Fast2Test
FIRST TEST, FIRST PASS!

Fast2Test

Instant Download

After Payment, our system will send you the products you purchase in mailbox in a minute after payment. If not received within 2 hours, please contact us.

365 Days Free Updates

Free update is available within 365 days after your purchase. After 365 days, you will get 50% discounts for updating.

Money Back Guarantee

Full refund if you fail the corresponding exam in 60 days after purchasing. And Free get any another product.

Security & Privacy

We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.

We're not the only ones **happy** about Fast2test Practice Materials ...

62316+ customers in 100+ countries use Fast2test Self Test Engine. Meet our customers.

https://tw.fast2test.com

高效的考試材料是最高通過率的考試題庫

Exam : **GREM**

Title : GIAC Reverse Engineering Malware

Vendor : GIAC

Version : DEMO

NO.1 What aspect of an embedded object within an RTF file is crucial to analyze for determining potential malicious intent?
A. The file extension of the embedded object
B. The metadata describing the creation date of the object
C. The binary data representing the object
D. The spatial positioning of the object within the document
Answer: C

NO.2 Which outcome indicates successful deobfuscation of malicious JavaScript?
A. The script is shorter than the original.
B. The script's original logic and function calls are understandable.
C. The script no longer executes in any browser.
D. The script shows increased use of clear text strings.
Answer: B

NO.3 What file structure is analyzed in the static analysis of a Windows executable?
A. ELF header
B. PE header
C. FAT32
D. X64 assembly
Answer: B

NO.4 Which Windows API most strongly indicates credential harvesting?
A. OpenProcess()
B. CryptEncrypt()
C. LogonUser()
D. CreateRemoteThread()
Answer: C

NO.5 Which section in a PDF file typically stores the most important structure and object references for analysis?
A. Trailer
B. Catalog
C. Info
D. Stream
Answer: A

NO.6 In malware analysis, what is the purpose of comparing the hash of a suspicious file to known malware databases?
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

NO.7 You see a PE section with very high entropy and no readable strings. What is the MOST likely condition?
A. DLL sideloading
B. Packed payload
C. System misconfiguration
D. Debug symbols stripped
Answer: B

NO.8 What aspect of a file is NOT typically considered during static analysis?
A. The file's hash value
B. The file's interaction with the operating system when executed
C. The presence of digital signatures
D. The embedded resources within the file
Answer: B

NO.9 What methods do malware developers use to bypass static analysis? (Choose two)
A. Using API hashing to resolve functions dynamically
B. Employing encrypted communication protocols
C. Compressing executable files to reduce their size
D. Obfuscating strings used in the malware
Answer: AD

NO.10 You are analyzing a suspicious Office document received as an email attachment. Upon opening, you notice the document attempts to run a macro that accesses external servers and makes changes to the registry.
Which of the following actions should be taken to confirm the malicious intent of the macro? (Choose three)
A. Disable macros and examine the document in a sandbox.
B. Decompile the macro and search for obfuscated code.
C. Investigate network traffic for outgoing connections made by the macro.
D. Check if the macro is digitally signed by a trusted authority.
E. Verify if the document contains unusual formatting commands.
Answer: ABC

NO.11 Which of the following best describes the process of unpacking malware?
A. Converting malware binaries to source code
B. Extracting the payload from a dropper or downloader
C. Removing obfuscation layers to reveal the actual code
D. Scanning the malware with multiple antivirus products
Answer: C

NO.12 Which of the following tools or methods can be effectively used to analyze malicious RTF files?
(Choose Two)
A. RTF-specific parser
B. Plain text editor
C. Hexadecimal editor
D. Word processor with macro execution enabled
Answer: AC

NO.13 You are analyzing a malware sample in IDA Pro and identify a suspicious function written in assembly. The function uses multiple PUSH and MOV instructions and ends with a RET. How would you proceed to understand the function's purpose? (Choose three)
A. Identify which register stores the return value of the function.
B. Analyze the instructions leading up to the RET to understand what values are being pushed.
C. Modify the function to replace the RET with a NOP.
D. Step through the function in a debugger to observe the changes in register values.
E. Look for calls to external libraries within the function.
Answer: ABD

NO.14 Which of the following is a potential indicator that an Office macro is attempting to download additional payloads?
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

NO.15 In the analysis of a suspicious Office file's macro, which of the following elements would be crucial to investigate? (Choose Three)
A. The execution flow of the macro.
B. The digital signature status of the document.
C. Any obfuscated strings within the macro.
D. The presence of user interaction prompts.
E. Auto-execution triggers within the macro.
Answer: ACE

NO.16 When analyzing a ransomware sample you find code referencing CryptDeriveKey. What does this indicate?
A. Code signing
B. Encryption routine
C. Persistence payload
D. VM introspection
Answer: B

NO.17 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

NO.18 What is the significance of identifying obfuscated code within a macro?
A. It typically signifies the presence of intellectual property.
B. It may indicate attempts to hide malicious code from analysis.
C. It enhances the macro's performance.
D. It ensures compatibility across different Office platforms.
Answer: B

NO.19 A malware dynamically allocates RWX memory and copies code into it. What is the BEST indication for next analysis step?
A. Breakpoint on WriteFile
B. Dump the memory region
C. Hash comparison
D. Examine TLS callbacks
Answer: B

NO.20 What does the presence of DllImport attribute indicate in a .NET assembly? (Choose Two)
A. Direct invocation of unmanaged code
B. An attempt to perform network communication
C. Interoperability with Windows API functions
D. Automatic garbage collection
Answer: AC