Free Questions for CFR-410 by dumpshq

Shared by Adkins on 29-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Various logs are collected for a data leakage case to make a forensic analysis. Which of the following are

MOST important for log integrity? (Choose two.)

Options:

A- Hash value

B- Time stamp

C- Log type

D- Modified date/time

E- Log path

Answer:

A, B

Question 2

Question Type: MultipleChoice

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?

Options:

A- syslog

B- MSConfig

C- Event Viewer

D- Process Monitor

Answer:

C

Question 3

Question Type: MultipleChoice

A Windows system administrator has received notification from a security analyst regarding new malware that executes under the process name of "armageddon.exe" along with a request to audit all department workstations for its presence. In the absence of GUI-based tools, what command could the administrator execute to complete this task?

Options:

A- ps -ef | grep armageddon

B- top | grep armageddon

C- wmic process list brief | find "armageddon.exe"

D- wmic startup list full | find "armageddon.exe"

Answer:

C

Question 4

Question Type: **MultipleChoice**

During a log review, an incident responder is attempting to process the proxy server's log files but finds that

they are too large to be opened by any file viewer. Which of the following is the MOST appropriate technique to open and analyze these log files?

Options:

A- Hex editor, searching

B- tcpdump, indexing

C- PE Explorer, indexing

D- Notepad, searching

Answer:

A

Question 5

Question Type: MultipleChoice

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?

Options:

A- cat * | cut --d ',' --f 2,5,7

B- more * | grep

C- diff

D- sort *

Answer:

C

Question 6

Question Type: **MultipleChoice**

A security administrator notices a process running on their local workstation called SvrsScEsdKexzCv.exe.

The unknown process is MOST likely:

Options:

A- Malware

B- A port scanner

C- A system process

D- An application process

Answer:

A

Question 7

Question Type: **MultipleChoice**

A security administrator needs to review events from different systems located worldwide. Which of the

following is MOST important to ensure that logs can be effectively correlated?

Options:

A- Logs should be synchronized to their local time zone.

B- Logs should be synchronized to a common, predefined time source.

C- Logs should contain the username of the user performing the action.

D- Logs should include the physical location of the action performed.

Answer:

A

Explanation:

Section: (none)

Explanation

Question 8

Question Type: MultipleChoice

Which of the following data sources could provide indication of a system compromise involving the exfiltration of data to an unauthorized destination?

Options:

A- IPS logs

B- DNS logs

C- SQL logs

D- SSL logs

Answer:

A