

GCIH^{Q&As}

GIAC Certified Incident Handler

Pass GIAC GCIH Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.leads4pass.com/gcih.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

Adam works as an Incident Handler for Umbrella Inc. His recent actions towards the incident are not up to the standard norms of the company. He always forgets some steps and procedures while handling responses as they are very hectic to perform.

Which of the following steps should Adam take to overcome this problem with the least administrative effort?

- A. Create incident manual read it every time incident occurs.
- B. Appoint someone else to check the procedures.
- C. Create incident checklists.
- D. Create new sub-team to keep check.

Correct Answer: C

QUESTION 2

Which of the following is the BEST set of methods one may use to validate a system once operations have been restored during the Recovery phase of Incident Handling?

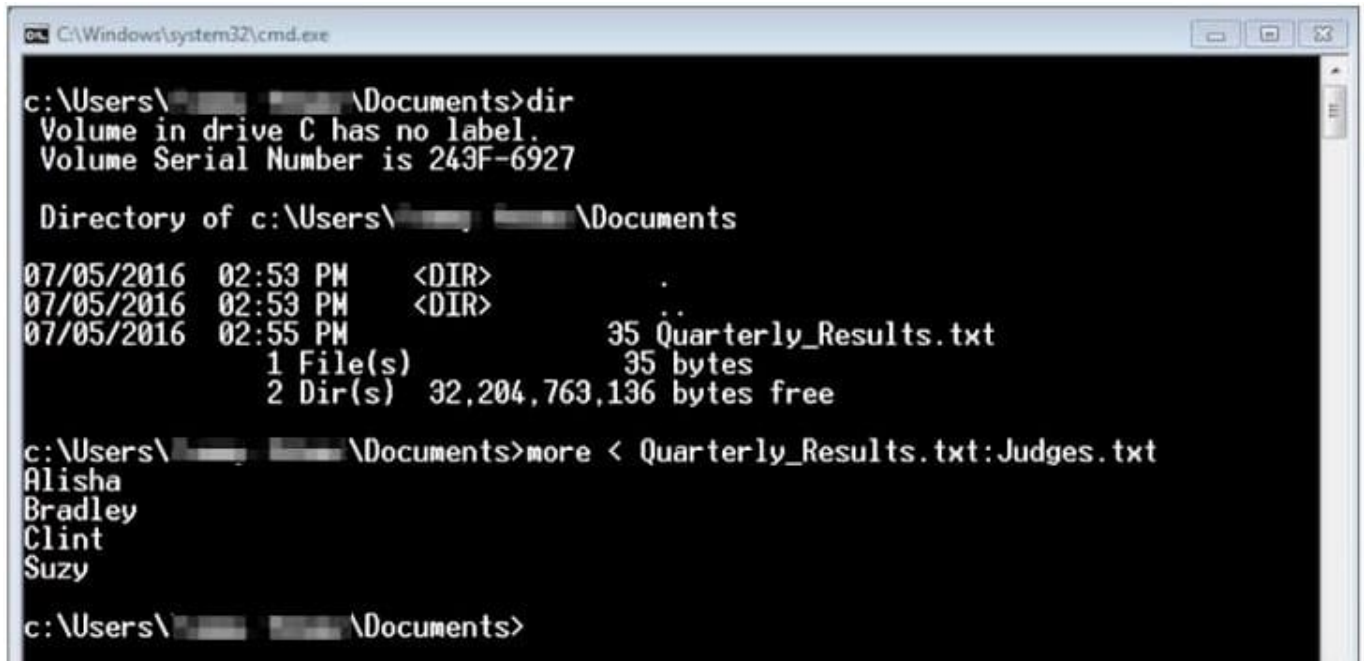
- A. Ensure the system boots, verify the applications start, and check network connectivity
- B. Obtain legal sign-off, validate the system recovery, and obtain incident handler sign-off
- C. Monitor syslog activity, create IDS signatures, and review the firewall configuration
- D. Follow test plans, use baseline documentation, and utilize business unit testing

Correct Answer: D

Documented test plans, baseline performance or behavior, and business unit testing can be used to validate that a system is back online and behaving as it should.

QUESTION 3

As indicated in the following image, an analyst runs the dir and more commands. What can the analyst conclude about Judges.txt?



```
C:\Windows\system32\cmd.exe
c:\Users\... \Documents>dir
Volume in drive C has no label.
Volume Serial Number is 243F-6927

Directory of c:\Users\... \Documents
07/05/2016  02:53 PM    <DIR>          .
07/05/2016  02:53 PM    <DIR>          ..
07/05/2016  02:55 PM                35 Quarterly_Results.txt
                1 File(s)        35 bytes
                2 Dir(s)  32,204,763,136 bytes free

c:\Users\... \Documents>more < Quarterly_Results.txt:Judges.txt
Alisha
Bradley
Clint
Suzy

c:\Users\... \Documents>
```

- A. The file size is 35 bytes
- B. The file is encoded by Quarterly_Results.txt
- C. It is on a FAT partition
- D. It is an alternate data stream

Correct Answer: A

QUESTION 4

What command would you issue on a Windows 7 system in order to list the open TCP and UDP ports and connections to these ports?

- A. Net use /all
- B. Nslookup all
- C. Netshell firewall show config
- D. Netstat -an

Correct Answer: D

QUESTION 5

Which of the following refers to the exploitation of a valid computer session to gain unauthorized access to information or services in a computer system?

- A. Piggybacking

B. Hacking

C. Session hijacking

D. Keystroke logging

Correct Answer: C

[Latest GCIH Dumps](#)

[GCIH Study Guide](#)

[GCIH Exam Questions](#)