



Free Questions for SY0-601 by go4braindumps

Shared by Merritt on 05-09-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: DragDrop

An attack has occurred against a company.

INSTRUCTIONS

You have been tasked to do the following:

Identify the type of attack that is occurring on the network by clicking on the attacker's tablet and reviewing the output. (Answer Area 1).

Identify which compensating controls should be implemented on the assets, in order to reduce the effectiveness of future attacks by dragging them to the correct server.

(Answer area 2) All objects will be used, but not all placeholders may be filled. Objects may only be used once.

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

Image not found or type unknown



Image not found or type unknown



Answer:

Question 2

Question Type: MultipleChoice

A security analyst was called to investigate a file received directly from a hardware manufacturer. The analyst is trying to determine whether the file was modified in transit before installation on the user's computer. Which of the following can be used to safely assess the file?

Options:

- A) Check the hash of the installation file
- B) Match the file names
- C) Verify the URL download location
- D) Verify the code-signing certificate

Answer:

A

Question 3

Question Type: MultipleChoice

A implementing a DLP solution In order to reslnct PHI documents which of the following should be performed FIRST?

Options:

- A) Retention
- B) Governance
- C) Classification
- D) Change management

Answer:

A

Question 4

Question Type: MultipleChoice

After a recent security breach a security analyst reports that several administrative usernames and passwords are being sent via cleartext across the network to access network devices over port 23. Which of the following should be implemented so all credentials sent over the network are encrypted when remotely accessing and configuring network devices?

Options:

- A) SSH
- B) SNMPv3
- C) SFTP
- D) Telnet
- E) FTP

Answer:

D

Question 5

Question Type: MultipleChoice

A forensics investigator is examining a number of unauthorized payments that were reported on the company's website. Some unusual log entries show users received an email for an unwanted mailing list and clicked on a link to attempt to unsubscribe. One of the users reported the email to the phishing team, and the forwarded email revealed the link to be:

Which of the following will the forensics investigator MOST likely determine has occurred?

Options:

- A) SQL injection
- B) CSRF
- C) XSS
- D) XSRF

Answer:

D

Question 6

Question Type: MultipleChoice

Due to unexpected circumstances, an IT company must vacate its main office, forcing all operations to alternate, off-site locations Which of the following will the company MOST likely reference for guidance during this change?

Options:

- A) The business continuity plan
- B) The retention policy
- C) The disaster recovery plan
- D) The incident response plan

Answer:

B

Question 7

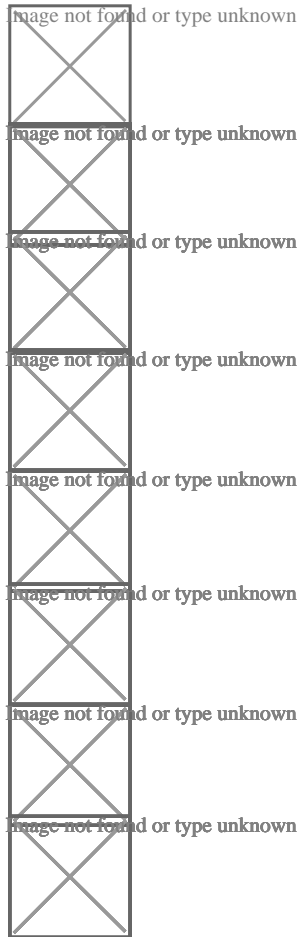
Question Type: DragDrop

A security engineer is setting up passwordless authentication for the first time.

INSTRUCTIONS

Use the minimum set of commands to set this up and verify that it works. Commands cannot be reused.

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



Question 8

Question Type: MultipleChoice

A company recently added a DR site and is redesigning the network. Users at the DR site are having issues browsing websites.

INSTRUCTIONS

Click on each firewall to do the following:

Deny cleartext web traffic.

Ensure secure management protocols are used. Resolve issues at the DR site.

The ruleset order cannot be modified due to outside constraints.

