Free Questions for CFR-410 by actualtestdumps

Shared by Dotson on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A company website was hacked via the following SQL query:

email, passwd, login_id, full_name FROM members

WHERE email = "attacker@somewhere.com"; DROP TABLE members; --"

Which of the following did the hackers perform?

Options:

A- Cleared tracks of attacker@somewhere.com entries

B- Deleted the entire members table

C- Deleted the email password and login details

D- Performed a cross-site scripting (XSS) attack

Answer:

C

Question 2

Question Type: MultipleChoice

An incident responder discovers that the CEO logged in from their New York City office and then logged in from a location in Beijing an hour later. The incident responder suspects that the CEO's account has been

compromised. Which of the following anomalies MOST likely contributed to the incident responder's suspicion?

Options:

A- Geolocation

B- False positive

C- Geovelocity

D- Advanced persistent threat (APT) activity

Answer:

C

Question 3

Question Type: MultipleChoice

An unauthorized network scan may be detected by parsing network sniffer data for:

Options:

A- IP traffic from a single IP address to multiple IP addresses.

B- IP traffic from a single IP address to a single IP address.

C- IP traffic from multiple IP addresses to a single IP address.

D- IP traffic from multiple IP addresses to other networks.

Answer:

C

Question 4

Question Type: MultipleChoice

A security operations center (SOC) analyst observed an unusually high number of login failures on a particular database server. The analyst wants to gather supporting evidence before escalating the observation to management. Which of the following expressions will

provide login failure data for 11/24/2015?

Options:

A- grep 20151124 security_log | grep --c "login failure"

B- grep 20150124 security_log | grep "login_failure"

C- grep 20151124 security_log | grep "login"

D- grep 20151124 security_log | grep --c "login"

Answer:

C

Question 5

Question Type: MultipleChoice

A Linux administrator is trying to determine the character count on many log files. Which of the following command and flag combinations should the administrator use?

Options:

A- tr -d

B- uniq -c

C- wc -m

D- grep -c

Answer:

C

Question 6

Question Type: MultipleChoice

An administrator investigating intermittent network communication problems has identified an excessive amount of traffic from an external-facing host to an unknown location on the Internet. Which of the following

BEST describes what is occurring?

Options:

A- The network is experiencing a denial of service (DoS) attack.

B- A malicious user is exporting sensitive data.

C- Rogue hardware has been installed.

D- An administrator has misconfigured a web proxy.

Answer:

B

Question 7

Question Type: MultipleChoice

An incident response team is concerned with verifying the integrity of security information and event

management (SIEM) events after being written to disk. Which of the following represents the BEST option for addressing this concern?

Options:

A- Time synchronization

B- Log hashing

C- Source validation

D- Field name consistency

Answer:

A

Question 8

Question Type: MultipleChoice

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?

Options:

A- System hardening techniques

B- System optimization techniques

C- Defragmentation techniques

D- Anti-forensic techniques

Answer:

D

Question 9

Question Type: **MultipleChoice**

A security engineer is setting up security information and event management (SIEM). Which of the following log sources should the engineer include that will contain indicators of a possible web server compromise? (Choose two.)

Options:

A- NetFlow logs

B- Web server logs

C- Domain controller logs

D- Proxy logs

E- FTP logs

Answer:

B, C

Question 10

Question Type: MultipleChoice

According to company policy, all accounts with administrator privileges should have suffix _j

a. While reviewing Windows workstation configurations, a security administrator discovers an account without the suffix in the administrator's group. Which of the following actions should the security administrator take?

Options:

A- Review the system log on the affected workstation.

B- Review the security log on a domain controller.

C- Review the system log on a domain controller.

D- Review the security log on the affected workstation.

Answer:

B