E 146 A

4/96 **1104N035** Candidate's Seat No :_____

IM.Sc. (CSF) Sem.-6 Examination

ICSF-309-EA

Funda. of Rev. Engg. & Malware Analysis

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

Question 1 Answer the following questions:

i. What are registers? Explain general purpose registers. 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 Flags and its types in detail. 7Marks

Question 2 Answer the following questions:

i. What is code obfuscation? And explain its types. 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. Explain the execution of program in assembly language with diagram. 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. In a suspected backdoor program, CALL instructions are traced to external libraries but never return. How can CALL instructions be abused in malware? 7Marks

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

Questions 4 Answer the following questions:

i. A system administrator reports unusual CPU spikes, network traffic to unknown IPs, and encrypted file extensions across shared drives. As a reverse engineer, explain how you would use a combination of dynamic malware analysis and Sysinternals tools to investigate this scenario? 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

i. Why examining static properties of suspicious program is much important? 7Marks

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

(2, T, 9)

E146A-2
A03E2

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

1. "Decompilers try to guess; disassemblers show you raw truth" Justify the statement.
2. "ISA is not the code, but the code's language" Justify the statement.
3. Explain the role of the Control Unit in instruction execution.
4. What is meant by CPU Clock Speed? What does 4 GHz represent?
5. What is a CALL instruction and how is it different from a JUMP?
6. What is the function of the .text and .data sections in a program?
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.....

E 146 A-3

1104N035-3 Candidate's Seat No :_____

IM.Sc. (CSF) Sem.-6 Examination

ICSF-309-EB

Security Incident Response

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

Question 1 Answer the following questions:

i. How does the preparation phase help in incident response? 7Marks

ii. Discuss the different phases of the incident response lifecycle and their significance. 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. What best practices should be followed for an effective incident response? 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 phases involved in security incident response? 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 are the lessons learned from recent major cybersecurity incidents, and how can organizations apply them to improve security? 7Marks

OR

i. What are the key components of an incident response plan? 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. How does endpoint detection and response (EDR) help in security incidents?
2. What is meant by "incident escalation"?
3. Why is network segmentation important in security?
4. What is the purpose of security awareness programs?
5. What are the key phases of the incident response lifecycle?

(P.T.O.)

E 146 A-4
N035-1

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 difference between recovery and remediation?
10 How does an organization test its incident response plan?
11 Name one common indicator of a security breach.
12 What is a honeypot in cybersecurity?

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