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

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 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

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 4

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 5

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.