

CompTIA

Exam Questions SY0-601

CompTIA Security+ Exam



NEW QUESTION 1

- (Exam Topic 3)

A building manager is concerned about people going in and out of the office during non-working hours. Which of the following physical security controls would provide the best solution?

- A. Cameras
- B. Badges
- C. Locks
- D. Bollards

Answer: B

Explanation:

Badges are physical security controls that provide a way to identify and authenticate authorized individuals who need to access a building or a restricted area. Badges can also be used to track the entry and exit times of people and monitor their movements within the premises. Badges can help deter unauthorized access by requiring people to present a valid credential before entering or leaving the office. Badges can also help prevent tailgating, which is when an unauthorized person follows an authorized person through a door or gate. Badges can be integrated with other security systems, such as locks, alarms, cameras, or biometrics, to enhance the level of protection.

NEW QUESTION 2

- (Exam Topic 3)

A local server recently crashed, and the team is attempting to restore the server from a backup. During the restore process, the team notices the file size of each daily backup is large and will run out of space at the current rate.

The current solution appears to do a full backup every night. Which of the following would use the least amount of storage space for backups?

- A. A weekly, incremental backup with daily differential backups
- B. A weekly, full backup with daily snapshot backups
- C. A weekly, full backup with daily differential backups
- D. A weekly, full backup with daily incremental backups

Answer: D

Explanation:

A weekly, full backup with daily incremental backups would use the least amount of storage space for backups, as it would only store the changes made since the last backup, whether it is a full or incremental backup. Incremental backups are faster and use less storage space than full or differential backups, but they require more time and media to restore data. A full backup is a complete copy of all data, which requires more time and storage space to perform, but allows a faster and easier recovery. A differential backup is a copy of the data that changed since the last full backup, which requires less time and storage space than a full backup, but more than an incremental backup. A differential backup allows a faster recovery than an incremental backup, but slower than a full backup. References:

➤ <https://www.nakivo.com/blog/backup-types-explained/>

NEW QUESTION 3

- (Exam Topic 3)

A security analyst is investigating what appears to be unauthorized access to a corporate web application. The security analyst reviews the web server logs and finds the following entries:

```
106.35.45.53 - - [22/May/2020:07:00:58 +0100] "GET /login?username=admin&pin=0000 HTTP/1.1" 200 11705
"http://www.example.com/login.php"
106.35.45.53 - - [22/May/2020:07:01:21 +0100] "GET /login?username=admin&pin=0001 HTTP/1.1" 200 11705
"http://www.example.com/login.php"
106.35.45.53 - - [22/May/2020:07:01:52 +0100] "GET /login?username=admin&pin=0002 HTTP/1.1" 200 11705
"http://www.example.com/login.php"
106.35.45.53 - - [22/May/2020:07:02:18 +0100] "GET /login?username=admin&pin=0003 HTTP/1.1" 200 11705
"http://www.example.com/login.php"
106.35.45.53 - - [22/May/2020:07:02:18 +0100] "GET /login?username=admin&pin=0004 HTTP/1.1" 200 11705
"http://www.example.com/login.php"
```

Which of the following password attacks is taking place?

- A. Dictionary
- B. Brute-force
- C. Rainbow table
- D. Spraying

Answer: D

Explanation:

Spraying is a password attack that involves trying a few common passwords against a large number of usernames. Spraying is different from brute-force attacks, which try many possible passwords against one username, or dictionary attacks, which try a list of words from a dictionary file against one username. Spraying is often used when the web application has a lockout policy that prevents multiple failed login attempts for the same username. Spraying can be detected by looking for patterns of failed login attempts from the same source IP address with different usernames and the same or similar passwords.

NEW QUESTION 4

- (Exam Topic 3)

Which of the following is a primary security concern for a company setting up a BYOD program?

- A. End of life
- B. Buffer overflow
- C. VM escape

D. Jailbreaking

Answer: D

Explanation:

Jailbreaking is a process of bypassing or removing the manufacturer-imposed restrictions on a mobile device's operating system, allowing users to install unauthorized applications, modify settings, etc. It is a primary security concern for setting up a BYOD program because it can expose the device and its data to malware, vulnerabilities, unauthorized access, etc.

NEW QUESTION 5

- (Exam Topic 3)

A large retail store's network was breached recently. and this news was made public. The Store did not lose any intellectual property, and no customer information was stolen. Although no fines were incurred as a result, the Store lost revenue after the breach. Which of the following is the most likely reason for this issue?

- A. Employee training
- B. Leadership changes
- C. Reputation
- D. Identity theft

Answer: C

Explanation:

Reputation is the perception or opinion that customers, partners, investors, etc., have about a company or its products and services. It can affect the revenue and profitability of a company after a network breach, even if no intellectual property or customer information was stolen, because it can damage the trust and confidence of the stakeholders and reduce their willingness to do business with the company

NEW QUESTION 6

- (Exam Topic 3)

Which of the following tools can assist with detecting an employee who has accidentally emailed a file containing a customer's PII?

- A. SCAP
- B. NetFlow
- C. Antivirus
- D. DLP

Answer: D

Explanation:

DLP stands for Data Loss Prevention, which is a technology that can monitor, detect and prevent the unauthorized transmission of sensitive data, such as PII (Personally Identifiable Information). DLP can be implemented on endpoints, networks, servers or cloud services to protect data in motion, in use or at rest. DLP can also block or alert on data transfers that violate predefined policies or rules. DLP is the best tool to assist with detecting an employee who has accidentally emailed a file containing a customer's PII, as it can scan the email content and attachments for any data that matches the criteria of PII and prevent the email from being sent or notify the administrator of the incident. Verified References:

- Data Loss Prevention Guide to Blocking Leaks - CompTIA <https://www.comptia.org/content/guides/data-loss-prevention-a-step-by-step-guide-to-blocking-leaks>
- Data Loss Prevention – SY0-601 CompTIA Security+ : 2.1 <https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/data-loss-prevention-4/>
- Data Loss Prevention – CompTIA Security+ SY0-501 – 2.1 <https://www.professormesser.com/security-plus/sy0-501/data-loss-prevention-3/>

NEW QUESTION 7

- (Exam Topic 3)

A company recently experienced a significant data loss when proprietary information was leaked to a competitor. The company took special precautions by using proper labels; however, email filter logs do not have any record of the incident. An investigation confirmed the corporate network was not breached, but documents were downloaded from an employee's COPE tablet and passed to the competitor via cloud storage. Which of the following is the best mitigation strategy to prevent this from happening in the future?

