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

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

QUESTION 1

Which of the following is an outcome of the initial triage during incident response?

A. Removal of unnecessary accounts from compromised systems

B. Segmentation of the network to protect critical assets

C. Resetting registry keys that vary from the baseline configuration

D. Determining whether encryption is in use on in scope systems

Correct Answer: B

QUESTION 2

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 3

Which Windows CLI tool can identify the command-line options being passed to a program at startup?

A. netstat

B. attrib

C. WMIC

D. Tasklist

Correct Answer: C

QUESTION 4

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

QUESTION 5

How would an attacker use the following configuration settings?

```
interface Tunnel0
ip address 192.168.55.1 255.255.255.0
tunnel source FastEthernet0/0
tunnel destination 192.17.250.2
```

A. A client based HIDS evasion attack

B. A firewall based DDoS attack

C. A router based MITM attack

D. A switch based VLAN hopping attack

Correct Answer: C