Vendor: GIAC

Exam Code: GREM

Exam Name: GIAC Reverse Engineering Malware

Version: DEMO

QUESTION 1
When analyzing a PDF file for malicious content, why is it important to examine the file's metadata?

A. To determine the software used to create the PDF
B. To identify the original author of the document
C. To find out the number of pages in the PDF
D. To check the file size for comparison with standard documents

Answer: C

QUESTION 2
In analyzing macros, why is it important to examine the API calls made by the macros?

A. They can reveal attempts to access sensitive system resources.
B. They are always indicative of malicious activity.
C. They are required for all macros to function.
D. They increase the efficiency of benign macros.

Answer: A

QUESTION 3
You are analyzing malware and notice a complex sequence of conditional branches and JMP instructions. The malware seems to randomly alter its execution flow based on certain conditions. What steps should you take to fully understand its behavior? (Choose three)

A. Step through the code in a debugger to observe how each condition is handled.
B. Modify the malware's code to disable all JMP instructions.
C. Analyze the malware's memory during execution to observe the effects of conditional statements.
D. Trace the instructions executed before and after each JMP instruction.
E. Run the malware in a sandbox environment to observe its network traffic.

Answer: ACD

QUESTION 4
Which tool is most commonly used to analyze JavaScript embedded within a malicious PDF?

A. Oletools
B. PDFiD
C. Wireshark
D. PEiD

Answer: B

QUESTION 5
What is the primary goal of static analysis in malware reverse engineering?

A. To determine how the malware behaves when executed
B. To analyze the malware without running it

C. To bypass the malware's encryption
D. To remove malware from the system

Answer: B

QUESTION 6
You are analyzing a malware sample in a debugger and notice the use of the CALL instruction followed by the manipulation of the EAX register. You suspect the malware is using custom functions for malicious purposes.
How would you proceed with the analysis? (Choose three)

A. Step into the CALL instruction to observe the function being executed.
B. Analyze the memory and stack before and after the CALL to understand how function arguments are passed.
C. Dump the memory to inspect the malware's unpacked payload.
D. Use static analysis tools to decompile the malware before proceeding further with dynamic analysis.
E. Set a breakpoint after the CALL to observe the returned value in the EAX register.

Answer: ABE

QUESTION 7
When encountering obfuscated JavaScript within a webpage, what is the initial step an analyst should take?

A. Execute the script in a browser to observe its behavior.
B. Deobfuscate the script manually line by line.
C. Use automated tools to attempt initial deobfuscation.
D. Report the script as malicious without further analysis.

Answer: C

QUESTION 8
Which tool is commonly used to extract metadata from a suspected malware file without executing it?

A. PEiD
B. OllyDbg
C. IDA Pro
D. Strings

Answer: D

QUESTION 9
Which of the following behaviors could indicate that a macro in an Office document is malicious? (Choose two)

A. The macro interacts with system processes outside of Office.
B. The macro repeatedly saves the document to disk.

C. The macro includes comments explaining its functionality.
D. The macro attempts to download additional files from the web.

Answer: AD

QUESTION 10
How can obfuscated call instructions within malware be identified and analyzed? (Choose Two)

A. By recognizing patterns that deviate from standard compilation outputs
B. Through the identification of unusual jumps and data movements that precede call instructions
C. By counting the frequency of call instructions
D. Monitoring stack changes prior to call operations

Answer: AB

QUESTION 11
In malware analysis, what does repairing unpacked malware refer to?

A. Correcting the malware's corrupted sections
B. Modifying the malware to remove its malicious payload
C. Rebuilding import tables and resolving dependencies to make the code analyzable
D. Enhancing the malware's ability to evade detection

Answer: C

QUESTION 12
What techniques are commonly used by attackers in malicious RTF files? (Choose two)

A. Exploiting CVE-2017-0199
B. Embedding malicious URLs in RTF comments
C. Embedding shellcode in OLE objects
D. Hiding malicious code in RTF metadata

Answer: AC

QUESTION 13
In assembly language, which instruction is commonly used for conditional execution?

A. TEST
B. LEA
C. CMP
D. INC

Answer: C

Thank You for Trying Our Product

Braindump2go Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.braindump2go.com/all-products.html

10% Discount Coupon Code: **ASTR14**