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

Which type of attack could be used to obtain IOS router configuration files without a valid user password?

A. ARP cache poisoning

B. CDP sniffing

C. SNMP man in the middle

D. TFTP brute force

Correct Answer: D

Explanation: TFTP is a protocol to transfer files and commonly used with routers for configuration files, IOS images, and more. It requires no authentication. To download a file you need only know (or guess) its name. CDP, SNMP and ARP are not used for accessing or transferring IOS configuration files.

QUESTION 2

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 3

Which of the following is the best way to establish and verify the integrity of a file before copying it during an investigation?

A. Write down the file size of the file before and after copying and ensure they match

B. Ensure that the MAC times are identical before and after copying the file

C. Establish the chain of custody with the system description to prove it is the same image

D. Create hash of the file before and after copying the image verifying they are identical

Correct Answer: D

QUESTION 4

Which type of media should the IR team be handling as they seek to understand the root cause of an incident?

A. Restored media from full backup of the infected host

B. Media from the infected host, copied to the dedicated IR host

C. Original media from the infected host

D. Bit-for-bit image from the infected host

Correct Answer: A

Explanation: By imaging the media with tools such as dd or Ghost and analyzing the copy, you preserve the original media for later analysis so that the results can be recreated by another competent examiner if necessary.

QUESTION 5

Monitoring the transmission of data across the network using a man-in-the-middle attack presents a threat against which type of data?

A. At-rest

B. In-transit

C. Public

D. Encrypted

Correct Answer: B