Free Questions for CS0-002 by certsdeals

Shared by Miranda on 07-06-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: **MultipleChoice**

Which indicators can be used to detect further occurrences of a data exfiltration incident. The analyst determines backups were not performed during this time and reviews the following:

Image not found or type unknown

Which of the following should the analyst review to find out how the data was exfilltrated?

Options:

A) Monday's logs

B) Tuesday's logs

C) Wednesday's logs

D) Thursday's logs

Answer:

D

Question 2

Question Type: MultipleChoice

While reviewing log files, a security analyst uncovers a brute-force attack that is being performed against an external webmail portal. Which of the following would be BEST to prevent this type of attack from beinq successful1?

Options:

A) Implement MFA on the email portal using out-of-band code delivery.

B) Create a new rule in the IDS that triggers an alert on repeated login attempts

C) Leverage password filters to prevent weak passwords on employee accounts from being exploited.

D) Alter the lockout policy to ensure users are permanently locked out after five attempts.

E) Configure a WAF with brute force protection rules in block mode

Answer:

D

Question 3

Question Type: MultipleChoice

An organization that uses SPF has been notified emails sent via its authorized third-party partner are getting rejected A security analyst reviews the DNS entry and sees the following:

v=spfl ip4:180.10.6.5 ip4: 180.10.6.10 include: robusmail.com -all

The organization's primary mail server IP is 180.10 6.6, and the secondary mail server IP is 180.10.6.5. The organization's third-party mail provider is 'Robust Mail' with the domain name robustmail.com.

Which of the following is the MOST likely reason for the rejected emails?

Options:

A) The wrong domain name is in the SPF record.

B) The primary and secondary email server IP addresses are out of sequence.

C) SPF version 1 does not support third-party providers

D) An incorrect IP version is being used.

Answer:

A

Question 4

Question Type: **MultipleChoice**

A from the production environment to the test environment to test accuracy and functionality.

Which of the following would BEST protect the sensitivity of this data while still allowing the team to perform the testing?

Options:

A) Deidentification

B) Encoding

C) Encryption

D) Watermarking

Answer:

A

Question 5

Question Type: **MultipleChoice**

A security analyst needs to assess the web server versions on a list of hosts to determine which are running a vulnerable version of the software and output that list into an XML file named Webserverlist. Xml. The host list is provided in a file named werbserverlist,text. Which of the fallowing Nmap commands would BEST accomplish this goal?

A)

Image not found or type unknown

B)

Image not found or type unknown

C)

Image not found or type unknown

D)

Image not found or type unknown

Options:

A) Option A

B) Option B

C) Option C

D) Option D

Answer:

A

Question 6

Question Type: **MultipleChoice**

A security analyst is auditing firewall rules with the goal of scanning some known ports to check the firewall's behavior and responses. The analyst executes the following commands.

Which of the following BEST describes the firewall rule?

Options:

A) REJECT with --tcp-reset

B) DROP

C) LOG -log-tcp-sequence

D) DNAt -to-destination 1.1.1.1:3000

Answer:

A

Question 7

Question Type: MultipleChoice

A custom script monitors real-time

Options:

A) Access to logs may be delayed for some time.

B) SAML logging is not supported for cloud-based authentication.

C) Log data may be visible to other customers.

D) Logs may contain incorrect information

Answer:

A

Question 8

Question Type: MultipleChoice

While investigating an incident in a company's SIEM console, a security analyst found hundreds of failed SSH login attempts, which all occurred in rapid succession. The failed attempts were followed by a successful login on the root user Company policy allows systems administrators to manage their systems only from the company's internal network using their assigned corporate logins. Which of the following are the BEST actions the analyst can take to stop any further compromise? (Select TWO).

Options:

A) Configure /etc/sshd_config to deny root logins and restart the SSHD service.

B) Add a rule on the network IPS to block SSH user sessions

C) Configure /etc/passwd to deny root logins and restart the SSHD service.

D) Reset the passwords for all accounts on the affected system.

E) Add a rule on the perimeter firewall to block the source IP address.

F) Add a rule on the affected system to block access to port TCP/22.

Answer:

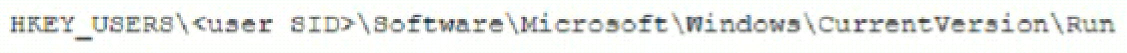
A, E

Question 9

Question Type: MultipleChoice

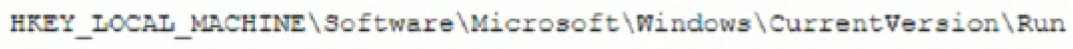
A security analyst is investigating a malware infection that occurred on a Windows system. The system was not connected to a network and had no wireless capability Company policy prohibits using portable media or mobile storage The security analyst is trying to determine which user caused the malware to get onto the system Which of the following registry keys would MOST likely have this information?

A)



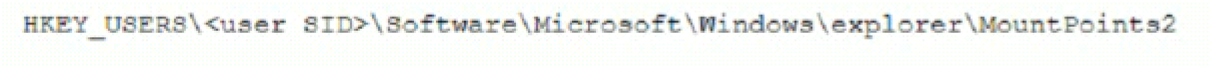
```
HKEY_USERS\<user SID>\Software\Microsoft\Windows\CurrentVersion\Run
```

B)



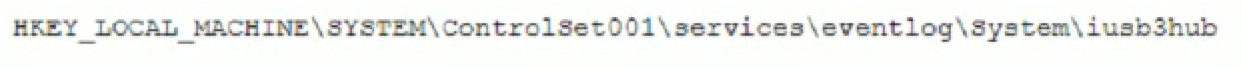
```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
```

C)



```
HKEY_USERS\<user SID>\Software\Microsoft\Windows\explorer\MountPoints2
```

D)



```
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\eventlog\System\iusb3hub
```

Options:

A) Option A

B) Option B

C) Option C

D) Option D

Answer:

C