SY0-601Q&As

CompTIA Security+

Pass CompTIA SY0-601 Exam with 100% Guarantee

QUESTION 1

A forensic analyst needs to prove that data has not been tampered with since it was collected

Which of the following methods will the analyst MOST likely use?

A. Look for tampenng on the evidence collection bag

B. Encrypt the collected data using asymmetric encryption

C. Ensure proper procedures for chain of custody are being followed

D. Calculate the checksum using a hashing algorithm

Correct Answer: D

A checksum is specifically intended to verify the integrity of data or find data corruption. Comparing a file\\'s original and current checksum. And if a byte or even a piece of the file\\'s data has been changed, the original and current checksum will

be different, and therefore you will know whether it\\'s the same file or not.

=====================

(A)

- This is essentially the physical version of checking if something was tampered but wouldn\\'t work for virtual data

(B)

- Dont need to encrypt anything

(C)

- Even if a proper chain of custody was followed, it doesn\\'t guarantee that data hasn\\'t been modified by anyone that had access to the data.

QUESTION 2

Which of the following allow access to remote computing resources, a operating system and centrdized configuration and data?

A. Containers

B. Edge computing

C. Thin client

D. Infrastructure as a service

Correct Answer: C

Thin clients are devices that have minimal hardware and software components and rely on a remote server to provide access to computing resources, an operating system, and centralized configuration and data. Thin clients can reduce the cost, complexity, and security risks of managing multiple devices.

QUESTION 3

To reduce and limit software and infrastructure costs, the Chief Information Officer has requested to move email services to the cloud. The cloud provider and the organization must have security controls to protect sensitive data. Which of the following cloud services would BEST accommodate the request?

A. laas

B. Paas

C. Daas

D. SaaS

Correct Answer: D

D. SaaS (Software as a Service) is the best option to accommodate the request to move email services to the cloud while protecting sensitive data. SaaS is a delivery model for software applications where the provider hosts the application and makes it available to customers over the internet. SaaS provides customers with the benefits of cloud computing such as scalability, low cost, and quick implementation without the need for expensive hardware, software, and support infrastructure. SaaS providers also have security controls in place to protect sensitive data, such as encryption, data backup, and disaster recovery. With SaaS, the customer\\'s sensitive data is stored and processed on the provider\\'s infrastructure, reducing the customer\\'s responsibility for securing the data and providing peace of mind.

QUESTION 4

An organization is building backup server rooms in geographically diverse locations The Chief Information Security Officer implemented a requirement on the project that states the new hardware cannot be susceptible to the same vulnerabilities in the existing server room

Which of the following should the systems engineer consider?

A. Purchasing hardware from different vendors

B. Migrating workloads to public cloud infrastructure

C. Implementing a robust patch management solution

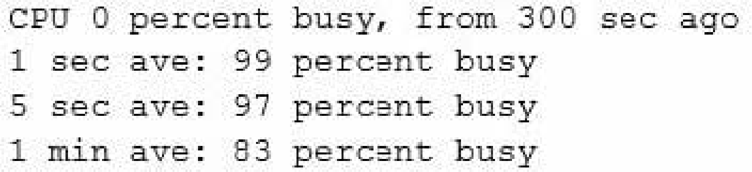
D. Designing new detective security controls

Correct Answer: A

different vendors, different products, different vulns on the devices. if you have all cisco equipment the vulns on the switches are the same.

QUESTION 5

A network administrator has been alerted that web pages are experiencing long load times. After determining it is not a routing or DNS issue, the administrator logs in to the router, runs a command, and receives the following output:



```
CPU 0 percent busy, from 300 sec ago
1 sec ave: 99 percent busy
5 sec ave: 97 percent busy
1 min ave: 83 percent busy
```

Which of the following is the router experiencing?

A. DDoS attack

B. Memory leak

C. Buffer overflow

D. Resource exhaustion

Correct Answer: D

QUESTION 6

Which of the following prevents an employee from seeing a colleague who is visting an inappropriate website?