- A. User training
- B. CAsB
- C. MDM
- D. EDR

Answer: D

Explanation:

MDM stands for mobile device management, which is a solution that allows organizations to manage and secure mobile devices used by employees. MDM can help prevent data loss and leakage by enforcing policies and restrictions on the devices, such as encryption, password, app installation, remote wipe, and so on. MDM can also monitor and audit the device activity and compliance status. MDM can be the best mitigation strategy to prevent data leakage from an employee's COPE tablet via cloud storage, as it can block or limit the access to cloud services, or apply data protection measures such as containerization or encryption.

References:

- <https://www.blackberry.com/us/en/solutions/corporate-owned-personally-enabled>
- <https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/mobile-device-management/>

NEW QUESTION 8

- (Exam Topic 3)

A company needs to centralize its logs to create a baseline and have visibility on its security events Which of the following technologies will accomplish this objective?

- A. Security information and event management

- B. A web application firewall
- C. A vulnerability scanner
- D. A next-generation firewall

Answer: A

Explanation:

Security information and event management (SIEM) is a solution that collects, analyzes, and correlates logs and events from various sources such as firewalls, servers, applications, etc., within an organization's network. It can centralize logs to create a baseline and have visibility on security events by providing a unified dashboard and reporting system for log management and security monitoring.

NEW QUESTION 9

- (Exam Topic 3)

A company wants the ability to restrict web access and monitor the websites that employees visit, Which Of the following would best meet these requirements?

- A. Internet Proxy
- B. VPN
- C. WAF
- D. Firewall

Answer: A

Explanation:

An internet proxy is a server that acts as an intermediary between a client and a destination server on the internet. It can restrict web access and monitor the websites that employees visit by filtering the requests and responses based on predefined rules and policies, and logging the traffic and activities for auditing purposes

NEW QUESTION 10

- (Exam Topic 3)

Which of the following automation use cases would best enhance the security posture Of an organi-zation by rapidly updating permissions when employees leave a company Or change job roles inter-nally?

- A. Provisioning resources
- B. Disabling access
- C. APIs
- D. Escalating permission requests

Answer: B

Explanation:

Disabling access is an automation use case that can enhance the security posture of an organization by rapidly updating permissions when employees leave a company or change job roles internally. It can prevent unauthorized access and data leakage by revoking or modifying the access rights of employees based on their current status and role.

NEW QUESTION 10

- (Exam Topic 3)

A company is developing a business continuity strategy and needs to determine how many staff members would be required to sustain the business in the case of a disruption.

Which of the following best describes this step?

- A. Capacity planning
- B. Redundancy
- C. Geographic dispersion
- D. Tabletop exercise

Answer: A

Explanation:

Capacity planning is the process of determining the resources needed to meet the demand for a service or product. It involves estimating the number of staff members required to sustain the business in the case of a disruption, as well as other factors such as equipment, space, and budget¹².

Redundancy, geographic dispersion, and tabletop exercise are not directly related to determining the staff members needed for business continuity. Redundancy is the duplication of critical components or functions to increase reliability and availability². Geographic dispersion is the distribution of resources across different locations to reduce the impact of a localized disaster². Tabletop exercise is a simulation of a potential scenario that tests the effectiveness of a business continuity plan

NEW QUESTION 11

- (Exam Topic 3)

A security architect is designing a remote access solution for a business partner. The business partner needs to access one Linux server at the company. The business partner wants to avoid managing a password for authentication and additional software installation. Which of the following should the architect recommend?

- A. Soft token
- B. Smart card
- C. CSR
- D. SSH key

Answer: D

Explanation:

SSH key is a pair of cryptographic keys that can be used for authentication and encryption when connecting to a remote Linux server via SSH protocol. SSH key authentication does not require a password and is more secure than password-based authentication. SSH key authentication also does not require additional software installation on the client or the server, as SSH is a built-in feature of most Linux distributions. A business partner can generate an SSH key pair on their own computer and send the public key to the company, who can then add it to the authorized_keys file on the Linux server. This way, the business partner can access the Linux server without entering a password or installing any software

NEW QUESTION 16

- (Exam Topic 3)

Which of the following can best protect against an employee inadvertently installing malware on a company system?

- A. Host-based firewall
- B. System isolation
- C. Least privilege
- D. Application allow list

Answer: C

Explanation:

Least privilege is a security principle that states that users should only be granted the permissions they need to do their job. This helps to protect against malware infections by preventing users from installing unauthorized software.

A host-based firewall can help to protect against malware infections by blocking malicious traffic from reaching a computer. However, it cannot prevent a user from installing malware if they have the necessary permissions.

System isolation is the practice of isolating systems from each other to prevent malware from spreading. This can be done by using virtual machines or network segmentation. However, system isolation can be complex and expensive to implement.

An application allow list is a list of applications that are allowed to run on a computer. This can help to prevent malware infections by preventing users from running unauthorized applications. However, an application allow list can be difficult to maintain and can block legitimate applications.

Therefore, the best way to protect against an employee inadvertently installing malware on a company system is to use the principle of least privilege. This will help to ensure that users only have the permissions they need to do their job, which will reduce the risk of malware infections.

Here are some additional benefits of least privilege:

- It can help to improve security by reducing the attack surface.
- It can help to simplify security management by reducing the number of permissions that need to be managed.
- It can help to improve compliance by reducing the risk of data breaches.

NEW QUESTION 20

- (Exam Topic 3)

A manufacturing company has several one-off legacy information systems that cannot be migrated to a newer OS due to software compatibility issues. The OSs are still supported by the vendor but the industrial software is no longer supported. The Chief Information Security Officer has created a resiliency plan for these systems that will allow OS patches to be installed in a non-production environment, while also creating backups of the systems for recovery. Which of the following resiliency techniques will provide these capabilities?

- A. Redundancy
- B. RAID 1+5
- C. Virtual machines
- D. Full backups

Answer: D

Explanation:

Virtual machines are software-based simulations of physical computers that run on a host system and share its resources. They can provide resiliency for legacy information systems that cannot be migrated to a newer OS due to software compatibility issues by allowing OS patches to be installed in a non-production environment without affecting the production environment. They can also create backups of the systems for recovery by taking snapshots or copies of the virtual machine files.

NEW QUESTION 25

- (Exam Topic 2)

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?

- 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 is multipathing. Multipathing is a technique that allows a system to use more than one path to access a storage device. 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 fails. Multipathing can be implemented using software or hardware solutions.

NEW QUESTION 27

- (Exam Topic 2)

A security administrator is evaluating remote access solutions for employees who are geographically dispersed. Which of the following would provide the MOST secure remote access? (Select TWO).

- A. IPSec
- B. SFTP

- C. SRTP
- D. LDAPS
- E. S/MIME
- F. SSL VPN

Answer: AF

Explanation:

IPSec (Internet Protocol Security) is a technology that provides secure communication over the internet by encrypting traffic and authenticating it at both the sender and receiver. It can be used to create secure tunnels between two or more devices, allowing users to access resources securely and privately.

