GCED Q&As

GIAC Certified Enterprise Defender Practice Test

Pass GIAC GCED Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/gced.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by GIAC Official Exam Center

QUESTION 1

The security team wants to detect connections that can compromise credentials by sending them in plaintext across the wire. Which of the following rules should they enable on their IDS sensor?

A. alert tcp any 22 any 22 (msg:SSH connection; class type:misc-attack;sid: 122:rev:1;)

B. alert tcp any any any 6000: (msg:X-Windows session; flow:from_server,established;nocase;classtype:misc-attack;sid:101;rev:1;)

C. alert tcp any 23 any 23 (msg:Telnet shell; class type:misc-attack;sid:100; rev:1;)

D. alert udp any any any 5060 (msg:VOIP message; classtype:misc-attack;sid:113; rev:2;)

Correct Answer: C

QUESTION 2

Which of the following is a major problem that attackers often encounter when attempting to develop or use a kernel mode rootkit?

A. Their effectiveness depends on the specific applications used on the target system.

B. They tend to corrupt the kernel of the target system, causing it to crash.

C. They are unstable and are easy to identify after installation

D. They are highly dependent on the target OS.

Correct Answer: B

QUESTION 3

You are responding to an incident involving a Windows server on your company\\'s network. During the investigation you notice that the system downloaded and installed two files, iexplorer.exe and iexplorer.sys. Based on the behavior of the system you suspect that these files are part of a rootkit. If this is the case what is the likely purpose of the .sys file?

A. It is a configuration file used to open a backdoor

B. It is a logfile used to collect usernames and passwords

C. It is a device driver used to load the rootkit

D. It is an executable used to configure a keylogger

Correct Answer: C

QUESTION 4

Which of the following would be used in order to restrict software form performing unauthorized operations, such as invalid access to memory or invalid calls to system access?

A. Perimeter Control

B. User Control

C. Application Control

D. Protocol Control

E. Network Control

Correct Answer: C

QUESTION 5

You have been tasked with searching for Alternate Data Streams on the following collection of Windows partitions; 2GB FAT16, 6GB FAT32, and 4GB NTFS. How many total Gigabytes and partitions will you need to search?

A. 4GBs of data, the NTFS partition only.

B. 12GBs of data, the FAT16, FAT32, and NTFS partitions.

C. 6GBs of data, the FAT32 partition only.

D. 10GBs of data, both the FAT32 and NTFS partitions.

Correct Answer: C