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.pass4itsure.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

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 2

A Windows system administrator has received notification from a security analyst regarding new malware that executes under the process name of "armageddon.exe" along with a request to audit all department workstations for its presence. In the absence of GUI-based tools, what command could the administrator execute to complete this task?

A. ps -ef | grep armageddon

B. top | grep armageddon

C. wmic process list brief | find "armageddon.exe"

D. wmic startup list full | find "armageddon.exe"

Correct Answer: C

Reference: https://www.andreafortuna.org/2017/08/09/windows-command-line-cheatsheet-part-2-wmic/

QUESTION 3

A security investigator has detected an unauthorized insider reviewing files containing company secrets. Which of the following commands could the investigator use to determine which files have been opened by this user?

A. ls

B. lsof

C. ps

D. netstat

Correct Answer: B

Reference: https://books.google.com.pk/books?id=sxr50IxP27ACandpg=PA49andlpg=PA49anddq=linux+commands+could+the+investigator+use+to+determine+which+files+have+been+opened+by+this +userandsource=blandots=RUG5bOAhGEandsig=ACfU3U3qv3h4lGh1GQP6mdNLy1RZH-SPDgandhl=enandsa=Xandved=2ahUKEwiNpPeambbpAhVmx

4UKHVt5CeIQ6AEwAHoECBMQAQ#v=onepageandq=linux%20commands%20could%20the% 20investigator%20use%20to%20determine%20which%20files%20have%20been%20opened%20by%20this%20userandf=false

QUESTION 4

An administrator investigating intermittent network communication problems has identified an excessive amount of traffic from an external-facing host to an unknown location on the Internet. Which of the following BEST describes what is occurring?

A. The network is experiencing a denial of service (DoS) attack.

B. A malicious user is exporting sensitive data.

C. Rogue hardware has been installed.

D. An administrator has misconfigured a web proxy.

Correct Answer: B

QUESTION 5

An organization recently suffered a data breach involving a server that had Transmission Control Protocol (TCP) port 1433 inadvertently exposed to the Internet. Which of the following services was vulnerable?

A. Internet Message Access Protocol (IMAP)

B. Network Basic Input/Output System (NetBIOS)

C. Database

D. Network Time Protocol (NTP)

Correct Answer: C

Reference: http://www.princeton.edu/~rblee/ELE572Papers/Fall04Readings/DDoSSurveyPaper_20030516_Final.pdf (9)