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.leads4pass.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

SATISFACTION GUARANTEED 100% SATISFACTION GUARANTEED

QUESTION 1

While performing routing maintenance on a Windows Server, a technician notices several unapproved Windows Updates and that remote access software has been installed. The technician suspects that a malicious actor has gained access to the system. Which of the following steps in the attack process does this activity indicate?

A. Expanding access

B. Covering tracks

C. Scanning

D. Persistence

Correct Answer: A

QUESTION 2

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 3

A system administrator identifies unusual network traffic from outside the local network. Which of the following is the BEST method for mitigating the threat?

A. Malware scanning

B. Port blocking

C. Packet capturing

D. Content filtering

Correct Answer: C

QUESTION 4

Senior management has stated that antivirus software must be installed on all employee workstations. Which of the following does this statement BEST describe?

A. Guideline

B. Procedure

C. Policy

D. Standard

Correct Answer: C

QUESTION 5

Tcpdump is a tool that can be used to detect which of the following indicators of compromise?

A. Unusual network traffic

B. Unknown open ports

C. Poor network performance

D. Unknown use of protocols

Correct Answer: A

Reference: https://books.google.com.pk/books?id=b7swDwAAQBAJandpg=PA122andlpg=PA122anddq=Tcpdump+is+a +tool+that+can+be+used+to+detect+which+of+the+following+indicators+of +compromiseandsource=blandots=RxkWHHpNC4andsig=ACfU3U2L48OSw8R8HdLy2ytAuYsRDi9Hmgandhl=enandsa=Xandved=2ahUKEwi44PjnybbpAhVNzIUKHSloCJgQ6AEwAHoECBMQAQ#v=onepageandq=Tcpdump%20is%20a%20tool%20that% 20can%20be%20used%20to%20detect%20which%20of%20the%20following%20indicators%20of%20compromiseandf=false

CFR-410 VCE Dumps CFR-410 Exam Questions CFR-410 Braindumps