Free Questions for SY0-601 by certscare

Shared by Powell on 18-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A new security engineer has started hardening systems. One of the hardening techniques the engineer is using involves disabling remote logins to the NAS. Users are now reporting the inability to use SCP to transfer files to the NAS, even though the data is still viewable from the users' PCs. Which of the following is the MOST likely cause of this issue?

A TFTP was disabled on the local hosts

Options:

B) SSH was turned off instead of modifying the configuration file

C) Remote login was disabled in the networkd.conf instead of using the sshd.conf.

D) Network services are no longer running on the NAS.

Answer:

B

Explanation:

Disabling remote logins to the NAS likely involved turning off SSH instead of modifying the configuration file. This would prevent users from using SCP to transfer files to the NAS, even though the data is still viewable from the users' PCs. Source: TechTarget

Question 2

Question Type: MultipleChoice

During an assessment, a systems administrator found several hosts running FTP and decided to immediately block FTP communications at the firewall. Which of the following describes the

greatest risk associated with using FTP?

A Private data can be leaked

Options:

B) FTP is prohibited by internal policy.

C) Users can upload personal files

D) Credentials are sent in cleartext.

Answer:

D

Explanation:

Credentials are sent in cleartext is the greatest risk associated with using FTP. FTP is an old protocol that does not encrypt the data or the credentials that are transmitted over the network. This means that anyone who can capture the network traffic can see the usernames and passwords of the FTP users, as well as the files they are transferring. This can lead to data breaches, identity theft, and unauthorized access. Private data can be leaked (Option A) is a possible consequence of using FTP, but not the root cause of the risk. FTP is prohibited by internal policy (Option B) is a compliance issue, but not a technical risk.Users can upload personal files (Option C) is a management issue, but not a security risk

https://www.infosectrain.com/blog/comptia-security-sy0-601-domain-5-governance-risk-and-compliance/

Question 3

Question Type: **MultipleChoice**

A security administrator is managing administrative access to sensitive systems with the following requirements:

* Common login accounts must not be used for administrative duties.

* Administrative accounts must be temporal in nature.

* Each administrative account must be assigned to one specific user.

* Accounts must have complex passwords.

' Audit trails and logging must be enabled on all systems.

Which of the following solutions should the administrator deploy to meet these requirements? (Give Explanation and References from CompTIA Security+ SY0-601 Official Text Book and Resources)

Options:

A) ABAC

B) SAML

C) PAM

D) CASB

Answer:

C

Explanation:

PAM is a solution that enables organizations to securely manage users' accounts and access to sensitive systems. It allows administrators to create unique and complex passwords for each user, as well as assign each account to a single user for administrative duties. PAM also provides audit trails and logging capabilities, allowing administrators to monitor user activity and ensure that all systems are secure. According to the CompTIA Security+ SY0-601 Course Book, ''PAM is the most comprehensive way to control and monitor privileged accounts''.

Question 4

Question Type: MultipleChoice

Leveraging the information supplied below, complete the CSR for the server to set up TLS (HTTPS)

* Hostname: ws01

* Domain: comptia.org

* IPv4: 10.1.9.50

* IPV4: 10.2.10.50

* Root: home.aspx

* DNS CNAME:homesite.

Instructions:

Drag the various data points to the correct locations within the CSR. Extension criteria belong in the let hand column and values belong in the corresponding row in the right hand column.

Image not found or type unknown

Image not found or type unknown

A security administrator needs to add fault tolerance and load balancing to the connection from the file server to the backup storage. Which of the following is the best choice to achieve this objective?

Options:

A) Multipathing

B) RAID

C) Segmentation

D) 8021.1

Answer:

A

Explanation:

to achieve the objective of adding fault tolerance and load balancing to the connection from the file server to the backup storage ismultipathing1.Multipathing is a technique that allows a system to use more than one path to access a storage device1.This can improve performance by distributing the workload across multiple paths, and also provide fault tolerance by switching to an alternative path if one path fails1.Multipathing can be implemented using software or hardware solutions1.

Question 5

Question Type: **MultipleChoice**

Given the following snippet of Python code:

Which of the following types of malware MOST likely contains this snippet?

Options:

A) Logic bomb

B) Keylogger

C) Backdoor

D) Ransomware

Answer:

A

Explanation:

A logic bomb is a type of malware that executes malicious code when certain conditions are met. A logic bomb can be triggered by various events, such as a specific date or time, a user action, a system configuration change, or a command from an attacker. A logic bomb can perform various malicious actions, such as deleting files, encrypting data, displaying messages, or launching other malware.

The snippet of Python code shows a logic bomb that executes a function called delete_all_files() when the current date is December 25th. The code uses the datetime module to get the current date and compare it with a predefined date object. If the condition is true, the code calls the delete_all_files() function, which presumably deletes all files on the system.

Question 6

Question Type: Hotspot

A systems administrator needs to install a new wireless network for authenticated guest access. The wireless network should support 802. IX using the most secure encryption and protocol available.

