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.passapply.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

What does the following WMIC command accomplish?

process where name=\\'malicious.exe\\' delete

A. Removes the `malicious.exe\\' process form the Start menu and Run registry key

B. Stops current process handles associated with the process named `malicious.exe\\'

C. Removes the executable `malicious.exe\\' from the file system

D. Stops the `malicious.exe\\' process from running and being restarted at the next reboot

Correct Answer: B

QUESTION 2

Why would the pass action be used in a Snort configuration file?

A. The pass action simplifies some filtering by specifying what to ignore.

B. The pass action passes the packet onto further rules for immediate analysis.

C. The pass action serves as a placeholder in the snort configuration file for future rule updates.

D. Using the pass action allows a packet to be passed to an external process.

E. The pass action increases the number of false positives, better testing the rules.

Correct Answer: A

Explanation: The pass action is defined because it is sometimes easier to specify the class of data to ignore rather than the data you want to see. This can cut down the number of false positives and help keep down the size of log data. False positives occur because rules failed and indicated a threat that is really not one. They should be minimized whenever possible. The pass action causes the packet to be ignored, not passed on further. It is an active command, not a placeholder.

QUESTION 3

An outside vulnerability assessment reveals that users have been routinely accessing Gmail from work for over a year, a clear violation of this organization\\'s security policy. The users report "it just started working one day". Later, a network administrator admits he meant to unblock Gmail for just his own IP address, but he made a mistake in the firewall rule.

Which security control failed?

A. Access control

B. Authentication

C. Auditing

D. Rights management

Correct Answer: C

Explanation: Audits are used to identify irregular activity in logged (after-the-fact) records. If this activity went unnoticed or uncorrected for over a year, the internal audits failed because they were either incomplete or inaccurate. Authentication, access control and managing user rights would not apply as a network admin could be expected to have the ability to configure firewall rules.

QUESTION 4

To detect worms and viruses buried deep within a network packet payload, Gigabytes worth of traffic content entering and exiting a network must be checked with which of the following technologies?

A. Proxy matching

B. Signature matching

C. Packet matching

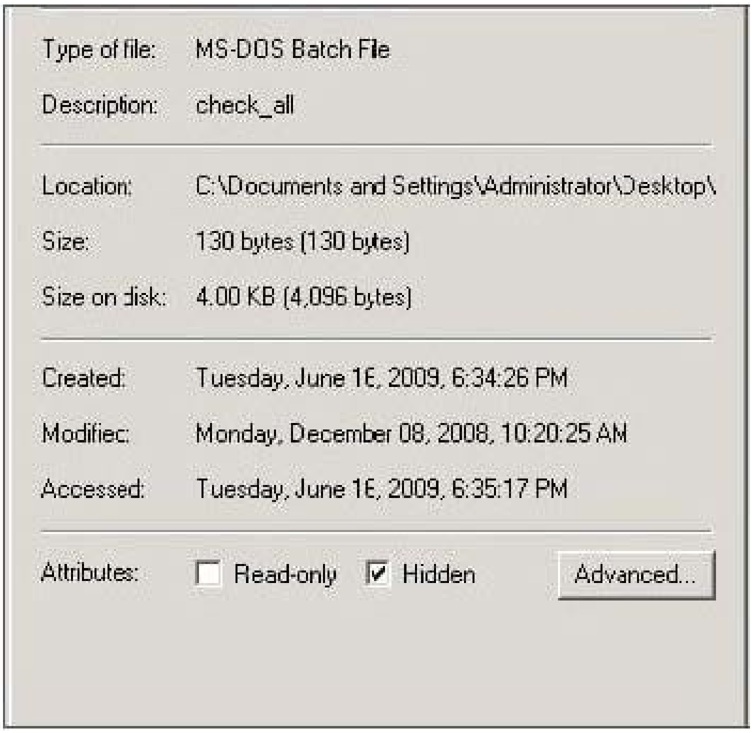
D. Irregular expression matching

E. Object matching

Correct Answer: C

QUESTION 5

Which command tool can be used to change the read-only or hidden setting of the file in the screenshot?



Type of file: MS-DOS Batch File

Description: check_all

Location: C:\Documents and Settings\Administrator\Desktop\

Size: 130 bytes (130 bytes)

Size on disk: 4.00 KB (4,096 bytes)

Created: Tuesday, June 16, 2009, 6:34:26 PM

Modified: Monday, December 08, 2008, 10:20:25 AM

Accessed: Tuesday, June 16, 2009, 6:35:17 PM

Attributes: □ Read-only ☑ Hidden

A. attrib

B. type

C. tasklist

D. dir

Correct Answer: A

Explanation: attrib ? or +r will remove or add the read only attribute from a file.

Latest GCED Dumps GCED Exam Questions GCED Braindumps