SSL VPN (Secure Sockets Layer Virtual Private Network) is a type of VPN that uses an SSL/TLS connection to encrypt traffic between two or more devices. It is a secure and reliable solution for providing remote access, as all traffic is encrypted and authenticated. Additionally, SSL VPNs can also be used to restrict access to certain websites and services, making them a secure and robust solution for remote access.

NEW QUESTION 32

- (Exam Topic 2)

A global pandemic is forcing a private organization to close some business units and reduce staffing at others. Which of the following would be best to help the organization's executives determine their next course of action?

- A. An incident response plan
- B. A communication plan
- C. A disaster recovery plan
- D. A business continuity plan

Answer: D

Explanation:

A business continuity plan (BCP) is a document that outlines how an organization will continue its critical functions during and after a disruptive event, such as a natural disaster, pandemic, cyberattack, or power outage. A BCP typically covers topics such as business impact analysis, risk assessment, recovery strategies, roles and responsibilities, communication plan, testing and training, and maintenance and review. A BCP can help the organization's executives determine their next course of action by providing them with a clear framework and guidance for managing the crisis and resuming normal operations.

References: <https://www.comptia.org/certifications/security#examdetails> <https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives>
<https://www.ready.gov/business-continuity-plan>

NEW QUESTION 37

- (Exam Topic 2)

A security analyst receives an alert that indicates a user's device is displaying anomalous behavior. The analyst suspects the device might be compromised. Which of the following should the analyst do first?

- A. Reboot the device
- B. Set the host-based firewall to deny an incoming connection
- C. Update the antivirus definitions on the device
- D. Isolate the device

Answer: D

Explanation:

Isolating the device is the first thing that a security analyst should do if they suspect that a user's device might be compromised. Isolating the device means disconnecting it from the network or placing it in a separate network segment to prevent further communication with potential attackers or malicious hosts. Isolating the device can help contain the incident, limit the damage or data loss, preserve the evidence, and facilitate the investigation and remediation.

References: <https://www.comptia.org/certifications/security#examdetails> <https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives>
<https://resources.infosecinstitute.com/topic/incident-response-process/>

NEW QUESTION 40

- (Exam Topic 2)

A company is concerned about individuals driving a car into the building to gain access. Which of the following security controls would work BEST to prevent this from happening?

- A. Bollard
- B. Camera
- C. Alarms
- D. Signage
- E. Access control vestibule

Answer: A

Explanation:

Bollards are posts designed to prevent vehicles from entering an area. They are usually made of steel or concrete and are placed close together to make it difficult for vehicles to pass through. In addition to preventing vehicles from entering an area, bollards can also be used to protect buildings and pedestrians from ramming attacks. They are an effective and cost-efficient way to protect buildings and pedestrians from unauthorized access.

NEW QUESTION 44

- (Exam Topic 2)

A security administrator is compiling information from all devices on the local network in order to gain better visibility into user activities. Which of the following is the best solution to meet this objective?

- A. SIEM
- B. HIDS

- C. CASB
- D. EDR

Answer: A

Explanation:

SIEM stands for Security Information and Event Management, which is a solution that can collect, correlate, and analyze security logs and events from various devices on a network. SIEM can provide better visibility into user activities by generating reports, alerts, dashboards, and metrics. SIEM can also help detect and respond to security incidents, comply with regulations, and improve security posture.

NEW QUESTION 47

- (Exam Topic 2)

A security analyst is investigating a report from a penetration test. During the penetration test, consultants were able to download sensitive data from a back-end server. The back-end server was exposing an API that should have only been available from the company's mobile application. After reviewing the back-end server logs, the security analyst finds the following entries:

```
10.35.45.53 - - [22/May/2020:06:57:31 +0100] "GET /api/cliend_id=1 HTTP/1.1" 403 1705 "http://www.example.com/api/" "PostmanRuntime/7.26.5"
10.35.45.53 - - [22/May/2020:07:00:58 +0100] "GET /api/cliend_id=2 HTTP/1.1" 403 1705 "http://www.example.com/api/" "PostmanRuntime/7.22.0"
10.32.40.13 - - [22/May/2020:08:08:52 +0100] "GET /api/cliend_id=1 HTTP/1.1" 302 21703 "http://www.example.com/api/" "CompanyMobileApp/1.1.1"
10.32.40.25 - - [22/May/2020:08:13:52 +0100] "GET /api/cliend_id=1 HTTP/1.1" 200 21703 "http://www.example.com/api/" "CompanyMobileApp/2.3.1"
10.35.45.53 - - [22/May/2020:08:20:18 +0100] "GET /api/cliend_id=2 HTTP/1.1" 200 22405 "http://www.example.com/api/" "CompanyMobileApp/2.3.0"
```

Which of the following is the most likely cause of the security control bypass?

- A. IP address allow list
- B. User-agent spoofing
- C. WAF bypass
- D. Referrer manipulation

Answer: B

Explanation:

User-agent spoofing is a technique that involves changing the user-agent string of a web browser or other client to impersonate another browser or device. The user-agent string is a piece of information that identifies the client to the web server and can contain details such as the browser name, version, operating system, and device type. User-agent spoofing can be used to bypass security controls that rely on the user-agent string to determine the legitimacy of a request. In this scenario, the consultants were able to spoof the user-agent string of the company's mobile application and access the API that should have been restricted to it.

NEW QUESTION 52

- (Exam Topic 2)

Security engineers are working on digital certificate management with the top priority of making administration easier. Which of the following certificates is the best option?

- A. User
- B. Wildcard
- C. Self-signed
- D. Root

Answer: B

Explanation:

A wildcard certificate is a type of digital certificate that can be used to secure multiple subdomains under a single domain name. For example, a wildcard certificate for *.example.com can be used to secure www.example.com, mail.example.com, blog.example.com, etc. A wildcard certificate can make administration easier by reducing the number of certificates that need to be issued, managed, and renewed. It can also save costs and simplify configuration.

NEW QUESTION 56

- (Exam Topic 2)

A financial institution recently joined a bug bounty program to identify security issues in the institution's new public platform. Which of the following best describes who the institution is working with to identify security issues?

- A. Script kiddie
- B. Insider threats
- C. Malicious actor
- D. Authorized hacker

Answer: D

Explanation:

An authorized hacker, also known as an ethical hacker or a white hat hacker, is someone who uses their skills and knowledge to find and report security issues in a system or application with the permission of the owner. An authorized hacker follows the rules and guidelines of the bug bounty program and does not cause any harm or damage to the system or its users.

