Free Questions for CFR-210 by certsinside

Shared by Cantu on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A user reports a pop-up error when starting a Windows machine. The error states that the machine has been infected with a virus and instructs the user to download a new antivirus client. In which of the following locations should the incidentresponder check to find what is generating the error message? (Choose two.)

Options:

A- Auto-start registry keys

B- Device Manager

C- Event Viewer

D- Programs and Features

E- Browser history

Answer:

A, C

Question 2

Question Type: MultipleChoice

A system administrator is informed that a user received an email containing a suspicious attachment. Which of the following methods is the FASTEST way to determine whether the file is suspicious or not?

Options:

A- Reverse engineering

B- Virus scanning

C- Virtualization

D- Sandboxing

Answer:

D

Question 3

Question Type: MultipleChoice

A forensics analyst is analyzing an executable and thinks it may have some text of interest hidden within it. Which of the following tools can the analyst use to assist in validating the suspicion?

Options:

A- lsof

B- cat command

C- hex editor

D- more

Answer:

C

Question 4

Question Type: MultipleChoice

A security auditor has been asked to analyze event logs to look for signs of suspicious behavior. The company operated on a normal workday schedule (e.g., Monday through Friday, 8 am -- 5 pm) and has implemented stringent access control policies (e.g. password complexity, failed login attempts). Which of the following provides the MOST reason for concern?

Options:

A- 15 failed login attempts taking place at 9 am.

B- Regularly occurring system calls taking place every day at midnight.

C- Two failed login attempts followed by a successful login in short succession.

D- A single instance of failed read attempts on a protected directory structure.

Answer:

A

Question 5

Question Type: **MultipleChoice**

While performing standard maintenance on a UNIX server, a system administrator notices a set of large files with .tar .gz file extensions in the /tmp folder. The system administrator reports this to a security analyst. Performing further research, the analyst has found the .tar .gz files contain information normally housed on one of the bank's data servers. Given this scenario, which of the following is MOST likely occurring?

Options:

A- A malicious actor, having breached the system, is staging collected data for exfiltration.

B- Having nearly exhausted the capacity of the home directory, a user is moving files to make room.

C- An error on the .hosts file has resultedin the data being backed up to the wrong server.

D- One of the newly hired system administrators has inadvertently backed up data to the wrong server.

Answer:

B

Question 6

Question Type: **MultipleChoice**

An outside organization has reported to the Chief Information Officer (CIO) of a company that it has received attack from a Linux system in the company's DMZ. Which of the following commands should an incident responder use to review a list of currently running programs on the potentially compromised system?

Options:

A- task manager

B- tlist

C- who

D- top

Answer:

D

Question 7

Question Type: MultipleChoice

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?

Options:

A- findstr

B- grep

C- awk

D- sigverif

Answer:

C