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.pass2lead.com/gced.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

What should happen before acquiring a bit-for-bit copy of suspect media during incident response?

A. Encrypt the original media to protect the data

B. Create a one-way hash of the original media

C. Decompress files on the original media

D. Decrypt the original media

Correct Answer: B

QUESTION 2

A company wants to allow only company-issued devices to attach to the wired and wireless networks. Additionally, devices that are not up-to-date with OS patches need to be isolated from the rest of the network until they are updated. Which technology standards or protocols would meet these requirements?

A. 802.1x and Network Access Control

B. Kerberos and Network Access Control

C. LDAP and Authentication, Authorization and Accounting (AAA)

D. 802.11i and Authentication, Authorization and Accounting (AAA)

Correct Answer: A

QUESTION 3

Which of the following applies to newer versions of IOS that decrease their attack surface?

A. Telnet cannot be enabled or used

B. The Cisco Discovery Protocol has been removed

C. More services are disabled by default

D. Two-factor authentication is default required

Correct Answer: C

Explanation: Recent versions of IOS have less services enabled by default, older versions vary but generally have more services (even those not needed) enabled by default; this increases the attack surface on the device.

QUESTION 4

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 5

Which of the following attacks would use ".." notation as part of a web request to access restricted files and directories, and possibly execute code on the web server?

A. URL directory

B. HTTP header attack

C. SQL injection

D. IDS evasion

E. Cross site scripting

Correct Answer: A