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.leads4pass.com/cfr-310.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

As part of an organization\\'s regular maintenance activities, a security engineer visits the Internet Storm Center advisory page to obtain the latest list of blacklisted host/network addresses. The security engineer does this to perform which of the following activities?

A. Update the latest proxy access list

B. Monitor the organization\\'s network for suspicious traffic

C. Monitor the organization\\'s sensitive databases

D. Update access control list (ACL) rules for network devices

Correct Answer: D

QUESTION 2

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

QUESTION 3

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 4

A company help desk is flooded with calls regarding systems experiencing slow performance and certain Internet sites taking a long time to load or not loading at all. The security operations center (SOC) analysts who receive these calls

take the following actions:

-Running antivirus scans on the affected user machines

-

Checking department membership of affected users

-

Checking the host-based intrusion prevention system (HIPS) console for affected user machine alerts

-

Checking network monitoring tools for anomalous activities

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

A. Identification

B. Preparation

C. Recovery

D. Containment

Correct Answer: A

QUESTION 5

Which of the following would MOST likely make a Windows workstation on a corporate network vulnerable to remote exploitation?

A. Disabling Windows Updates

B. Disabling Windows Firewall

C. Enabling Remote Registry

D. Enabling Remote Desktop

Correct Answer: D

Latest CFR-310 Dumps CFR-310 PDF Dumps CFR-310 Study Guide