https://www.geekcert.com/cfr-410.html
2024 Latest geekcert CFR-410 PDF and VCE dumps Download

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.geekcert.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

An incident at a government agency has occurred and the following actions were taken:

-Users have regained access to email accounts

-Temporary VPN services have been removed

-Host-based intrusion prevention system (HIPS) and antivirus (AV) signatures have been updated

-

Temporary email servers have been decommissioned

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

A.

Containment

B.

Post-incident

C.

Recovery

D. Identification

Correct Answer: A

QUESTION 2

A company that maintains a public city infrastructure was breached and information about future city projects was leaked. After the post-incident phase of the process has been completed, which of the following would be PRIMARY focus of the incident response team?

A. Restore service and eliminate the business impact.

B. Determine effective policy changes.

C. Inform the company board about the incident.

D. Contact the city police for official investigation.

Correct Answer: B

QUESTION 3

If a hacker is attempting to alter or delete system audit logs, in which of the following attack phases is the hacker

involved?

A. Covering tracks

B. Expanding access

C. Gaining persistence

D. Performing reconnaissance

Correct Answer: A

Reference: https://resources.infosecinstitute.com/category/certifications-training/ethical-hacking/covering-tracks/log-tampering-101/#gref

QUESTION 4

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+would+an+attacker+use +Shodanandsource=blandots=phUbfR8BOYandsig=ACfU3U1sg5J67s_sL_Ixpr3OiqdCIraKUwandhl=enandsa=Xandved=2ahUKEwjazaKCssXpAhUC4YUKHcJ5CVwQ6AEwAXoECBMQAQ#v=onepageandq=attack%20phases%20would%20an%20attacker %20use%20Shodanandf=false

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