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

Image not found or type unknown



Image not found or type unknown



Image not found or type unknown



Options:

A) Explanation:

Firewall 1:

DNS Rule -- ANY --> ANY --> DNS --> PERMIT

HTTPS Outbound -- 10.0.0.1/24 --> ANY --> HTTPS --> PERMIT

Management -- ANY --> ANY --> SSH --> PERMIT

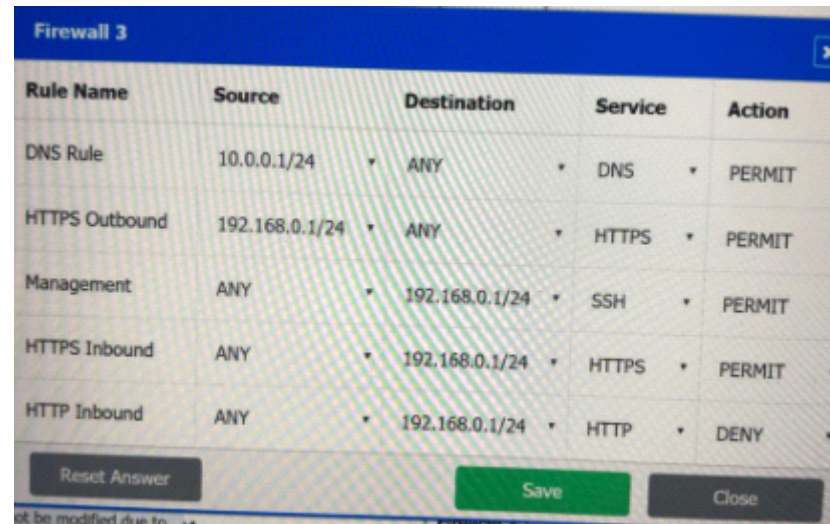
HTTPS Inbound -- ANY --> ANY --> HTTPS --> PERMIT

HTTP Inbound -- ANY --> ANY --> HTTP --> DENY

Firewall 2:

No changes should be made to this firewall

Firewall 3:

A screenshot of a network configuration interface for Firewall 3. It displays a table with five rows of firewall rules. The columns are Rule Name, Source, Destination, Service, and Action. The rules are: DNS Rule (Source: 10.0.0.1/24, Destination: ANY, Service: DNS, Action: PERMIT), HTTPS Outbound (Source: 192.168.0.1/24, Destination: ANY, Service: HTTPS, Action: PERMIT), Management (Source: ANY, Destination: 192.168.0.1/24, Service: SSH, Action: PERMIT), HTTPS Inbound (Source: ANY, Destination: 192.168.0.1/24, Service: HTTPS, Action: PERMIT), and HTTP Inbound (Source: ANY, Destination: 192.168.0.1/24, Service: HTTP, Action: DENY). At the bottom of the table, there are three buttons: 'Reset Answer', 'Save', and 'Close'.

Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.0.1/24	ANY	DNS	PERMIT
HTTPS Outbound	192.168.0.1/24	ANY	HTTPS	PERMIT
Management	ANY	192.168.0.1/24	SSH	PERMIT
HTTPS Inbound	ANY	192.168.0.1/24	HTTPS	PERMIT
HTTP Inbound	ANY	192.168.0.1/24	HTTP	DENY

Rule Name	Source	Destination	Service	Action
DNS Rule	10.0.0.1/24	ANY	DNS	PERMIT
HTTPS Outbound	192.168.0.1/24	ANY	HTTPS	PERMIT
Management	ANY	192.168.0.1/24	SSH	PERMIT
HTTPS Inbound	ANY	192.168.0.1/24	HTTPS	PERMIT
HTTP Inbound	ANY	192.168.0.1/24	HTTP	DENY

DNS Rule -- ANY --> ANY --> DNS --> PERMIT

HTTPS Outbound -- 192.168.0.1/24 --> ANY --> HTTPS --> PERMIT

Management -- ANY --> ANY --> SSH --> PERMIT

HTTPS Inbound -- ANY --> ANY --> HTTPS --> PERMIT

HTTP Inbound -- ANY --> ANY --> HTTP --> DENY

Answer:

A

Question 9

Question Type: MultipleChoice

Which of the following will MOST likely adversely impact the operations of unpatched traditional programmable-logic controllers, running a back-end LAMP server and OT systems with human-management interfaces that are accessible over the Internet via a web interface? (Choose two.)

Options:

- A) Cross-site scripting
- B) Data exfiltration
- C) Poor system logging
- D) Weak encryption
- E) SQL injection
- F) Server-side request forgery

Answer:

D, F

To Get Premium Files for SY0-601 Visit

<https://www.p2pexams.com/products/sy0-601>

For More Free Questions Visit

<https://www.p2pexams.com/comptia/pdf/sy0-601>