Perform the following steps:

1. Configure the RADIUS server.

2. Configure the WiFi controller.

3. Preconfigure the client for an

incoming guest. The guest AD

credentials are:

User: guest01

Password: guestpass

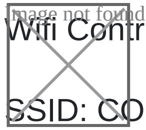
Image not found or type unknown

Wifi Controller

SSID: CORPGUEST

SHARED KEY: Secret

AAA server IP: 192.168.1.20

PSK: Blank

Authentication type: WPA2-EAP-PEAP-MSCHAPv2

Controller IP: 192.168.1.10

Radius Server

Shared Key: Secret

Client IP: 192.168.1.10

Authentication Type: Active Directory

Server IP: 192.168.1.20

Wireless Client

SSID: CORPGUEST

Username: guest01

Userpassword: guestpass

PSK: Blank

Authentication type: WPA2-Enterprise

Answer:

Question 7

Question Type: Hotspot

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

Image not found or type unknown

INSTRUCTIONS

Click on each firewall to do the following:

1. Deny cleartext web traffic

2. Ensure secure management protocols are used.

3. Resolve issues at the DR site.

The ruleset order cannot be modified due to outside constraints.

Hat any time you would like to bring back the initial state of the simulation, please dick the Reset All button.

In Firewall 1, HTTP inbound Action should be DENY. As shown below

Image not found or type unknown

In Firewall 2, Management Service should be DNS, As shown below.

Image not found or type unknown

In Firewall 3, HTTP Inbound Action should be DENY, as shown below

Image not found or type unknown

Answer:

Question 8

Question Type: DragDrop

Leveraging the information supplied below, complete the CSR for the server to set up TLS (HTTPS)

* Hostname: ws01

* Domain: comptia.org

* IPv4: 10.1.9.50

* IPV4: 10.2.10.50

* Root: home.aspx

* DNS CNAME:homesite.

Instructions:

Drag the various data points to the correct locations within the CSR. Extension criteria belong in the let hand column and values belong in the corresponding row in the right hand column.

Image not found or type unknown

A security administrator needs to add fault tolerance and load balancing to the connection from the file server to the backup storage. Which of the following is the best choice to achieve this objective?

to achieve the objective of adding fault tolerance and load balancing to the connection from the file server to the backup storage ismultipathing1.Multipathing is a technique that allows a system to use more than one path to access a storage device1.This can improve performance by distributing the workload across multiple paths, and also provide fault tolerance by switching to an alternative path if one path fails1.Multipathing can be implemented using software or hardware solutions1.

Image not found or type unknown

Image not found or type unknown

Image not found or type unknown

Image not found or type unknown

Answer:

Image not found or type unknown

Image not found or type unknown

Image not found or type unknown

Question 9

Image not found or type unknown

Image not found or type unknown

Question Type: **MultipleChoice**

Which of the following vulnerabilities is the attacker trying to exploit?

Options:

A) SSRF

B) CSRF

C) xss

D) SQLi

Answer:

D

Explanation:

SQLi stands for SQL injection, which is a type of web security vulnerability that allows an attacker to execute malicious SQL statements on a database server. SQLi can result in data theft, data corruption, denial of service, or remote code execution.

The attacker in the web server log is trying to exploit a SQLi vulnerability by sending a malicious GET request that contains a UNION ALL SELECT statement. This statement is used to combine the results of two or more SELECT queries into a single result set. The attacker is attempting to retrieve user login, user pass, and user email from the wp users table, which is a WordPress database table that stores user information. The attacker may use this information to compromise the WordPress site or the users' accounts.

Question 10

Question Type: **MultipleChoice**

DRAG DROP - 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.

Image not found or type unknown

1. ssh-keygen -t rsa (creating the key-pair)

2. ssh-copy-id -i /.ssh/id_rsa.pub user@server (copy the public-key to user@server)

3. ssh -i ~/.ssh/id_rsa user@server (login to remote host with private-key)

A small business just recovered from a ransomware attack against its file servers by purchasing the decryption keys from the attackers. The issue was triggered by a phishing email and the IT administrator wants to ensure it does not happen again. Which of the following should the IT administrator do FIRST after recovery?

Options:

A) Scan the NAS for residual or dormant malware and take new daily backups that are tested on a frequent basis.

B) Restrict administrative privileges and patch all systems and applications.

C) Rebuild all workstations and install new antivirus software.

D) Implement application whitelisting and perform user application hardening.

Answer:

A

Explanation:

The reason the company had to pay the ransom is because they did not have valid backups, otherwise they would have just restored their data. If your company just had to pay ransom and your boss says, 'Don't let this happen again', what is the first thing you are going to do. The only action after a ransomware attack is 'restore from backup'.

Question 11

Question Type: **MultipleChoice**

A security analyst is receiving numerous alerts reporting that the response time of an internet-facing application has been degraded However, the internal network performance was not degraded. Which of the following MOST likely explains this behavior?

Options:

A) DNS poisoning

B) MAC flooding

C) DDoS attack

D) ARP poisoning

Answer:

C

Question 12

Question Type: **MultipleChoice**

Which of the following documents provides expectations at a technical level for quality, availability, and responsibilities?

Options:

A) EOL

B) SLA

C) MOU

D) EOSL

Answer:

B