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.geekcert.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 would the output of the following command help an incident handler determine? cscript manage-bde . wsf –status

A. Whether scripts can be run from the command line

B. Which processes are running on the system

C. When the most recent system reboot occurred

D. Whether the drive has encryption enabled

Correct Answer: D

QUESTION 2

Requiring criminal and financial background checks for new employees is an example of what type of security control?

A. Detective Support Control

B. Detective Operational Control

C. Detective Technical Control

D. Detective Management Control

Correct Answer: D

Explanation: Management Controls include: Policies, guidelines, checklists, and reporting.

Detective management controls include personnel security. As a detective control, we are referring to

indepth background investigations, clearances, and rotation of duties.

QUESTION 3

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 4

A company classifies data using document footers, labeling each file with security labels "Public", "Pattern", or "Company Proprietary". A new policy forbids sending "Company Proprietary" files via email. Which control could help security analysis identify breaches of this policy?

A. Monitoring failed authentications on a central logging device

B. Enforcing TLS encryption for outbound email with attachments

C. Blocking email attachments that match the hashes of the company\\'s classification templates

D. Running custom keyword scans on outbound SMTP traffic from the mail server

Correct Answer: D

QUESTION 5

An analyst will capture traffic from an air-gapped network that does not use DNS. The analyst is looking for unencrypted Syslog data being transmitted. Which of the following is most efficient for this purpose?

A. tcpdump –s0 –i eth0 port 514

B. tcpdump –nnvvX –i eth0 port 6514

C. tcpdump –nX –i eth0 port 514

D. tcpdump –vv –i eth0 port 6514

Correct Answer: B

When using tcpdump, a –n switch will tell the tool to not resolve hostnames; as this network makes no use of DNS this is efficient. The –vv switch increases the tools output verbosity. The –s0 increases the snaplength to “all” rather than the default of 96 bytes. The –nnvvX would make sense here except that the port in the filter is 6514 which is the default port for encrypted Syslog transmissions.