4/41

1405E637

Candidate's Seat No:____

IMSc CSF Sem.-8 Examination

EA-Adv Reverse Engineering & Malware Analysis (Ele-1)

Time : 2.30 Hours] **May-2025** **[Max. Marks : 70**

Question 1 Answer the following questions:

i. How can abnormalities in each of the major PE sections—.text, .data, .rdata, .rsrc, .idata, and .pdata—reveal malicious intent? Explain what each section typically contains and how deviations may indicate malware activity. 7Marks

ii. Explain CPU registers in detail and their role in reverse engineering. 7Marks

OR

i. Elaborate on the role of system call hooking and API redirection in advanced malware. How do these techniques interfere with normal OS behaviour? 7Marks

ii. You receive a security alert indicating that a known system process (explorer.exe) is executing unfamiliar instructions, yet no new process appears in the task manager. The behaviour is stealthy and persistent. Identify and explain technique allows such code execution. 7Marks

Question 2 Answer the following questions:

i. Explain the impact of sandbox fingerprinting through CPUID, memory artifacts, and MAC address checks. Why are these techniques difficult to circumvent at scale in virtualized malware analysis? 7Marks

ii. Analyze how modern malware detects execution within debuggers. Discuss the forensic challenges posed by anti-debug techniques. 7Marks

OR

i. What is fileless malware? How does it leverage LOLBins to avoid detection and persist within a system? Describe the steps involved from initial access to execution. 7Marks

ii. Explain command and Control (C2) infrastructure in malware communication. Describe the methods used by malware to establish and maintain C2 communication channels. 7Marks

Question 3 Answer the following questions:

i. Differentiate between Base Image Address, Relative Virtual Address (RVA), and Virtual Address (VA) in the context of PE file structure. How are these addresses used in reverse engineering and debugging? Illustrate with suitable examples and formulas. 7Marks

ii. What is a sandbox in the context of malware analysis? Explain its types, advantages, and challenges. How does sandboxing contribute to forensic investigations and threat intelligence? 7Marks

OR

i. An analyst runs a packed malware sample in a virtual sandbox but fails to see post-decryption behaviour. Explain procedure to unpack the malware in a live analysis environment. 7Marks

ii. A disassembler shows many jumps to empty or unused labels in the code. What could this indicate about instruction flow obfuscation, and how would it affect analysing of the program? 7Marks

(P.T.O)

E637-2

Questions 4 Answer the following questions:

i. Explain what compiler optimizations are and why they are crucial in binary analysis. Distinguish between high-level and low-level compiler optimizations with examples. 7Marks

ii. Explain the structure and function of the MITRE ATT&CK framework. How does it help security professionals identify attacker tactics, techniques, and procedures (TTPs)? 7Marks

OR

i. How is an ELF file structured, and what roles do its main components play during execution? In what ways can attackers misuse its sections for malicious activity? 7Marks

ii. Explain how container-based malware infiltrates and operates within Docker or Kubernetes environments, and discuss key indicators of compromise along with effective security measures. 7Marks

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

1. The entry point of a PE file may not contain the actual malicious code. Justify how this misleads reverse engineers.
2. What are LOLBins?
3. Polymorphic malware relies on encryption; metamorphic malware does not. Which is harder to detect and why?
4. What is the size of a DWORD and a QWORD in bytes?
5. How analyzing entropy in PE sections can reveal packing or encryption?
6. What is process hollowing?
7. Explain function of regshot tool.
8. A YARA rule with too many fixed string matches may miss polymorphic variants. Justify briefly.
9. Explain why attackers prefer uploading malicious container images to public registries rather than exploiting vulnerabilities post-deployment?
10. How can exception-triggering behaviour like division by zero serve as a debugging detection tool without crashing real-world systems?
11. Differentiate between MITRE ATT&CK and MISP (Malware Information Sharing Platform).
12. AX = 1100110011001100 BX = 0010101010101010
    Calculate- I) OR AX BX II) XOR AX BX

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

1405E637-3 Candidate's Seat No:____

IMSc CSF Sem.-8 Examination

EB-Adv. Security Incident Response (Ele-2)

Time : 2.30 Hours] **May-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. Explain the key components of an effective security incident response framework. 7Marks

OR

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

ii. How does an organization identify and classify security incidents? 7Marks

Question 2 Answer the following questions:

i. How do security teams collaborate with external entities such as law enforcement and cybersecurity organizations during an incident? 7Marks

ii. How should organizations document and report security incidents effectively? 7Marks

OR

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

ii. Discuss the importance of communication and coordination during an incident response process. 7Marks

Question 3 Answer the following questions:

i. What are the goals of security incident response? 7Marks

ii. What is the incident response lifecycle? 7Marks

OR

i. What are the key components of an incident response plan? 7Marks

ii. What is the incident response lifecycle? 7Marks

Questions 4 Answer the following questions:

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

ii. What are the primary objectives of digital forensics during an incident response? 7Marks

OR

(P.T.O)

i. How do cloud environments present unique challenges in digital forensics during incident response? 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 ransomware, and how does it affect organizations?
3. Define a security incident in the context of cybersecurity.
4. What is the first step in responding to a security incident?
5. How does malware analysis help in incident response?
6. What is a security log, and why is it important?
7. What is meant by "threat intelligence" in incident response?
8. What is the role of law enforcement in cyber incident response?
9. What is the difference between recovery and remediation?
10 What is the function of a Security Information and Event Management (SIEM) system?
11 Name one common indicator of a security breach.
12 What is a honeypot in cybersecurity?

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