GIAC GREM

GIAC Reverse Engineering Malware Certification Questions & Answers

Exam Summary – Syllabus –Questions

GREM
GIAC Reverse Engineering Malware
75 Questions Exam – 73% Cut Score – Duration of 180 minutes

Table of Contents:

Know Your GREM Certification Well:

The GREM is best suitable for candidates who want to gain knowledge in the GIAC Digital Forensics, Incident Response & Threat Hunting. Before you start your GREM preparation you may struggle to get all the crucial GIAC Reverse Engineering Malware materials like GREM syllabus, sample questions, study guide.

But don't worry the GREM PDF is here to help you prepare in a stress free manner.
The PDF is a combination of all your queries like-

- What is in the GREM syllabus?
- How many questions are there in the GREM exam?
- Which Practice test would help me to pass the GREM exam at the first attempt?

Passing the GREM exam makes you GIAC Reverse Engineering Malware. Having the GIAC Reverse Engineering Malware certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

GREM GIAC Reverse Engineering Malware Certification Details:

Exam Name	GIAC Reverse Engineering Malware (GREM)
Exam Code	GREM
Exam Price	$979 (USD)
Duration	180 mins
Number of Questions	75
Passing Score	73%
Books / Training	**FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques**
Schedule Exam	**Pearson VUE**
Sample Questions	**GIAC GREM Sample Questions**
Practice Exam	**GIAC GREM Certification Practice Exam**

GREM Syllabus:

Topic	Details
Analyzing Malicious Office Macros	- The candidate will be able to analyze macros and scripts embedded in suspicious Microsoft Office files to understand their capabilities.
Analyzing Malicious PDFs	- The candidate will be able to analyze suspicious PDFs and embedded scripts to understand the nature of the threat they might pose.
Analyzing Malicious RTF Files	- The candidate will be able to analyze suspicious RTF files and embedded shellcode to understand their capabilities.
Analyzing Obfuscated Malware	- The candidate will be able to identify packed Windows executables and obfuscated malicious JavaScript and unpack it to gain visibility of it's key capabilities.
Behavioral Analysis Fundamentals	- The candidate will be able analyze static properties of a suspected malware sample, develop theories regarding its nature, and determine subsequent analysis steps.
Common Malware Patterns	- The candidate will be able to identify common API calls used by malware and understand what capabilities the APIs offer to the malware samples. The candidate will be able to identify common techniques used by malware including code injection, hooking, and process hollowing techniques.
Core Reverse Engineering Concepts	- The candidate will apply dynamic analysis techniques to examine a malware sample in a debugger and will apply static analysis techniques to interpret common assembly instructions and patterns in Windows malware using a disassembler.
Examining .NET Malware	- The candidate will be able to analyze .NET programs to understand their capabilities.
Identifying and Bypassing Anti-Analysis Techniques	- The candidate will be able to identify and bypass common debugger detection and data protection measures used in malware, including the detection of security tools.
Malware Analysis Fundamentals	- The candidate will be able to describe key methods for analyzing malicious software and identify the needs of malware analysis lab.
Malware Flow Control and Structures	- The candidate will be able to analyze common execution flow control mechanisms, such as loops and conditional statements, in assembly language.

Topic	Details
Overcoming Misdirection Techniques	- The candidate will be able to overcome misdirecting execution workflow as an anti-analysis technique used in malware.
Reversing Functions in Assembly	- The candidate will be able to analyze malware functions in assembly language to understand use of parameters, return values and other structural elements.
Static Analysis Fundamentals	- The candidate will be able analyze static properties of a suspected malware sample, develop theories regarding its nature, and determine subsequent analysis steps.
Unpacking and Debugging Packed Malware	- The candidate will demonstrate process for unpacking malware using a debugger and repairing unpacked malware for further analysis.

GIAC GREM Sample Questions:

Question: 1

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

(Choose Two)

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: 2

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

Question: 3

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

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: 4

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

a) Modification of document metadata.
b) Execution of complex mathematical calculations.
c) Interaction with a local database.
d) Use of system networking commands.

Answer: d

Question: 5

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

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: 6

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

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: 7

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

a) To verify the document's compatibility with different viewers
b) To understand the document's layout structure
c) To identify custom styles applied to the document
d) To detect hidden instructions or shellcode

Answer: d

Question: 8

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

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: 9

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

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: 10

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

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

Study Guide to Crack GIAC Reverse Engineering Malware GREM Exam:

- Getting details of the GREM syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the GREM exam.
- Making a schedule is vital. A structured method of preparation leads to success. A candidate must plan his schedule and follow it rigorously to attain success.
- Joining the GIAC provided training for GREM exam could be of much help. If there is specific training for the exam, you can discover it from the link above.
- Read from the GREM sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.
- Practicing on GREM practice tests is must. Continuous practice will make you an expert in all syllabus areas.

Reliable Online Practice Test for GREM Certification

Make EduSum.com your best friend during your GIAC Reverse Engineering Malware exam preparation. We provide authentic practice tests for the GREM exam. Experts design these online practice tests, so we can offer you an exclusive experience of taking the actual GREM exam. We guarantee you 100% success in your first exam attempt if you continue practicing regularly. Don’t bother if you don’t get 100% marks in initial practice exam attempts. Just utilize the result section to know your strengths and weaknesses and prepare according to that until you get 100% with our practice tests. Our evaluation makes you confident, and you can score high in the GREM exam.

Start Online practice of GREM Exam by visiting URL
https://www.edusum.com/giac/grem-giac-reverse-engineering-malware