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

Which of the following is considered a preventative control in operational security?

A. Smoke Sensors

B. Fire Suppressant

C. Voltage Regulators

D. Vibration Alarms

Correct Answer: B

Explanation: A fire suppressant device is a preventive control. Smoke sensors, vibration alarms, and voltage regulators are part of detection controls.

QUESTION 2

Which command is the Best choice for creating a forensic backup of a Linux system?

A. Run form a bootable CD: tar cvzf image.tgz /

B. Run from compromised operating system: tar cvzf image.tgz /

C. Run from compromised operating system: dd if=/ dev/hda1 of=/mnt/backup/hda1.img

D. Run from a bootable CD: dd if=/dev/hda1 of=/mnt/backup/hda1.img

Correct Answer: D

Explanation: Using dd from a bootable CD is the only forensically sound method of creating an image. Using tar does not capture slack space on the disk. Running any command from a compromised operating system will raise integrity issues.

QUESTION 3

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 4

What attack was indicated when the IDS system picked up the following text coming from the Internet to the web server?

select user, password from user where user= "jdoe" and password= `myp@55!\\' union select "text",2 into outfile "/tmp/file1.txt" - - \\'

A. Remote File Inclusion

B. URL Directory Traversal

C. SQL Injection

D. Binary Code in HTTP Headers

Correct Answer: C

Explanation: An example of manipulating SQL statements to perform SQL injection includes using the semi-colon to perform multiple queries. The following example would delete the users table:

Username: ` or 1=1; drop table users; - Password: [Anything]

QUESTION 5

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