CFR-410 ^{Q&As}

CyberSec First Responder (CFR)

Pass CertNexus CFR-410 Exam with 100% Guarantee

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

https://www.leads4pass.com/cfr-410.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

When attempting to determine which system or user is generating excessive web traffic, analysis of which of the following would provide the BEST results?

A. Browser logs

B. HTTP logs

C. System logs

D. Proxy logs

Correct Answer: D

Reference: https://www.exabeam.com/siem-guide/events-and-logs/

QUESTION 2

An incident at a government agency has occurred and the following actions were taken:

-Users have regained access to email accounts

-Temporary VPN services have been removed

-Host-based intrusion prevention system (HIPS) and antivirus (AV) signatures have been updated

-

Temporary email servers have been decommissioned

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

A.

Containment

B.

Post-incident

C.

Recovery

D. Identification

Correct Answer: A

QUESTION 3

After imaging a disk as part of an investigation, a forensics analyst wants to hash the image using a tool that supports piecewise hashing. Which of the following tools should the analyst use?

A. md5sum

B. sha256sum

C. md5deep

D. hashdeep

Correct Answer: A

QUESTION 4

Which of the following is the FIRST step taken to maintain the chain of custody in a forensic investigation?

A. Security and evaluating the electronic crime scene.

B. Transporting the evidence to the forensics lab

C. Packaging the electronic device

D. Conducting preliminary interviews

Correct Answer: C

QUESTION 5

In which of the following attack phases would an attacker use Shodan?

A. Scanning

B. Reconnaissance

C. Gaining access

D. Persistence

Correct Answer: A

Reference: https://books.google.com.pk/books?id=3bzPDwAAQBAJandpg=PA41andlpg=PA41anddq=attack+phases+w ould+an+attacker+use +Shodanandsource=blandots=phUbfR8BOYandsig=ACfU3U1sg5J67s_sL_Ixpr3OiqdCIraKUwan dhl=enandsa=Xandved=2ahUKEwjazaKCssXpAhUC4YUKHcJ5CVwQ6AEwAXoECBMQAQ#v=onepageandq=attack% 20phases%20would%20an%20attacker %20use%20Shodanandf=false

[CFR-410 Study Guide](#)   [CFR-410 Exam Questions](#)   [CFR-410 Braindumps](#)