CS0-003 Q&As

CompTIA Cybersecurity Analyst (CySA+)

Pass CompTIA CS0-003 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/cs0-003.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

An employee accessed a website that caused a device to become infected with invasive malware. The incident response analyst has:

1.

created the initial evidence log.

2.

disabled the wireless adapter on the device.

3.

interviewed the employee, who was unable to identify the website that was accessed.

4.

reviewed the web proxy traffic logs.

Which of the following should the analyst do to remediate the infected device?

A. Update the system firmware and reimage the hardware.

B. Install an additional malware scanner that will send email alerts to the analyst.

C. Configure the system to use a proxy server for Internet access.

D. Delete the user profile and restore data from backup.

Correct Answer: A

Updating the system firmware and reimaging the hardware is the best action to perform to remediate the infected device, as it helps to ensure that the device is restored to a clean and secure state and that any traces of malware are removed. Firmware is a type of software that controls the low-level functions of a hardware device, such as a motherboard, hard drive, or network card. Firmware can be updated or flashed to fix bugs, improve performance, or enhance security. Reimaging is a process of erasing and restoring the data on a storage device, such as a hard drive or a solid state drive, using an image file that contains a copy of the operating system, applications, settings, and files. Reimaging can help to recover from system failures, data corruption, or malware infections. Updating the system firmware and reimaging the hardware can help to remediate the infected device by removing any malicious code or configuration changes that may have been made by the malware, as well as restoring any missing or damaged files or settings that may have been affected by the malware. This can help to prevent further damage, data loss, or compromise of the device or the network. The other actions are not as effective or appropriate as updating the system firmware and reimaging the hardware, as they do not address the root cause of the infection or ensure that the device is fully cleaned and secured. Installing an additional malware scanner that will send email alerts to the analyst may help to detect and remove some types of malware, but it may not be able to catch all malware variants or remove them completely. It may also create conflicts or performance issues with other security tools or systems on the device. Configuring the system to use a proxy server for Internet access may help to filter or monitor some types of malicious traffic or requests, but it may not prevent or remove malware that has already infected the device or that uses other methods of communication or propagation. Deleting the user profile and restoring data from backup may help to recover some data or settings that may have been affected by the malware, but it may not remove malware that has infected other parts of the system or that has persisted on the device.

QUESTION 2

Which of the following concepts is using an API to insert bulk access requests from a file into an identity management system an example of?

A. Command and control

B. Data enrichment

C. Automation

D. Single sign-on

Correct Answer: C

Using an API to insert bulk access requests from a file into an identity management system is an example of automation. Automation involves using technology, like APIs, scripts, or tools, to perform tasks and processes automatically without manual intervention.

QUESTION 3

A security analyst discovers the following firewall log entries during an incident:

Source	Destination	Destination port	Bytes	Flags
10.0.30.100	10.0.40.20	21	0	syn
10.0.30.100	10.0.40.20	22	0	syn
10.0.30.100	10.0.40.20	80	0	syn
10.0.30.100	10.0.40.20	443	0	syn
10.0.30.100	10.0.40.20	3389	0	syn
10.0.30.100	10.0.40.20	445	0	syn

Which of the following is MOST likely occurring?

A. Banner grabbing

B. Port scanning

C. Beaconing

D. Data exfiltration

Correct Answer: B

QUESTION 4

The security analyst received the monthly vulnerability report. The following findings were included in the report:

1.

Five of the systems only required a reboot to finalize the patch application

2.

Two of the servers are running outdated operating systems and cannot be patched

The analyst determines that the only way to ensure these servers cannot be compromised is to isolate them. Which of the following approaches will best minimize the risk of the outdated servers being compromised?

A. Compensating controls

B. Due diligence

C. Maintenance windows

D. Passive discovery

Correct Answer: A

Compensating controls are the best approach to minimize the risk of the outdated servers being compromised, as they can provide an alternative or additional layer of security when the primary control is not feasible or effective. Compensating controls are security measures that are implemented to mitigate the risk of a vulnerability or an attack when the primary control is not feasible or effective. For example, if the servers are running outdated operating systems and cannot be patched, a compensating control could be to isolate them from the rest of the network, or to implement a firewall or an intrusion prevention system to monitor and block any malicious traffic to or from the servers. Compensating controls can help reduce the likelihood or impact of an exploit, but they do not eliminate the risk completely. Therefore, the security analyst should also consider upgrading or replacing the outdated servers as soon as possible.

QUESTION 5

An incident response team found IoCs in a critical server. The team needs to isolate and collect technical evidence for further investigation. Which of the following pieces of data should be collected first in order to preserve sensitive information before isolating the server?

A. Hard disk

B. Primary boot partition

C. Malicious tiles

D. Routing table

E. Static IP address

Correct Answer: D