NEW QUESTION 60

- (Exam Topic 2)

Several users have been violating corporate security policy by accessing inappropriate Sites on corporate-issued mobile devices while off campus. The senior leadership team wants all mobile devices to be hardened with controls that:

- Limit the sites that can be accessed
- Only allow access to internal resources while physically on campus.

➤ Restrict employees from downloading images from company email
Which of the following controls would best address this situation? (Select two).

- A. MFA
- B. GPS tagging
- C. Biometric authentication
- D. Content management
- E. Geofencing
- F. Screen lock and PIN requirements

Answer: DE

Explanation:

Content management is a security control that can limit the sites that can be accessed by corporate-issued mobile devices. It can also restrict employees from downloading images from company email by filtering or blocking certain types of content¹. Geofencing is a security control that can only allow access to internal resources while physically on campus. It can use GPS or other location services to define a virtual boundary around a physical area and enforce policies based on the device's location².

References:

- 1: <https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening>
2: <https://www.makeuseof.com/how-to-secure-your-content-management-system/>

NEW QUESTION 64

- (Exam Topic 2)

An email security vendor recently added a retroactive alert after discovering a phishing email had already been delivered to an inbox. Which of the following would be the best way for the security administrator to address this type of alert in the future?

- A. Utilize a SOAR playbook to remove the phishing message.
- B. Manually remove the phishing emails when alerts arrive.
- C. Delay all emails until the retroactive alerts are received.
- D. Ingest the alerts into a SIEM to correlate with delivered messages.

Answer: A

Explanation:

One possible way to address this type of alert in the future is to use a SOAR (Security Orchestration, Automation, and Response) playbook to automatically remove the phishing message from the inbox³. A SOAR playbook is a set of predefined actions that can be triggered by certain events or conditions. This can help reduce the response time and human error in dealing with phishing alerts.

NEW QUESTION 65

- (Exam Topic 2)

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)

- 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".

NEW QUESTION 67

- (Exam Topic 2)

A company that provides an online streaming service made its customers' personal data including names and email addresses publicly available in a cloud storage service. As a result, the company experienced an increase in the number of requests to delete user accounts. Which of the following best describes the consequence of this data disclosure?

- A. Regulatory fines
- B. Reputation damage
- C. Increased insurance costs
- D. Financial loss

Answer: B

Explanation:

Reputation damage Short explanation

Reputation damage is the loss of trust or credibility that a company suffers when its customers' personal data is exposed or breached. This can lead to customer

dissatisfaction, loss of loyalty, and requests to delete user accounts. References: <https://www.comptia.org/content/guides/what-is-cybersecurity>

NEW QUESTION 71

- (Exam Topic 2)

A company is switching to a remote work model for all employees. All company and employee resources will be in the cloud. Employees must use their personal computers to access the cloud computing environment. The company will manage the operating system. Which of the following deployment models is the company implementing?

- A. CYOD
- B. MDM
- C. COPE
- D. VDI

Answer: D

Explanation:

According to Professor Messer's video¹, VDI stands for Virtual Desktop Infrastructure and it is a deploy model where employees use their personal computers to access a virtual machine that runs the company's operating system and applications.

In the scenario described, the company is implementing a virtual desktop infrastructure (VDI) deployment model [1]. This allows employees to access the cloud computing environment using their personal computers, while the company manages the operating system. The VDI model is suitable for remote work scenarios because it provides secure and centralized desktop management, while allowing employees to access desktops from any device.

NEW QUESTION 73

- (Exam Topic 2)

Which of the following would satisfy three-factor authentication requirements?

- A. Password, PIN, and physical token
- B. PIN, fingerprint scan, and iris scan
- C. Password, fingerprint scan, and physical token
- D. PIN, physical token, and ID card

Answer: C

Explanation:

Three-factor authentication combines three types of authentication methods: something you know (password), something you have (physical token), and something you are (fingerprint scan). Option C satisfies these requirements, as it uses a password (something you know), a physical token (something you have), and a fingerprint scan (something you are) for authentication.

Reference: CompTIA Security+ Study Guide (SY0-601) 7th Edition by Emmett Dulaney, Chuck Easttom Note: There could be other options as well that could satisfy the three-factor authentication requirements as per the organization's security policies.

NEW QUESTION 75

- (Exam Topic 2)

During a recent cybersecurity audit, the auditors pointed out various types of vulnerabilities in the production area. The production area hardware runs applications that are critical to production. Which of the following describes what the company should do first to lower the risk to the Production the hardware.

- A. Back up the hardware.
- B. Apply patches.
- C. Install an antivirus solution.
- D. Add a banner page to the hardware.

Answer: B

Explanation:

Applying patches is the first step to lower the risk to the production hardware, as patches are updates that fix vulnerabilities or bugs in the software or firmware.

Patches can prevent attackers from exploiting known vulnerabilities and compromising the production hardware. Applying patches should be done regularly and in a timely manner, following a patch management policy and process. References: 1

CompTIA Security+ Certification Exam Objectives, page 9, Domain 2.0: Architecture and Design, Objective 2.3: Summarize secure application development, deployment, and automation concepts 2

CompTIA Security+ Certification Exam Objectives, page 10, Domain 2.0: Architecture and Design, Objective 2.4: Explain the importance of embedded and specialized systems security 3 <https://www.comptia.org/blog/patch-management-best-practices>

NEW QUESTION 78

- (Exam Topic 2)

A cybersecurity analyst needs to adopt controls to properly track and log user actions to an individual. Which of the following should the analyst implement?

- A. Non-repudiation
- B. Baseline configurations
- C. MFA
- D. DLP

Answer: A

Explanation:

Non-repudiation is the process of ensuring that a party involved in a transaction or communication cannot deny their involvement. By implementing non-repudiation controls, a cybersecurity analyst can properly track and log user actions, attributing them to a specific individual. This can be achieved through methods such as digital signatures, timestamps, and secure logging mechanisms.

References:

- * 1. CompTIA Security+ Certification Exam Objectives (SY0-601): <https://www.comptia.jp/pdf/CompTIA%20Security%2B%20SY0-601%20Exam%20Objectives.pdf>
- * 2. Stewart, J. M., Chapple, M., & Gibson, D. (2021). CompTIA Security+ Study Guide: Exam SY0-601. John Wiley & Sons.

NEW QUESTION 82

- (Exam Topic 2)

Unauthorized devices have been detected on the internal network. The devices' locations were traced to Ether ports located in conference rooms. Which of the following would be the best technical controls to implement to prevent these devices from accessing the internal network?

- A. NAC
- B. DLP
- C. IDS
- D. MFA

Answer: A

Explanation:

NAC stands for network access control, which is a security solution that enforces policies and controls on devices that attempt to access a network. NAC can help prevent unauthorized devices from accessing the internal network by verifying their identity, compliance, and security posture before granting them access. NAC can also monitor and restrict the activities of authorized devices based on predefined rules and roles.

