CS0-002 Q&As

CompTIA Cybersecurity Analyst (CySA+)

Pass CompTIA CS0-002 Exam with 100% Guarantee

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

https://www.geekcert.com/cs0-002.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

A newly appointed Chief Information Security Officer (CISO) has completed a risk assessment review of the organization and wants to reduce the numerous risks that were identified. Which of the following will provide a trend of risk mitigation?

A. Risk response

B. Risk analysis

C. Planning

D. Oversight

E. Continuous monitoring

Correct Answer: B

QUESTION 2

HOTSPOT

Malware is suspected on a server in the environment. The analyst is provided with the output of commands from servers in the environment and needs to review all output files in order to determine which process running on one of the servers

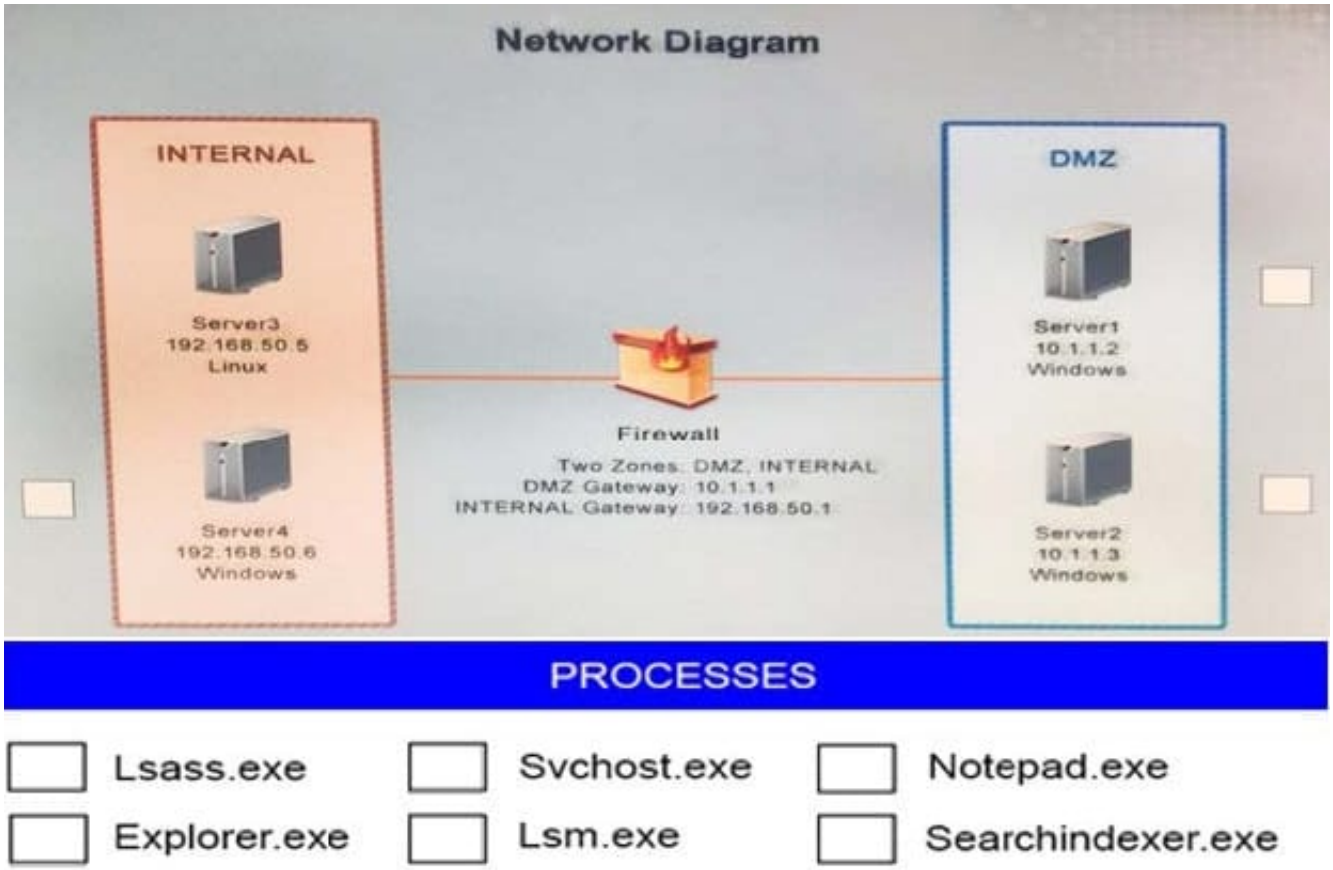
may be malware. Servers 1, 2 and 4 are clickable. Select the Server which hosts the malware, and select the process which hosts this malware.

