

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/>

Visit us at: <https://www.examsempire.com/grem>

Latest Version: 6.0

Question: 1

API hooking implemented by malware is primarily used for which purpose?

- A. Increasing the speed of the malware execution
- B. Making the malware more detectable
- C. Intercepting and possibly altering the function calls, messages, or events passed between software components
- D. Simplifying the malware code

Answer: C

Question: 2

What is a key indicator that JavaScript code has been obfuscated?

- A. Presence of detailed comments
- B. Consistent use of meaningful variable names
- C. Unusual or inconsistent formatting and encoding
- D. Frequent use of JavaScript best practices

Answer: C

Question: 3

When analyzing a Windows executable, which of the following indicators most strongly suggests that the file is packed?

- A. The file has a high entropy value.
- B. The file contains numerous readable strings.
- C. The file size is unusually large for its functionality.
- D. The executable has multiple sections named with standard names (e.g., .text, .data).

Answer: A

Question: 4

When using a debugger on .NET malware, what would be a primary reason to set a breakpoint at a specific method?

- A. To observe the values of arguments passed to the method at runtime
- B. To change the execution flow of the program
- C. To prevent the malware from communicating over the network
- D. To decompile the entire assembly

Answer: A

Question: 5

What is the primary objective of conducting a static analysis on a suspected malware file?

- A. To immediately identify and delete malware from the system
- B. To observe the malware's interaction with its environment in real-time
- C. To gather information about the malware without executing it
- D. To determine the internet domains to which the malware communicates

Answer: C

Question: 6

You are analyzing a malware sample that appears to inject malicious code into the explorer.exe process. During execution, the malware creates a remote thread in explorer.exe and uses API calls to manipulate its memory.

How would you proceed with the analysis? (Choose three)

- A. Monitor the API calls used for process injection, such as VirtualAllocEx() and CreateRemoteThread().
- B. Dump the memory of the explorer.exe process and search for injected code.
- C. Use a tool like Procmon to observe filesystem activity.
- D. Analyze network traffic to detect any malicious communications initiated by explorer.exe.
- E. Set breakpoints at the process injection-related API calls in a debugger.

Answer: A,B,E

Question: 7

Which of the following are common flow control instructions used in malware? (Choose two)

- A. JMP
- B. XOR

- C. CALL
- D. POP

Answer: A,C

Question: 8

Which of the following is a common obfuscation technique used in .NET malware?

- A. String encryption
- B. Packed sections
- C. Code injection
- D. Process hollowing

Answer: A

Question: 9

Which API calls are commonly used by malware to manipulate processes and inject code? (Choose two)

- A. VirtualAllocEx()
- B. WriteProcessMemory()
- C. SendMessage()
- D. NtQueryInformationFile()

Answer: A,B

Question: 10

In reverse engineering .NET malware, what does dynamic analysis allow you to observe?

- A. The source code in its original high-level language
- B. How the application interacts with its environment in real-time
- C. The static set of APIs called by the application
- D. The file size and checksum

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/>