References: <https://www.comptia.org/certifications/security#examdetails> <https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives>
<https://www.cisco.com/c/en/us/products/security/what-is-network-access-control-nac.html>

NEW QUESTION 84

- (Exam Topic 2)

A backup operator wants to perform a backup to enhance the RTO and RPO in a highly time- and storage-efficient way that has no impact on production systems. Which of the following backup types should the operator use?

- A. Tape
- B. Full
- C. Image
- D. Snapshot

Answer: D

Explanation:

A snapshot backup is a type of backup that captures the state of a system at a point in time. It is highly time- and storage-efficient because it only records the changes made to the system since the last backup. It also has no impact on production systems because it does not require them to be offline or paused during the backup process. References: <https://www.comptia.org/blog/what-is-a-snapshot-backup>

NEW QUESTION 86

- (Exam Topic 2)

A company has numerous employees who store PHI data locally on devices. The Chief Information Officer wants to implement a solution to reduce external exposure of PHI but not affect the business.

The first step the IT team should perform is to deploy a DLP solution:

- A. for only data in transit.
- B. for only data at reset.
- C. in blocking mode.
- D. in monitoring mode.

Answer: D

Explanation:

A DLP solution in monitoring mode is a good first step to deploy for data loss prevention. It allows the IT team to observe and analyze the data flows and activities without blocking or interfering with them. It helps to identify the sources and destinations of sensitive data, the types and volumes of data involved, and the potential risks and violations. It also helps to fine-tune the DLP policies and rules before switching to blocking mode, which can disrupt business operations if not configured properly.

NEW QUESTION 88

- (Exam Topic 2)

Which of the following should a Chief Information Security Officer consider using to take advantage of industry standard guidelines?

- A. SSAE SOC 2
- B. GDPR
- C. PCI DSS
- D. NIST CSF

Answer: D

Explanation:

NIST CSF (National Institute of Standards and Technology Cybersecurity Framework) is a set of guidelines and best practices for managing cybersecurity risks. It is based on existing standards, guidelines, and practices that are widely recognized and applicable across different sectors and organizations. It provides a common language and framework for understanding, communicating, and managing cybersecurity risks. References: 1 CompTIA Security+ Certification Exam Objectives, page 7, Domain 1.0: Attacks, Threats, and Vulnerabilities, Objective 1.4: Explain the techniques used in security assessments 2 CompTIA Security+ Certification Exam Objectives, page 8, Domain 2.0: Architecture and Design, Objective 2.1: Explain the importance of secure staging deployment concepts 3 <https://www.nist.gov/cyberframework>

NEW QUESTION 92

- (Exam Topic 2)

A candidate attempts to go to but accidentally visits <http://comptia.org>. The malicious website looks exactly like the legitimate website. Which of the following best describes this type of attack?

- A. Reconnaissance
- B. Impersonation
- C. Typosquatting
- D. Watering-hole

Answer: C

Explanation:

Typosquatting is a type of cyberattack that involves registering domains with deliberately misspelled names of well-known websites. The attackers do this to lure unsuspecting visitors to alternative websites, typically for malicious purposes. Visitors may end up at these alternative websites by inadvertently mistyping the name of popular websites into their web browser or by being lured by a phishing scam. The attackers may emulate the look and feel of the legitimate websites and trick users into entering sensitive information or downloading malware.

References: <https://www.comptia.org/certifications/security#examdetails> <https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives>
<https://www.kaspersky.com/resource-center/definitions/what-is-typosquatting>

NEW QUESTION 94

- (Exam Topic 2)

An employee's company email is configured with conditional access and requires that MFA is enabled and used. An example of MFA is a phone call and:

- A. a push notification
- B. a password.
- C. an SMS message.
- D. an authentication application.

Answer: D

Explanation:

An authentication application can generate one-time passwords or QR codes that are time-based and unique to each user and device. It does not rely on network connectivity or SMS delivery, which can be intercepted or delayed. It also does not require the user to respond to a push notification, which can be accidentally approved or ignored.

NEW QUESTION 97

- (Exam Topic 2)

A security investigation revealed that malicious software was installed on a server using a server administrator credentials. During the investigation the server administrator explained that Telnet was regularly used to log in. Which of the following most likely occurred?

- A. A spraying attack was used to determine which credentials to use
- B. A packet capture tool was used to steal the password
- C. A remote-access Trojan was used to install the malware
- D. A directory attack was used to log in as the server administrator

Answer: B

Explanation:

Telnet is an insecure protocol that transmits data in cleartext over the network. This means that anyone who can intercept the network traffic can read the data, including the username and password of the server administrator. A packet capture tool is a software or hardware device that can capture and analyze network packets. An attacker can use a packet capture tool to steal the password and use it to install malicious software on the server. References:

<https://www.comptia.org/content/guides/what-is-network-security>

NEW QUESTION 100

- (Exam Topic 2)

An upcoming project focuses on secure communications and trust between external parties. Which of the following security components will need to be considered to ensure a chosen trust provider is used and the selected option is highly scalable?

- A. Self-signed certificate
- B. Certificate attributes
- C. Public key Infrastructure
- D. Domain validation

Answer: C

Explanation:

PKI is a security technology that enables secure communication between two parties by using cryptographic functions. It consists of a set of components that are used to create, manage, distribute, store, and revoke digital certificates. PKI provides a secure way to exchange data between two parties, as well as a trust provider to ensure that the data is not tampered with. It also helps to create a highly scalable solution, as the same certificate can be used for multiple parties. According to the CompTIA Security+ Study Guide, "PKI is a technology used to secure communications between two external parties. PKI is based on the concept of digital certificates, which are used to authenticate the sender and recipient of a message. PKI provides a trust provider to ensure that the digital certificate is valid and has not been tampered with. It also provides a scalable solution, as multiple parties can use the same certificate."

NEW QUESTION 102

- (Exam Topic 2)

Which of the following procedures would be performed after the root cause of a security incident has been identified to help avoid future incidents from occurring?

- A. Walk-throughs
- B. Lessons learned
- C. Attack framework alignment
- D. Containment

Answer: B

Explanation:

After the root cause of a security incident has been identified, it is important to take the time to analyze what went wrong and how it could have been prevented. This process is known as “lessons learned” and allows organizations to identify potential improvements to their security processes and protocols. Lessons learned typically involve a review of the incident and the steps taken to address it, a review of the security systems and procedures in place, and an analysis of any potential changes that can be made to prevent similar incidents from occurring in the future.

