



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**

An attacker intercepts a hash and compares it to pre-computed hashes to crack a password. Which of the following methods has been used?

- A. Password sniffing
- B. Brute force attack
- C. Rainbow tables
- D. Dictionary attack

Correct Answer: C

Reference: https://books.google.com.pk/books?id=knlkHAsKNRwCandpg=PA174andlpg=PA174anddq=attacker+intercepts+a+hash+and+compares+it+to+pre-computed+hashes+to+crack+a+passwordandsource=blandots=k8bSf5CPV7a&ndsig=ACfU3U1ZagQatV8sP0-7-zS7RU_EsKoQAwandhl=enandsa=Xandved=2ahUKEwj_k6f-prbpAhUBBGMBHeQaCdwQ6AEwCXoECBMQAQ#v=onepageandq=attacker%20intercepts%20a%20hash%20and%20compares%20it%20to%20pre-computed%20hashes%20to%20crack%20a%20passwordandf=false

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

Which common source of vulnerability should be addressed to BEST mitigate against URL redirection attacks?

- A. Application
- B. Users
- C. Network infrastructure
- D. Configuration files

Correct Answer: A



Reference: <https://blog.qualys.com/securitylabs/2016/01/07/open-redirection-a-simple-vulnerability-threatens-your-web-applications>

QUESTION 4

When attempting to determine which system or user is generating excessive web traffic, analysis of which of the following would provide the BEST results?

- A. Browser logs
- B. HTTP logs
- C. System logs
- D. Proxy logs

Correct Answer: D

Reference: <https://www.exabeam.com/siem-guide/events-and-logs/>

QUESTION 5

A Linux system administrator found suspicious activity on host IP 192.168.10.121. This host is also establishing a connection to IP 88.143.12.123. Which of the following commands should the administrator use to capture only the traffic between the two hosts?

- A. # tcpdump -i eth0 host 88.143.12.123
- B. # tcpdump -i eth0 dst 88.143.12.123
- C. # tcpdump -i eth0 host 192.168.10.121
- D. # tcpdump -i eth0 src 88.143.12.123

Correct Answer: B

[Latest CFR-410 Dumps](#)

[CFR-410 PDF Dumps](#)

[CFR-410 Study Guide](#)