Free Questions for SY0-701 by certsdeals

Shared by Olsen on 13-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which of the following should a systems administrator use to ensure an easy deployment of resources within the cloud provider?

Options:

A- Software as a service

B- Infrastructure as code

C- Internet of Things

D- Software-defined networking

Answer:

B

Explanation:

Infrastructure as code (IaC) is a method of using code and automation to manage and provision cloud resources, such as servers, networks, storage, and applications. IaC allows for easy deployment, scalability, consistency, and repeatability of cloud environments. IaC is also a key component of DevSecOps, which integrates security into the development and operations processes.Reference:CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 6: Cloud and Virtualization Concepts, page 294.

Question 2

Question Type: MultipleChoice

After a recent vulnerability scan, a security engineer needs to harden the routers within the corporate network. Which of the following is the most appropriate to disable?

Options:

A- Console access

B- Routing protocols

C- VLANs

D- Web-based administration

Answer:

D

Explanation:

Web-based administration is a feature that allows users to configure and manage routers through a web browser interface. While this feature can provide convenience and ease of use, it can also pose a security risk, especially if the web interface is exposed to the internet or uses weak authentication or encryption methods. Web-based administration can be exploited by attackers to gain unauthorized access to the router's settings, firmware, or data, or to launch attacks such as cross-site scripting (XSS) or cross-site request forgery (CSRF). Therefore, disabling web-based administration is a good practice to harden the routers within the corporate network. Console access, routing protocols, and VLANs are other features that can be configured on routers, but they are not the most appropriate to disable for hardening purposes. Console access is a physical connection to the router that requires direct access to the device, which can be secured by locking the router in a cabinet or using a strong password. Routing protocols are essential for routers to exchange routing information and maintain network connectivity, and they can be secured by using authentication or encryption mechanisms. VLANs are logical segments of a network that can enhance network performance and security by isolating traffic and devices, and they can be secured by using VLAN access control lists (VACLs) or private VLANs (PVLANs). Reference:CCNA SEC: Router HardeningYour Router's Security Stinks: Here's How to Fix It

Question 3

Question Type: **MultipleChoice**

A security analyst locates a potentially malicious video file on a server and needs to identify both the creation date and the file's creator. Which of the following actions would most likely give the security analyst the information required?

Options:

A- Obtain the file's SHA-256 hash.

B- Use hexdump on the file's contents.

C- Check endpoint logs.

D- Query the file's metadata.

Answer:

D

Explanation:

Metadata is data that describes other data, such as its format, origin, creation date, author, and other attributes. Video files, like other types of files, can contain metadata that can provide useful information for forensic analysis. For example, metadata can reveal the camera model, location, date and time, and software used to create or edit the video file.To query the file's metadata, a security analyst can use various tools, such as MediaInfo1, ffprobe2, or hexdump3, to extract and display the metadata from the video file. By querying the file's metadata, the security analyst can most likely identify both the creation date and the file's creator, as well as other relevant information. Obtaining the file's SHA-256 hash, checking endpoint logs, or using hexdump on the file's contents are other possible actions, but they are not the most appropriate to answer the question. The file's SHA-256 hash is a cryptographic value that can be used to verify the integrity or uniqueness of the file, but it does not reveal any information about the file's creation date or creator. Checking endpoint logs can provide some clues about the file's origin or activity, but it may not be reliable or accurate, especially if the logs are tampered with or incomplete.Using hexdump on the file's contents can show the raw binary data of the file, but it may not be easy or feasible to interpret the metadata from the hex output, especially if the file is large or encrypted. Reference:1:How do I get the meta-data of a video file?2:How to check if an mp4 file contains malware?3: [Hexdump - Wikipedia]

Question 4

Question Type: MultipleChoice

One of a company's vendors sent an analyst a security bulletin that recommends a BIOS update. Which of the following vulnerability types is being addressed by the patch?

Options:

A- Virtualization

B- Firmware

C- Application

D- Operating system

Answer:

B

Explanation:

Firmware is a type of software that is embedded in hardware devices, such as BIOS, routers, printers, or cameras. Firmware controls the basic functions and operations of the device, and can be updated or patched to fix bugs, improve performance, or enhance security. Firmware vulnerabilities are flaws or weaknesses in the firmware code that can be exploited by attackers to gain unauthorized access, modify settings, or cause damage to the device or the network. A BIOS update is a patch that addresses a firmware vulnerability in the basic input/output system of a computer, which is responsible for booting the operating system and managing the communication between the hardware and the software. The other options are not types of vulnerabilities, but rather categories of software or technology.

Question 5

Question Type: MultipleChoice

A systems administrator wants to prevent users from being able to access data based on their responsibilities. The administrator also wants to apply the required access structure via a simplified format. Which of the following should the administrator apply to the site recovery resource group?

Options:

A- RBAC

B- ACL

C- SAML

D- GPO

Answer:

A

Explanation:

RBAC stands for Role-Based Access Control, which is a method of restricting access to data and resources based on the roles or responsibilities of users. RBAC simplifies the management of permissions by assigning roles to users and granting access rights to roles, rather than to individual users. RBAC can help enforce the principle of least privilege and reduce the risk of unauthorized access or data leakage.The other options are not as suitable for the scenario as RBAC, as they either do not prevent access based on responsibilities, or do not apply a simplified format.Reference:CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 1331

Question 6

Question Type: **MultipleChoice**

A company's end users are reporting that they are unable to reach external websites. After reviewing the performance data for the DNS severs, the analyst discovers that the CPU, disk, and memory usage are minimal, but the network interface is flooded with inbound traffic. Network logs show only a small number of DNS queries sent to this server. Which of the following best describes what the security analyst is seeing?

Options:

A- Concurrent session usage

B- Secure DNS cryptographic downgrade

C- On-path resource consumption

D- Reflected denial of service

Answer:

D

Explanation:

A reflected denial of service (RDoS) attack is a type of DDoS attack that uses spoofed source IP addresses to send requests to a third-party server, which then sends responses to the victim server. The attacker exploits the difference in size between the request and the response, which can amplify the amount of traffic sent to the victim server. The attacker also hides their identity by using the victim's IP address as the source. A RDoS attack can target DNS servers by sending forged DNS queries that generate large DNS responses.This can flood the network interface of the DNS server and prevent it from serving legitimate requests from end users.Reference:CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 215-2161

Question 7

Question Type: **MultipleChoice**

An organization is struggling with scaling issues on its VPN concentrator and internet circuit due to remote work. The organization is looking for a software solution that will allow it to reduce traffic on the VPN and internet circuit, while still providing encrypted tunnel access to the data center and monitoring of remote employee internet traffic. Which of the following will help achieve these objectives?

Options:

A- Deploying a SASE solution to remote employees

B- Building a load-balanced VPN solution with redundant internet

C- Purchasing a low-cost SD-WAN solution for VPN traffic

D- Using a cloud provider to create additional VPN concentrators

Answer:

A

Explanation:

SASE stands for Secure Access Service Edge. It is a cloud-based service that combines network and security functions into a single integrated solution. SASE can help reduce traffic on the VPN and internet circuit by providing secure and optimized access to the data center and cloud applications for remote employees. SASE can also monitor and enforce security policies on the remote employee internet traffic, regardless of their location or device.SASE can offer benefits such as lower costs, improved performance, scalability, and flexibility compared to traditional VPN solutions.Reference:CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 457-4581