NEW QUESTION 106

- (Exam Topic 2)

A systems engineer thinks a business system has been compromised and is being used to exfiltrate data to a competitor. The engineer contacts the CSIRT. The CSIRT tells the engineer to immediately disconnect the network cable and to not do anything else. Which of the following is the most likely reason for this request?

- A. The CSIRT thinks an insider threat is attacking the network
- B. Outages of business-critical systems cost too much money
- C. The CSIRT does not consider the systems engineer to be trustworthy
- D. Memory contents including files and malware are lost when the power is turned off

Answer: D

Explanation:

Memory contents including files and malware are lost when the power is turned off. This is because memory is a volatile storage device that requires constant power to retain data. If a system has been compromised and is being used to exfiltrate data to a competitor, the CSIRT may want to preserve the memory contents for forensic analysis and evidence collection. Therefore, the CSIRT may tell the engineer to immediately disconnect the network cable and not do anything else to prevent further data loss or tampering.

References: <https://www.comptia.org/certifications/security#examdetails> <https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives>
<https://resources.infosecinstitute.com/topic/memory-acquisition-and-analysis/>

NEW QUESTION 107

- (Exam Topic 2)

The findings in a consultant's report indicate the most critical risk to the security posture from an incident response perspective is a lack of workstation and server investigation capabilities. Which of the following should be implemented to remediate this risk?

- A. HIDS
- B. FDE
- C. NGFW
- D. EDR

Answer: D

Explanation:

EDR solutions are designed to detect and respond to malicious activity on workstations and servers, and they provide a detailed analysis of the incident, allowing organizations to quickly remediate the threat. According to the CompTIA Security+ SY0-601 Official Text Book, EDR solutions can be used to detect malicious activity on endpoints, investigate the incident, and contain the threat. EDR solutions can also provide real-time monitoring and alerting for potential security events, as well as detailed forensic analysis for security incidents. Additionally, the text book recommends that organizations also implement a host-based intrusion detection system (HIDS) to alert them to malicious activity on their workstations and servers.

NEW QUESTION 109

- (Exam Topic 2)

A security engineer updated an application on company workstations. The application was running before the update, but it is no longer launching successfully. Which of the following most likely needs to be updated?

- A. Blocklist
- B. Deny list
- C. Quarantine list
- D. Approved list

Answer: D

Explanation:

Approved list is a list of applications or programs that are allowed to run on a system or network. An approved list can prevent unauthorized or malicious software from running and compromising the security of the system or network. An approved list can also help with patch management and compatibility issues. If the security engineer updated an application on the company workstations, the application may need to be added or updated on the approved list to be able to launch successfully. References: 1

CompTIA Security+ Certification Exam Objectives, page 10, Domain 2.0: Architecture and Design, Objective 2.4: Explain the importance of embedded and specialized systems security 2

CompTIA Security+ Certification Exam Objectives, page 12,

Domain 3.0: Implementation, Objective 3.1: Implement secure network architecture concepts 3

<https://www.comptia.org/blog/what-is-application-whitelisting>

NEW QUESTION 112

- (Exam Topic 2)

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

- A. Containers
- B. Edge computing
- C. Thin client
- D. Infrastructure as a service

Answer: C

Explanation:

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.

NEW QUESTION 113

- (Exam Topic 2)

An engineer wants to inspect traffic to a cluster of web servers in a cloud environment Which of the following solutions should the engineer implement? (Select two).

- A. CASB
- B. WAF
- C. Load balancer
- D. VPN
- E. TLS
- F. DAST

Answer: BC

Explanation:

A web application firewall (WAF) is a solution that inspects traffic to a cluster of web servers in a cloud environment and protects them from common web-based attacks, such as SQL injection, cross-site scripting, and denial-of-service¹. A WAF can be deployed as a cloud service or as a virtual appliance in front of the web servers. A load balancer is a solution that distributes traffic among multiple web servers in a cloud environment and improves their performance, availability, and scalability². A load balancer can also perform health checks on the web servers and route traffic only to the healthy ones. The other options are not relevant to this scenario. A CASB is a cloud access security broker, which is a solution that monitors and controls the use of cloud services by an organization's users³. A VPN is a virtual private network, which is a solution that creates a secure and encrypted connection between two networks or devices over the internet. TLS is Transport Layer Security, which is a protocol that provides encryption and authentication for data transmitted over a network. DAST is dynamic application security testing, which is a method of testing web applications for vulnerabilities by simulating attacks on them.

References: 1: <https://www.imperva.com/learn/application-security/what-is-a-web-application-firewall-waf/> 2:

<https://www.imperva.com/learn/application-security/load-balancing/> 3: <https://www.imperva.com/learn/application-security/cloud-access-security-broker-casb/> :

<https://www.imperva.com/learn/application-security/vpn-virtual-private-network/> : <https://www.imperva.com/learn/application-security/transport-layer-security-tls/> :

<https://www.imperva.com/learn/application-security/dynamic-application-security-testing-dast/> : <https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/azure-best-practices/plan-for-traffic-ins>

: <https://docs.microsoft.com/en-us/azure/private-link/inspect-traffic-with-azure-firewall> : <https://docs.microsoft.com/en-us/azure/architecture/example-scenario/gateway/application-gateway-before-azur>

NEW QUESTION 117

- (Exam Topic 2)

Which of the following would a security analyst use to determine if other companies in the same sector have seen similar malicious activity against their systems?

- A. Vulnerability scanner
- B. Open-source intelligence
- C. Packet capture
- D. Threat feeds

Answer: D

Explanation:

Threat feeds, also known as threat intelligence feeds, are a source of information about current and emerging threats, vulnerabilities, and malicious activities targeting organizations. Security analysts use threat feeds to gather information about attacks and threats targeting their industry or sector. These feeds are typically provided by security companies, research organizations, or industry-specific groups. By using threat feeds, analysts can identify trends, patterns, and potential threats that may target their own organization, allowing them to take proactive steps to protect their systems.

References:

* 1. CompTIA Security+ Certification Exam Objectives (SY0-601): <https://www.comptia.jp/pdf/Security%2B%20SY0-601%20Exam%20Objectives.pdf>

* 2. SANS Institute: Threat Intelligence: What It Is, and How to Use It Effectively: <https://www.sans.org-room/whitepapers/analyst/threat-intelligence-is-effectively-36367>

NEW QUESTION 121

- (Exam Topic 2)

The alert indicates an attacker entered thousands of characters into the text box of a web form. The web form was intended for legitimate customers to enter their phone numbers. Which of the attacks has most likely occurred?

