



CFR-310^{Q&As}

CyberSec First Responder

Pass CertNexus CFR-310 Exam with 100% Guarantee

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

<https://www.geekcert.com/cfr-310.html>

100% Passing Guarantee
100% Money Back Assurance

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

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





QUESTION 1

A Linux system administrator found suspicious activity on host IP 192.168.10.121. This host is also establishing a connection to IP 88.143.12.123. Which of the following commands should the administrator use to capture only the traffic between the two hosts?

- A. # tcpdump -i eth0 host 88.143.12.123
- B. # tcpdump -i eth0 dst 88.143.12.123
- C. # tcpdump -i eth0 host 192.168.10.121
- D. # tcpdump -i eth0 src 88.143.12.123

Correct Answer: B

QUESTION 2

During a log review, an incident responder is attempting to process the proxy server's log files but finds that they are too large to be opened by any file viewer. Which of the following is the MOST appropriate technique to open and analyze these log files?

- A. Hex editor, searching
- B. tcpdump, indexing
- C. PE Explorer, indexing
- D. Notepad, searching

Correct Answer: A

Reference: <https://superuser.com/questions/45142/hex-editor-for-large-files-in-linux>

QUESTION 3

A company help desk is flooded with calls regarding systems experiencing slow performance and certain Internet sites taking a long time to load or not loading at all. The security operations center (SOC) analysts who receive these calls take the following actions:

-Running antivirus scans on the affected user machines

-

Checking department membership of affected users

-

Checking the host-based intrusion prevention system (HIPS) console for affected user machine alerts

-



Checking network monitoring tools for anomalous activities

Which of the following phases of the incident response process match the actions taken?

- A. Identification
- B. Preparation
- C. Recovery
- D. Containment

Correct Answer: A

QUESTION 4

A secretary receives an email from a friend with a picture of a kitten in it. The secretary forwards it to the ~COMPANYWIDE mailing list and, shortly thereafter, users across the company receive the following message:

“You seem tense. Take a deep breath and relax!”

The incident response team is activated and opens the picture in a virtual machine to test it. After a short analysis, the following code is found in C:

```
\Temp\chill.exe:Powershell.exe -Command "do {(for /L %i in (2,1,254) do shutdown /r /m Error! Hyperlink reference not valid.&gt; /f /t / 0 (/c "You seem tense. Take a deep breath and relax!");Start-Sleep -s 900) } while(1)"
```

Which of the following BEST represents what the attacker was trying to accomplish?

- A. Taunt the user and then trigger a shutdown every 15 minutes.
- B. Taunt the user and then trigger a reboot every 15 minutes.
- C. Taunt the user and then trigger a shutdown every 900 minutes.
- D. Taunt the user and then trigger a reboot every 900 minutes.

Correct Answer: B

QUESTION 5

As part of an organization's regular maintenance activities, a security engineer visits the Internet Storm Center advisory page to obtain the latest list of blacklisted host/network addresses. The security engineer does this to perform which of the following activities?

- A. Update the latest proxy access list
- B. Monitor the organization's network for suspicious traffic
- C. Monitor the organization's sensitive databases



D. Update access control list (ACL) rules for network devices

Correct Answer: D

[Latest CFR-310 Dumps](#)

[CFR-310 Exam Questions](#)

[CFR-310 Braindumps](#)