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.geekcert.com/gcih.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by GIAC Official Exam Center

QUESTION 1

What is one of the functions CyberCPR performs?

A. It can act as a NIDS when traffic is routed through it

B. All uploaded files are hashed

C. CyperCPR can act as an secure email server

D. It can act as a HIDS on the system it is installed on

Correct Answer: A

QUESTION 2

What kind of topics should be addressed by the Lessons Learned report?

A. Official press release, evidence from the intrusion, and future testing plans

B. Process modifications, technology needs, and incident handling improvements

C. Personnel issues, disciplinary actions, and mistakes made by incident handlers

D. Individual accounts of the incident, system log entries, and legal warrants

Correct Answer: B

The Lessons Learned report should address process improvements, technology recommendations, and improvements that can be made to the Incident Handling process.

QUESTION 3

Analyze the data shown below. Where does this data originate from?

```
? (172.16.62.254) at 00:50:56:e8:b1:4b [ether] on eth0
? (172.16.62.2) at 00:50:56:e8:68:e7 [ether] on eth0
? (172.16.62.84) at 04:b0:77:81:90:5f [ether] on eth0
? (172.16.62.102) at 30:40:50:d3:14:af [ether] on eth0
```

A. Established connections

B. Routing table

C. ARP cache

D. Network interfaces

Correct Answer: C

Reference: https://petri.com/csc_arp_cache

QUESTION 4

Observe the following command; what is the analyst doing?

A. Connecting to an SMB share on 192.168.230.138

B. Listing active network connections to 192.168.230.138

C. Determining what services are running on 192.168.230.138

D. Acquiring a memory image from 192.168.230.138

Correct Answer: B

Reference: https://superuser.com/questions/486886/run-wmic-command-across-network

QUESTION 5

You discover that your network routers are being flooded with broadcast packets that have the return address of one of the servers on your network. This is resulting in an overwhelming amount of traffic going back to that server and flooding it. What is this called?

A. Syn flood

B. Blue jacking

C. Smurf attack

D. IP spoofing

Correct Answer: C