- A. Privilege escalation
- B. Buffer overflow
- C. Resource exhaustion
- D. Cross-site scripting

Answer: B

Explanation:

A buffer overflow attack occurs when an attacker inputs more data than the buffer can store, causing the excess data to overwrite adjacent memory locations and corrupt or execute code¹. In this case, the attacker entered thousands of characters into a text box that was intended for phone numbers, which are much shorter. This could result in a buffer overflow attack that compromises the web application or server. The other options are not related to this scenario. Privilege escalation is when an attacker gains unauthorized access to higher-level privileges or resources². Resource exhaustion is when an attacker consumes all the available

resources of a system, such as CPU, memory, disk space, etc., to cause a denial of service³. Cross-site scripting is when an attacker injects malicious code into a web page that is executed by the browser of a victim who visits the page.

References: 1: <https://www.fortinet.com/resources/cyberglossary/buffer-overflow> 2:

<https://www.imperva.com/learn/application-security/privilege-escalation/> 3: <https://www.imperva.com/learn/application-security/resource-exhaustion/> :

<https://owasp.org/www-community/attacks/xss/>

NEW QUESTION 123

- (Exam Topic 2)

A security administrator recently used an internal CA to issue a certificate to a public application. A user tries to reach the application but receives a message stating, "Your connection is not private." Which of the following is the best way to fix this issue?

- A. Ignore the warning and continue to use the application normally.
- B. Install the certificate on each endpoint that needs to use the application.
- C. Send the new certificate to the users to install on their browsers.
- D. Send a CSR to a known CA and install the signed certificate on the application's server.

Answer: D

Explanation:

A certificate issued by an internal CA is not trusted by default by external users or applications. Therefore, when a user tries to reach the application that uses an internal CA certificate, they will receive a warning message that their connection is not private¹. The best way to fix this issue is to use a certificate signed by a well-known public CA that is trusted by most browsers and operating systems¹. To do this, the security administrator needs to send a certificate signing request (CSR) to a public CA and install the signed certificate on the application's server². The other options are not recommended or feasible. Ignoring the warning and continuing to use the application normally is insecure and exposes the user to potential man-in-the-middle attacks³. Installing the certificate on each endpoint that needs to use the application is impractical and cumbersome, especially if there are many users or devices involved³. Sending the new certificate to the users to install on their browsers is also inconvenient and may not work for some browsers or devices³.

References: 1:

<https://learn.microsoft.com/en-us/azure/active-directory/develop/howto-create-self-signed-certificate> 2:

<https://learn.microsoft.com/en-us/azure/application-gateway/mutual-authentication-certificate-management> 3: <https://serverfault.com/questions/1106443/should-i-use-a-public-or-a-internal-ca-for-client-certificate-mtls>

NEW QUESTION 124

- (Exam Topic 2)

A web server log contains two million lines. A security analyst wants to obtain the next 500 lines starting from line 4,600. Which of the following commands will help the security analyst to achieve this objective?

- A. `cat webserver.log | head -4600 | tail +500 |`
- B. `cat webserver.log | tail -1995400 | tail -500 |`
- C. `cat webserver.log | tail -4600 | head -500 |`
- D. `cat webserver.log | head -5100 | tail -500 |`

Answer: D

Explanation:

the cat command displays the contents of a file, the head command displays the first lines of a file, and the tail command displays the last lines of a file. To display a specific number of lines from a file, you can use a minus sign followed by a number as an option for head or tail. For example, head -10 will display the first 10 lines of a file.

To obtain the next 500 lines starting from line 4,600, you need to use both head and tail commands. <https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/file-manipulation-tools/>

NEW QUESTION 128

- (Exam Topic 2)

Which of the following would provide guidelines on how to label new network devices as part of the initial configuration?

- A. IP schema
- B. Application baseline configuration
- C. Standard naming convention policy
- D. Wireless LAN and network perimeter diagram

Answer: C

Explanation:

A standard naming convention policy would provide guidelines on how to label new network devices as part of the initial configuration. A standard naming convention policy is a document that defines the rules and formats for naming network devices, such as routers, switches, firewalls, servers, or printers. A standard naming convention policy can help an organization achieve consistency, clarity, and efficiency in network management and administration.

References: <https://www.comptia.org/certifications/security#examdetails> <https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives>

https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Network_Virtualization/PathIsolationDesignGuide/P

NEW QUESTION 133

- (Exam Topic 2)

A junior human resources administrator was gathering data about employees to submit to a new company awards program The employee data included job title business phone number location first initial with last name and race Which of the following best describes this type of information?

- A. Sensitive
- B. Non-PII
- C. Private
- D. Confidential

Answer: B

Explanation:

Non-PII stands for non-personally identifiable information, which is any data that does not directly identify a specific individual. Non-PII can include information such as job title, business phone number, location, first initial with last name, and race. Non-PII can be used for various purposes, such as statistical analysis, marketing, or research. However, non-PII may still pose some privacy risks if it is combined or linked with other data that can reveal an individual's identity. References: <https://www.comptia.org/certifications/security#examdetails>
<https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives> <https://www.investopedia.com/terms/n/non-personally-identifiable-information-npii.asp>

NEW QUESTION 138

- (Exam Topic 2)

A company recently implemented a patch management policy; however, vulnerability scanners have still been flagging several hosts, even after the completion of the patch process. Which of the following is the most likely cause of the issue?

- A. The vendor firmware lacks support.
- B. Zero-day vulnerabilities are being discovered.
- C. Third-party applications are not being patched.
- D. Code development is being outsourced.

Answer: C

Explanation:

Third-party applications are applications that are developed and provided by external vendors or sources, rather than by the organization itself. Third-party applications may introduce security risks if they are not properly vetted, configured, or updated. One of the most likely causes of vulnerability scanners flagging several hosts after the completion of the patch process is that third-party applications are not being patched. Patching is the process of applying updates or fixes to software to address bugs, vulnerabilities, or performance issues. Patching third-party applications is essential for maintaining their security and functionality, as well as preventing attackers from exploiting known flaws.

References: <https://www.comptia.org/certifications/security#examdetails> <https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives>
<https://www.csoonline.com/article/2124681/why-third-party-security-is-your-security.html>

NEW QUESTION 140

- (Exam Topic 2)

A company a "right to forgotten" request To legally comply, the company must remove data related to the requester from its systems. Which Of the following Company most likely complying with?

- A. NIST CSF
- B. GDPR
- C. PCI OSS
- D. ISO 27001

Answer: B

Explanation:

GDPR stands for General Data Protection Regulation, which is a law that regulates data protection and privacy in the European Union (EU) and the European Economic Area (EEA). GDPR also applies to the transfer of personal data outside the EU and EEA areas. GDPR grants individuals the right to request the deletion or removal of their personal data from an organization's systems under certain circumstances. This right is also known as the "right to be forgotten" or the "right to erasure". An organization that receives such a request must comply with it within a specified time frame, unless there are legitimate grounds for retaining the data.

