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

QUESTION 1

A security administrator needs to review events from different systems located worldwide. Which of the following is MOST important to ensure that logs can be effectively correlated?

A. Logs should be synchronized to their local time zone.

B. Logs should be synchronized to a common, predefined time source.

C. Logs should contain the username of the user performing the action.

D. Logs should include the physical location of the action performed.

Correct Answer: A

QUESTION 2

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)

QUESTION 3

While reviewing some audit logs, an analyst has identified consistent modifications to the sshd_config file for an organization\\'s server. The analyst would like to investigate and compare contents of the current file with archived versions of files that are saved weekly. Which of the following tools will be MOST effective during the investigation?

A. cat * | cut –d ‘,’ –f 2,5,7

B. more * | grep

C. diff

D. sort *

Correct Answer: C

Reference: https://www.tldp.org/LDP/abs/html/filearchiv.html

QUESTION 4

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 5

A security analyst has discovered that an application has failed to run. Which of the following is the tool MOST likely used by the analyst for the initial discovery?

A. syslog

B. MSConfig

C. Event Viewer

D. Process Monitor

Correct Answer: C