4/21

1405E626

Candidate's Seat No:_____

IMBA CSM Sem.-8 Examination

CSM_MBA_410

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

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

Question 1 Answer the following questions:

i. Explain the concept of dead-listing (offline analysis). What are its advantages and limitations? 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 working mechanism of virtualization-based obfuscation. How does it hinder reverse engineering efforts. 7Marks

ii. Analyze how modern malware detects execution within virtual machines. Discuss the forensic challenges posed by anti-VM 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 behavior. Explain procedure to unpack the malware in a live analysis environment. 7Marks

ii. Describe the internal structure of a Portable Executable (PE) file. Explain the purpose of each major component. How are sections like .text, .data, .rsrc, .reloc exploited or manipulated by attackers? 7Marks

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

(P.T.O)

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. If a malware sample executes different behaviours each time it's run, what techniques might it uses?
2. Polymorphic malware relies on encryption; metamorphic malware does not. Which is harder to detect and why?
3. How analysing entropy in PE sections can reveal packing or encryption?
4. What is process hollowing?
5. Explain function of regshot tool.
6. A YARA rule with too many fixed string matches may miss polymorphic variants. Justify briefly.
7. How can exception-triggering behaviours like division by zero serve as a debugging detection tool without crashing real-world systems?
8. Differentiate between MITRE ATT&CK and MISP (Malware Information Sharing Platform).
9. Why is identifying the decryption stub the key to reversing polymorphic malware?
10. Explain why attackers prefer uploading malicious container images to public registries rather than exploiting vulnerabilities post-deployment?
11. What is the size of a DWORD and a QWORD in bytes?
12. What are LOLBins?

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

1405E626 - 3 Candidate's Seat No:_____

IMBA CSM Sem.-8 Examination

CSM_MBA_410

EB-Adv Security Incident Response (Ele-2)

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

Question 1 Answer the following questions:

i. Explain the key components of an effective security incident response framework. 7Marks

ii. Discuss the different phases of the incident response lifecycle and their significance. 7Marks

OR

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

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

Question 2 Answer the following questions:

i. What measures should organizations take to recover from a major security breach? 7Marks

ii. What is security incident response and why is it important? 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 best practices should be followed for an effective incident response? 7Marks

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

OR

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

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

(P.T.O)

E626-4

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

i. How do cloud environments present unique challenges in digital forensics during incident response? 7Marks

ii. What is the importance of post-incident review and lessons learned? 7Marks

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

1. What is meant by "incident escalation"?
2. What is the role of law enforcement in cyber incident response?
3. What is the purpose of digital forensics in incident response?
4. What is meant by "incident severity classification"?
5. How does patch management help prevent security incidents?
6. What is the role of artificial intelligence in security incident response?
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 two common indicators of a security breach.
12. What is a honeypot in cybersecurity?

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