Instructions:

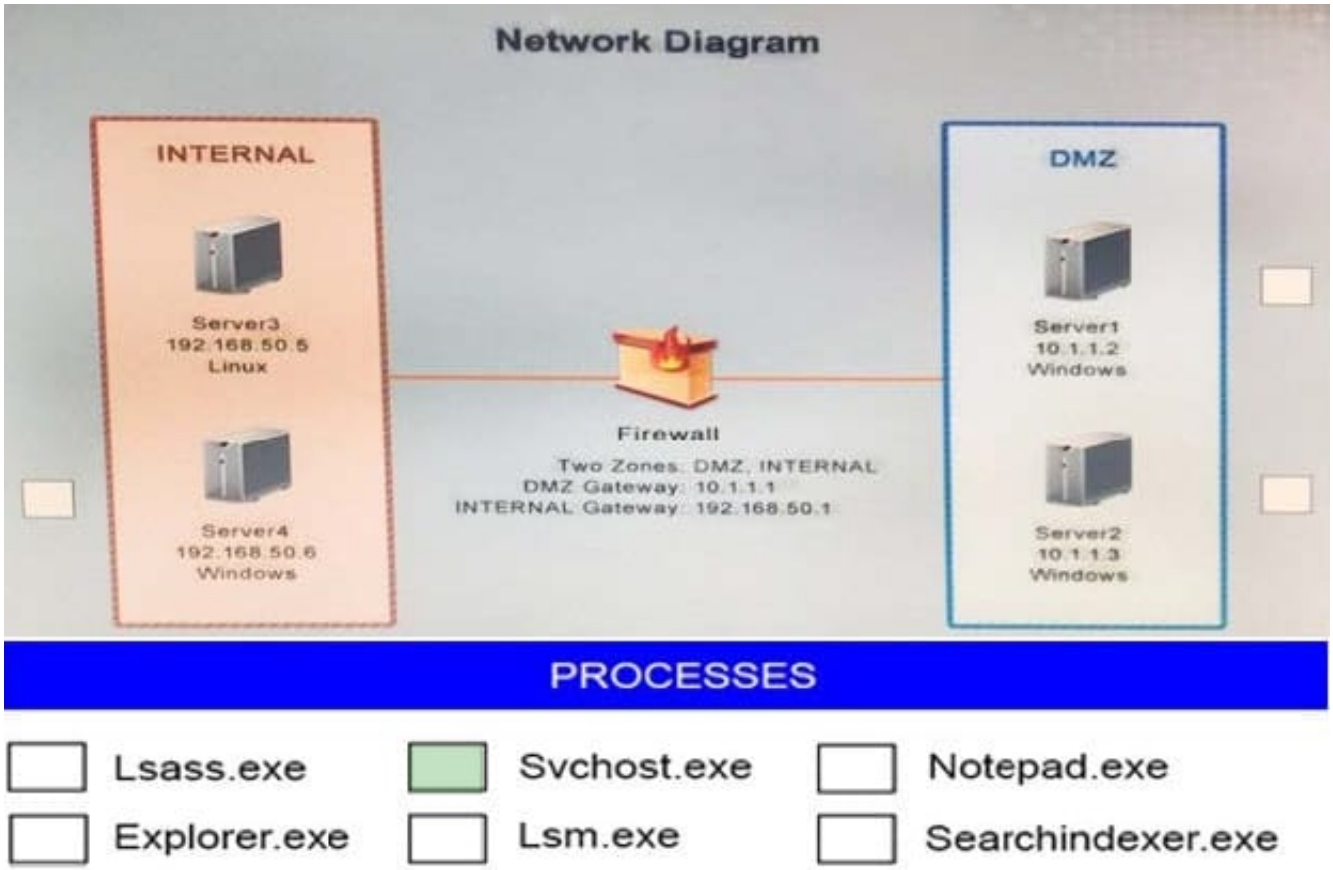
If any time you would like to bring back the initial state of the simulation, please select the Reset button.

When you have completed the simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.

Hot Area:



Correct Answer:



QUESTION 3

A company recently experienced financial fraud, which included shared passwords being compromised and improper levels of access being granted. The company has asked a security analyst to help improve its controls. Which of the following will MOST likely help the security analyst develop better controls?

A. An evidence summarization

B. An incident response plan

C. A lessons-learned report

D. An indicator of compromise

Correct Answer: C

QUESTION 4

A security analyst\\'s daily review of system logs and SIEM showed fluctuating patterns of latency. During the analysis, the analyst discovered recent attempts of intrusion related to malware that overwrites the MBR. The facilities manager informed the analyst that a nearby construction project damaged the primary power lines, impacting the analyst\\'s support systems. The electric company has temporarily restored power, but the area may experience temporary outages.

Which of the following issues the analyst focus on to continue operations?

A. Updating the ACL

B. Conducting backups

C. Virus scanning

D. Additional log analysis

Correct Answer: C

QUESTION 5

A security analyst is reviewing the following log from an email security service.

```
Rejection type:           Drop
Rejection description:    IP found in RBL
Event time:               Today at 16:06
Rejection information:    mail.comptia.org
                          https://www.spamfilter.org/query?P=192.167.28.243
From address:             user@comptex.org
To address:               tests@comptia.org
IP address:               192.167.28.243
Remote server name:       192.167.28.243
```

Which of the following BEST describes the reason why the email was blocked?

A. The To address is invalid.

B. The email originated from the www.spamfilter.org URL.

C. The IP address and the remote server name are the same.

D. The IP address was blacklisted.

E. The From address is invalid.

Correct Answer: C

Reference: https://www.webopedia.com/TERM/R/RBL.html