CFR-410$^{Q\&As}$

CyberSec First Responder (CFR)

Pass CertNexus CFR-410 Exam with 100% Guarantee

QUESTION 1

When performing an investigation, a security analyst needs to extract information from text files in a Windows operating system. Which of the following commands should the security analyst use?

A. findstr

B. grep

C. awk

D. sigverif

Correct Answer: C

Reference: https://books.google.com.pk/books?id=8qTxCAAAQBAJandpg=PA6andlpg=PA6anddq=awk+extract+information+from+text+files+in+a+Windows+operating +systemandsource=blandots=mm7bH69viVandsig=ACfU3U2sg2lNmZXZW0FKQWctyfH89yAz3Qandhl=enandsa=Xandved=2ahUKEwiFioWCgbbpAhVFQBoKHavGAcUQ6AEwAHoECBQQAQ#v=onepageandq=awk%20extract%20information%20from%20text%20files%20in%20a%20Windows%20operating%20systemandf=false

QUESTION 2

Which of the following enables security personnel to have the BEST security incident recovery practices?

A. Crisis communication plan

B. Disaster recovery plan

C. Occupant emergency plan

D. Incident response plan

Correct Answer: B

QUESTION 3

A secretary receives an email from a friend with a picture of a kitten in it. The secretary forwards it to the ~COMPANYWIDE mailing list and, shortly thereafter, users across the company receive the following message:

“You seem tense. Take a deep breath and relax!”

The incident response team is activated and opens the picture in a virtual machine to test it. After a short analysis, the following code is found in C:

\Temp\chill.exe:Powershell.exe –Command “do {(for /L %i in (2,1,254) do shutdown /r /m Error! Hyperlink reference not valid.andgt; /f /t / 0 (/c “You seem tense. Take a deep breath and relax!”);Start-Sleep –s 900) } while(1)”

Which of the following BEST represents what the attacker was trying to accomplish?

A. Taunt the user and then trigger a shutdown every 15 minutes.

B. Taunt the user and then trigger a reboot every 15 minutes.

C. Taunt the user and then trigger a shutdown every 900 minutes.

D. Taunt the user and then trigger a reboot every 900 minutes.

Correct Answer: B

QUESTION 4

A network security analyst has noticed a flood of Simple Mail Transfer Protocol (SMTP) traffic to internal clients. SMTP traffic should only be allowed to email servers. Which of the following commands would stop this attack? (Choose two.)

A. iptables -A INPUT -p tcp –dport 25 -d x.x.x.x -j ACCEPT

B. iptables -A INPUT -p tcp –sport 25 -d x.x.x.x -j ACCEPT

C. iptables -A INPUT -p tcp –dport 25 -j DROP

D. iptables -A INPUT -p tcp –destination-port 21 -j DROP

E. iptables -A FORWARD -p tcp –dport 6881:6889 -j DROP

Correct Answer: AC

QUESTION 5

During the forensic analysis of a compromised computer image, the investigator found that critical files are missing, caches have been cleared, and the history and event log files are empty. According to this scenario, which of the following techniques is the suspect using?

A. System hardening techniques

B. System optimization techniques

C. Defragmentation techniques

D. Anti-forensic techniques

Correct Answer: D