A. Job roration policy

B. NDA

C. AUP

D. Separation of duties policy

Correct Answer: C

"Which of the following prevents an employee from visiting an inappropriate website"

.....which would somewhat make more sense. An acceptable use policy (AUP) is a document that outlines the rules and restrictions employees must follow in regard to the company\\'s network, software, internet connection and devices. The

employee shouldn\\'t access the inappropriate website as it would go against proper use of the company network.

================

Helpful Info I Guess

NDA (Non-disclosure agreement) - a binding contract between two or more parties that prevents sensitive information from being shared with others.

Separation of Duty - refers to the principle that no user should be given enough privileges to misuse the system on their own.

Job rotation - A concept that has employees rotate through different jobs to learn the procedures and processes in each. From a security perspective, job rotation helps to prevent or expose dangerous shortcuts or even fraudulent activity.

QUESTION 7

A security analyst is evaluating solutions to deploy an additional layer of protection for a web application The goal is to allow only encrypted communications without relying on network devices Which of the following can be implemented?

A. HTTP security header

B. DNSSEC implementation

C. SRTP

D. S/MIME

Correct Answer: A

When enabled on the server, HTTP Strict Transport Security (HSTS), part of HTTP Security header, enforces the use of encrypted HTTPS connections instead of plain-text HTTP communication.

QUESTION 8

A network-connected magnetic resonance imaging (MRI) scanner at a hospital is controlled and operated by an outdated and unsupported specialized Windows OS. Which of the following is most likely preventing the IT manager at the hospital from upgrading the specialized OS?

A. The time needed for the MRI vendor to upgrade the system would negatively impact patients.

B. The MRI vendor does not support newer versions of the OS.

C. Changing the OS breaches a support SLA with the MRI vendor.

D. The IT team does not have the budget required to upgrade the MRI scanner.

Correct Answer: B

This option is the most likely reason for preventing the IT manager at the hospital from upgrading the specialized OS. The MRI scanner is a complex and sensitive device that requires a specific OS to control and operate it. The MRI vendor may not have developed or tested newer versions of the OS for compatibility and functionality with the scanner. Upgrading the OS without the vendor\\'s support may cause the scanner to malfunction or stop working altogether.

QUESTION 9

A company recently enhanced mobile device configuration by implementing a set of security controls: biometrics, context-aware authentication, and full device encryption. Even with these settings in place, an unattended phone was used by a malicious actor to access corporate data.

Which of the following additional controls should be put in place first?

A. GPS tagging

B. Remote wipe

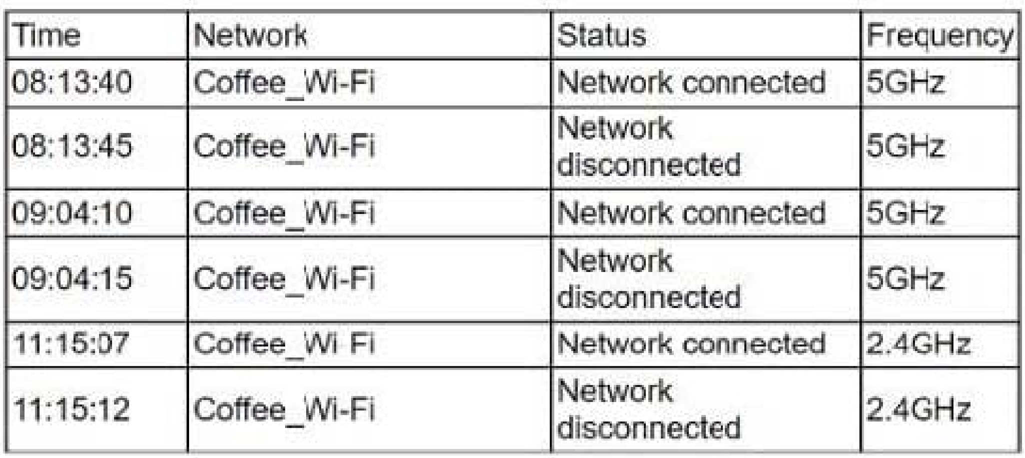
C. Screen lock timer

D. SEAndroid

Correct Answer: B

QUESTION 10

A user is having network connectivity issues when working from a coffee shop. The user has used the coffee shop as a workspace for several months without any issues. None of the other customers at the coffee shop are experiencing these issues. A help desk analyst at the user\\'s company reviews the following Wi-Fi log:



Time	Network	Status	Frequency
08:13:40	Coffee_Wi-Fi	Network connected	5GHz
08:13:45	Coffee_Wi-Fi	Network disconnected	5GHz
09:04:10	Coffee_Wi-Fi	Network connected	5GHz
09:04:15	Coffee_Wi-Fi	Network disconnected	5GHz
11:15:07	Coffee_Wi-Fi	Network connected	2.4GHz
11:15:12	Coffee_Wi-Fi	Network disconnected	2.4GHz

Which of the following best describes what is causing this issue?

A. Another customer has configured a rogue access point.

B. The coffee shop network is using multiple frequencies.

C. A denial-of-service attack by disassociation is occurring.

D. An evil twin access point is being utilized.

Correct Answer: C

QUESTION 11

A systems administrator set up an automated process that checks for vulnerabilities across the entire environment every morning. Which of the following activities is the systems administrator conducting?

A. Scanning

B. Alerting

C. Reporting

D. Archiving

Correct Answer: A

Scanning involves using automated tools to actively check the entire environment for vulnerabilities. The process typically involves using vulnerability scanning tools to identify and assess potential security weaknesses in the network, systems, and applications. The scan may include checks for known security vulnerabilities, misconfigurations, outdated software versions, and other potential issues that could be exploited by attackers.

By performing regular vulnerability scanning, the systems administrator can proactively identify and address security risks, allowing them to take appropriate measures to patch or mitigate vulnerabilities before they can be exploited by malicious actors. Scanning is an essential part of a proactive security posture and helps ensure that the organization\\'s systems and data remain secure and protected from potential threats.

QUESTION 12

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

A. EOL

B. SLA

C. MOU

D. EOSL

Correct Answer: B

A document that provides expectations at a technical level for quality, availability, and responsibilities is a Service Level Agreement (SLA). An SLA is a contract between a service provider and a customer that specifies the level of service that the provider will deliver. This typically includes technical details such as uptime, response times, and performance criteria. The SLA is used to ensure that the customer receives the level of service that they have agreed to and that the provider is held accountable for meeting those expectations. Options A, C, and D are not related to the technical level of service expectations. EOL refers to the end of life for a product or service, MOU is a memorandum of understanding, and EOSL is the end of service life.

QUESTION 13

A security administrator needs to provide secure access to internal networks for external partners The administrator has given the PSK and other parameters to the third-party security administrator. Which of the following is being used to establish this connection?

A. Kerberos

B. SSL/TLS

C. IPSec

D. SSH

Correct Answer: C

IPSec is a protocol suite that provides secure communication over IP networks. It uses encryption, authentication, and integrity mechanisms to protect data from unauthorized access or modification. IPSec can operate in two modes: transport mode and tunnel mode. In tunnel mode, IPSec can create a virtual private network (VPN) between two endpoints, such as external partners and internal networks. To establish a VPN connection, IPSec requires a pre-shared key (PSK) or other parameters to negotiate the security association.

References: https://www.comptia.org/content/guides/what-is-vpn

QUESTION 14

An organization wants to implement a third factor to an existing multifactor authentication. The organization already uses a smart card and password. Which of the following would meet the organization\\'s needs for a third factor?

A. Date of birth

B. Fingerprints

C. PIN

D. TPM

Correct Answer: B

QUESTION 15

Which of the following statements BEST describes zero-day exploits\\'?

A. When a zero-day exploit is discovered, the system cannot be protected by any means

B. Zero-day exploits have their own scoring category in CVSS

C. A zero-day exploit is initially undetectable and no patch for it exists

D. Discovering zero-day exploits is always performed via bug bounty programs

Correct Answer: C

Zero-day = Never seen before attack

Therefore it cannot be patched or recognized in a database if it has not occurred or been documented before.