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

CyberSec First Responder (CFR)

QUESTION 1

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 2

An organization recently suffered a data breach involving a server that had Transmission Control Protocol (TCP) port 1433 inadvertently exposed to the Internet. Which of the following services was vulnerable?

A. Internet Message Access Protocol (IMAP)

B. Network Basic Input/Output System (NetBIOS)

C. Database

D. Network Time Protocol (NTP)

Correct Answer: C

Reference: http://www.princeton.edu/~rblee/ELE572Papers/Fall04Readings/DDoSSurveyPaper_20030516_Final.pdf (9)

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 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 5

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

CFR-410 PDF Dumps CFR-410 VCE Dumps CFR-410 Exam Questions