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.leads4pass.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

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

QUESTION 2

Network administrators are often hesitant to patch the operating systems on CISCO router and switch operating systems, due to the possibility of causing network instability, mainly because of which of the following?

A. Having to rebuild all ACLs

B. Having to replace the kernel

C. Having to re-IP the device

D. Having to rebuild ARP tables

E. Having to rebuild the routing tables

Correct Answer: B

Explanation: Many administrators are hesitant to upgrade the IOS on routers based on past experience with the code introducing instability into the network. It is often difficult to completely test an IOS software upgrade in a production environment because the monolithic kernel requires that the IOS be replaced before the device can be tested. Because of these reasons, IOS upgrades to resolve security flaws are often left undone in many organizations.

QUESTION 3

Why would an incident handler acquire memory on a system being investigated?

A. To determine whether a malicious DLL has been injected into an application

B. To identify whether a program is set to auto-run through a registry hook

C. To list which services are installed on they system

D. To verify which user accounts have root or admin privileges on the system

Correct Answer: C

QUESTION 4

An analyst will capture traffic from an air-gapped network that does not use DNS. The analyst is looking for unencrypted Syslog data being transmitted. Which of the following is most efficient for this purpose?

A. tcpdump –s0 –i eth0 port 514

B. tcpdump –nnvvX –i eth0 port 6514

C. tcpdump –nX –i eth0 port 514

D. tcpdump –vv –i eth0 port 6514

Correct Answer: B

When using tcpdump, a –n switch will tell the tool to not resolve hostnames; as this network makes no use of DNS this is efficient. The –vv switch increases the tools output verbosity. The –s0 increases the snaplength to “all” rather than the default of 96 bytes. The –nnvvX would make sense here except that the port in the filter is 6514 which is the default port for encrypted Syslog transmissions.

QUESTION 5

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]