VCE & PDF
Pass4itSure.com

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

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

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

QUESTION 2

An incident responder has collected network capture logs in a text file, separated by five or more data fields. Which of the following is the BEST command to use if the responder would like to print the file (to terminal/screen) in numerical order?

A. cat | tac

B. more

C. sort –n

D. less

Correct Answer: C

Reference: https://kb.iu.edu/d/afjb

QUESTION 3

When performing an investigation, a security analyst needs to extract information from text files in a Windows operating system. Which of the following commands should the security analyst use?

A. findstr

B. grep

C. awk

D. sigverif

Correct Answer: C

Reference: https://books.google.com.pk/books?id=8qTxCAAAQBAJandpg=PA6andlpg=PA6anddq=awk+extract+inform
ation+from+text+files+in+a+Windows+operating +systemandsource=blandots=mm7bH69viVandsig=ACfU3U2sg2lNmZ
XZW0FKQWctyfH89yAz3Qandhl=enandsa=Xandved=2ahUKEwiFioWCgbbpAhVFQBoKHavGAcUQ6AEwAHoECBQQ
AQ#v=onepageandq=awk%20extract%20information%20from%
20text%20files%20in%20a%20Windows%20operating%20systemandf=false

QUESTION 4

Which of the following are part of the hardening phase of the vulnerability assessment process? (Choose two.)

A. Installing patches

B. Updating configurations

C. Documenting exceptions

D. Conducting audits

E. Generating reports

Correct Answer: AB

QUESTION 5

A security administrator is investigating a compromised host. Which of the following commands could the investigator
use to display executing processes in real time?

A. ps

B. top

C. nice

D. pstree

Correct Answer: B

Reference: https://www.cyberciti.biz/faq/show-all-running-processes-in-linux/

CFR-410 Practice Test   CFR-410 Study Guide   CFR-410 Exam Questions