

GIAC

GREM
GIAC Reverse Engineering Malware

For More Information – Visit link below:

<https://www.examsempire.com/>

Product Version

- 1. Up to Date products, reliable and verified.**
- 2. Questions and Answers in PDF Format.**



<https://examsempire.com/>

Latest Version: 6.0

Question: 1

Analyzing the decompressed content of an RTF file is essential for what reason?

Response:

- A. To identify any embedded scripts or macros
- B. To understand the document's formatting hierarchy
- C. To detect hidden or obfuscated malicious payloads
- D. To verify the integrity of embedded images

Answer: C

Question: 2

When analyzing a function in assembly language, how can you identify the function's parameters?

Response:

- A. By locating values pushed onto the stack immediately before a call instruction
- B. By identifying the first arithmetic instructions in the function
- C. By counting the number of RET instructions
- D. By looking for direct register assignments at the start of the function

Answer: A

Question: 3

Which of the following is a potential indicator that an Office macro is attempting to download additional payloads?

Response:

- A. Interaction with a local database.
- B. Execution of complex mathematical calculations.
- C. Use of system networking commands.
- D. Modification of document metadata.

Answer: C

Question: 4

Why might malware use indirect jumps and calls as part of its execution flow?

Response:

- A. To make decompilation and debugging more difficult by obscuring the control flow
- B. To enhance the readability of the code for maintenance purposes
- C. To reduce the overall size of the compiled binary
- D. To improve the efficiency of execution on multi-core processors

Answer: A

Question: 5

How can an analyst use the entropy value of a file during malware analysis?

Response:

- A. To measure the file's compression ratio
- B. To determine the complexity and randomness within the file, indicating potential obfuscation or encryption
- C. To calculate the file's execution time
- D. To identify the programming language used to create the file

Answer: B

Question: 6

Which approach can help in bypassing malware that employs timing checks to detect analysis tools?

Response:

- A. Modifying the system clock
- B. Patching the malware binary to remove the checks
- C. Using network traffic generators
- D. Increasing the priority of the malware process

Answer: B

Question: 7

What aspects should be analyzed to determine if a macro in an Office file is self-replicating?

(Choose Two)

Response:

- A. The macro's ability to copy itself to other documents.
- B. The presence of code that modifies the startup folder.
- C. The macro's interaction with the Office clipboard.
- D. Code snippets that duplicate the macro within the same document.

Answer: A,D

Question: 8

When analyzing malicious software, what is an indicator of anti-emulation techniques being used?

Response:

- A. The malware performs redundant calculations.
- B. The malware checks for the presence of a mouse or user interaction.
- C. The malware avoids using system calls.
- D. The malware exclusively targets 32-bit systems.

Answer: B

Question: 9

In malware analysis, what is the purpose of comparing the hash of a suspicious file to known malware databases?

Response:

- A. To identify the file's original author
- B. To determine the exact changes made to the system by the malware
- C. To potentially identify the malware and its known behaviors
- D. To understand the network behavior of the malware

Answer: C

Question: 10

Why is it important to analyze the control words within an RTF document when investigating for malicious content?

Response:

- A. To identify custom styles applied to the document

-
- B. To detect hidden instructions or shellcode
 - C. To understand the document's layout structure
 - D. To verify the document's compatibility with different viewers

Answer: B

Thank You for Trying Our Product

Special 16 USD Discount Coupon: **NSZUBG3X**

Email: support@examsempire.com

**Check our Customer Testimonials and ratings
available on every product page.**

Visit our website.

<https://examsempire.com/>