Marks

Question 2 Answer the following questions:

i. Explain how organizations can use threat intelligence to improve their incident response capabilities. 7Marks

ii. Discuss the process of post-incident analysis and its impact on future security strategies. 7Marks

OR

i. Explain the importance of tabletop exercises and simulations in preparing for security incidents. 7Marks

ii. What are the key security parameters in cybersecurity? 7Marks

Question 3 Answer the following questions:

i. What is a Computer Security Incident Response Team (CSIRT) and what roles does it include? 7Marks

ii. What is the incident response lifecycle? 7Marks

OR

i. What steps are taken during the detection and analysis phase? 7Marks

ii. What actions are taken during the eradication and recovery phase? 7Marks

Questions 4 Answer the following questions:

i. What is the role of digital forensics in an incident response process? 7Marks

ii. How do you ensure the integrity and authenticity of digital evidence during an incident investigation? 7Marks

OR

i. What steps should be taken to preserve digital evidence while preventing further damage to systems? 7Marks

ii. What forensic techniques can be used to ensure that a compromised system is completely cleaned of malware or unauthorized access? 7Marks

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

1. What is the primary goal of a security incident response plan?
2. What is meant by "incident escalation"?
3. Define a security incident in the context of cybersecurity.

(P.T.O)

E130-4

4. How does multi-factor authentication (MFA) enhance security?
5. What are the key phases of the incident response lifecycle?
6. What is the role of law enforcement in cyber incident response?
7. Why is incident detection important in cybersecurity?
8. What is the role of law enforcement in cyber incident response?
9. What is the first step in responding to a security incident?
10 How does an organization test its incident response plan?
11 Name one common indicator of a security breach.
12 What is the role of law enforcement in cyber incident response?

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