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

Which action would be the responsibility of the First Responder once arriving at the scene of a suspected incident as part of a Computer Security Incident Response Plan (CSIRP)?

A. Making the decision of whether or not to notify law enforcement on behalf of the organization.

B. Performing timeline creation on the system files in order to identify and remove discovered malware.

C. Copying critical data from suspected systems to known good systems so productivity is not affected by the investigation.

D. Conducting initial interviews and identifying the systems involved in the suspected incident.

Correct Answer: D

Explanation: The First Responder plays a critical role in the Incident Response process on the CSIRT

(Computer Security Incident Response Team).

Here is a list of some typical responder tasks:

Make sure that the correct system is identified and photograph the scene, if necessary.

Conduct an initial interview (not an interrogation) of any witnesses.

The decision to notify law enforcement requires explicit approval and direction form management and/or

counsel. While a First Responder may collect initial data while minimally intruding on the system, no major

changes, or indepth media analysis should be performed by the First Responder when initially responding

to a suspected incident.

QUESTION 2

Which tool uses a Snort rules file for input and by design triggers Snort alerts?

A. snot

B. stick

C. Nidsbench

D. ftester

Correct Answer: C

QUESTION 3

A legacy server on the network was breached through an OS vulnerability with no patch available. The server is used only rarely by employees across several business units. The theft of information from the server goes unnoticed until the company is notified by a third party that sensitive information has been posted on the Internet. Which control was the first to fail?

A. Security awareness

B. Access control

C. Data classification

D. Incident response

Correct Answer: C

Explanation: The legacy system was not properly classified or assigned an owner. It is critical that an organization identifies and classifies information so proper controls and measures should be put in place. The ultimate goal of data classification is to make sure that all information is properly protected at the correct level.

This was not a failure of incident response, access control or security awareness training.

QUESTION 4

Which tool keeps a backup of all deleted items, so that they can be restored later if need be?

A. ListDLLs

B. Yersinia

C. Ettercap

D. ProcessExplorer

E. Hijack This

Correct Answer: E

Explanation: After selecting "fix it!" with Hijack This you can always restore deleted items, because Hijack This keeps a backup of them.

QUESTION 5

Of the following pieces of digital evidence, which would be collected FIRST from a live system involved in an incident?

A. Event logs from a central repository

B. Directory listing of system files

C. Media in the CDrom drive

D. Swap space and page files

Correct Answer: D

Explanation: Best practices suggest that live response should follow the order of volatility, which means that you want to collect data which is changing the most rapidly. The order of volatility is: Memory Swap or page file Network status and current / recent network connections Running processes Open files

GCED Practice Test GCED Study Guide GCED Exam Questions