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

QUESTION 1

Which of the following is the GREATEST risk of having security information and event management (SIEM) collect computer names with older log entries?

A. There may be duplicate computer names on the network.

B. The computer name may not be admissible evidence in court.

C. Domain Name System (DNS) records may have changed since the log was created.

D. There may be field name duplication when combining log files.

Correct Answer: D

QUESTION 2

A security engineer is setting up security information and event management (SIEM). Which of the following log sources should the engineer include that will contain indicators of a possible web server compromise? (Choose two.)

A. NetFlow logs

B. Web server logs

C. Domain controller logs

D. Proxy logs

E. FTP logs

Correct Answer: BC

Reference: https://www.techrepublic.com/blog/data-center/top-three-indicators-of-compromised-web-servers/

QUESTION 3

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.andgt; /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 4

After successfully enumerating the target, the hacker determines that the victim is using a firewall. Which of the following techniques would allow the hacker to bypass the intrusion prevention system (IPS)?

A. Stealth scanning

B. Xmas scanning

C. FINS scanning

D. Port scanning

Correct Answer: C

Reference: https://nmap.org/book/firewall-subversion.html

QUESTION 5

A Linux administrator is trying to determine the character count on many log files. Which of the following command and flag combinations should the administrator use?

A. tr -d

B. uniq -c

C. wc -m

D. grep -c

Correct Answer: C

Reference: https://cmdlinetips.com/2011/08/how-to-count-the-number-of-lines-words-and-characters-in-a-text-file-from-terminal/