References: <https://www.comptia.org/certifications/security#examdetails> <https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives>
<https://gdpr-info.eu/issues/right-to-be-forgotten/>

NEW QUESTION 141

- (Exam Topic 2)

A security team suspects that the cause of recent power consumption overloads is the unauthorized use of empty power outlets in the network rack. Which of the following options will mitigate this issue without compromising the number of outlets available?

- A. Adding a new UPS dedicated to the rack
- B. Installing a managed PDU
- C. Using only a dual power supplies unit
- D. Increasing power generator capacity

Answer: B

Explanation:

Installing a managed PDU is the most appropriate option to mitigate the issue without compromising the number of outlets available. A managed Power Distribution Unit (PDU) helps monitor, manage, and control power consumption at the rack level. By installing a managed PDU, the security team will have greater visibility into power usage in the network rack, and they can identify and eliminate unauthorized devices that consume excessive power from empty outlets. <https://www.comptia.org/training/books/security-sy0-601-study-guide>

NEW QUESTION 142

- (Exam Topic 2)

A company is moving its retail website to a public cloud provider. The company wants to tokenize audit card data but not allow the cloud provider to see the stored credit card information. Which of the following would BEST meet these objectives?

- A. WAF
- B. CASB
- C. VPN
- D. TLS

Answer: B

Explanation:

CASB stands for cloud access security broker, which is a software tool or service that acts as an intermediary between users and cloud service providers. CASB can help protect data stored in cloud services by enforcing security policies and controls such as encryption, tokenization, authentication, authorization, logging, auditing, and threat detection. Tokenization is a process that replaces sensitive data with non-sensitive substitutes called tokens that have no intrinsic value. Tokenization can help prevent data leakage by ensuring that only authorized users can access the original data using a tokenization system.

References: <https://www.comptia.org/certifications/security#examdetails> <https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives>
<https://www.cisco.com/c/en/us/products/security/what>

NEW QUESTION 144

- (Exam Topic 2)

A security administrator Installed a new web server. The administrator did this to Increase the capacity (or an application due to resource exhaustion on another server. Which o(the following algorithms should the administrator use to split the number of the connections on each server In half?

- A. Weighted response
- B. Round-robin
- C. Least connection
- D. Weighted least connection

Answer: B

Explanation:

The administrator should use a round-robin algorithm to split the number of connections on each server in half. Round-robin is a load-balancing algorithm that distributes incoming requests to the available servers one by one in a cyclical order. This helps to evenly distribute the load across all of the servers, ensuring that no single server is overloaded.

NEW QUESTION 146

- (Exam Topic 2)

A Security engineer needs to implement an MDM solution that complies with the corporate mobile device policy. The policy states that in order for mobile users to access corporate resources on their devices, the following requirements must be met:

- Mobile device OSs must be patched up to the latest release.
- A screen lock must be enabled (passcode or biometric).
- Corporate data must be removed if the device is reported lost or stolen.

Which of the following controls should the security engineer configure? (Select two).

- A. Disable firmware over-the-air
- B. Storage segmentation
- C. Posture checking
- D. Remote wipe
- E. Full device encryption
- F. Geofencing

Answer: CD

Explanation:

Posture checking and remote wipe are two controls that the security engineer should configure to comply with the corporate mobile device policy. Posture checking is a process that verifies if a mobile device meets certain security requirements before allowing it to access corporate resources. For example, posture checking can check if the device OS is patched up to the latest release and if a screen lock is enabled. Remote wipe is a feature that allows the administrator to erase all data from a mobile device remotely, in case it is lost or stolen. This can prevent unauthorized access to corporate data on the device.

NEW QUESTION 150

- (Exam Topic 2)

A Chief Information Security Officer (CISO) is evaluating the dangers involved in deploying a new ERP system for the company. The CISO categorizes the system, selects the controls that apply to the system, implements the controls, and then assesses the success of the controls before authorizing the system. Which of the following is the CISO using to evaluate the environment for this new ERP system?

- A. The Diamond Model of Intrusion Analysis
- B. CIS Critical Security Controls
- C. NIST Risk Management Framework
- D. ISO 27002

Answer: C

Explanation:

The NIST Risk Management Framework (RMF) is a process for evaluating the security of a system and implementing controls to reduce potential risks associated with it. The RMF process involves categorizing the system, selecting the controls that apply to the system, implementing the controls, and then assessing the success of the controls before authorizing the system. For more information on the NIST Risk Management Framework and other security processes, refer to the CompTIA Security+ SY0-601 Official Text Book and Resources.

NEW QUESTION 153

- (Exam Topic 2)

The new Chief Information Security Officer at a company has asked the security learn to implement stronger user account policies. The new policies require:

- Users to choose a password unique to their last ten passwords
- Users to not log in from certain high-risk countries

Which of the following should the security team implement? (Select two).

- A. Password complexity
- B. Password history

- C. Geolocation
- D. Geospatial
- E. Geotagging
- F. Password reuse

Answer: BC

Explanation:

Password history is a policy that prevents users from reusing their previous passwords. This can reduce the risk of password cracking or compromise. Geolocation is a policy that restricts users from logging in from certain locations based on their IP address. This can prevent unauthorized access from high-risk countries or regions. References: <https://www.comptia.org/content/guides/what-is-identity-and-access-management>

NEW QUESTION 154

- (Exam Topic 2)

A systems analyst is responsible for generating a new digital forensics chain-of-custody form. Which of the following should the analyst include in this documentation? (Select two).

- A. The order of volatility
- B. A forensics NDA
- C. The provenance of the artifacts
- D. The vendor's name
- E. The date and time
- F. A warning banner

Answer: CE

Explanation:

A digital forensics chain-of-custody form is a document that records the chronological and logical sequence of custody, control, transfer, analysis, and disposition of digital evidence. A digital forensics chain-of-custody form should include the following information:

➤ The provenance of the artifacts: The provenance of the artifacts refers to the origin and history of the digital evidence, such as where, when, how, and by whom it was collected, handled, analyzed, or otherwise controlled.

➤ The date and time: The date and time refer to the specific moments when the digital evidence was collected, handled, analyzed, transferred, or disposed of by each person involved in the chain of custody.

Other information that may be included in a digital forensics chain-of-custody form are:

➤ The identification of the artifacts: The identification of the artifacts refers to the unique identifiers or labels assigned to the digital evidence, such as serial numbers, barcodes, hashes, or descriptions.

➤ The signatures of the custodians: The signatures of the custodians refer to the names and signatures of each person who had custody or control of the digital evidence at any point in the chain of custody.

➤ The location of the artifacts: The location of the artifacts refers to the physical or logical places where the digital evidence was stored or processed, such as a lab, a server, a cloud service, or a device.

References: <https://www.comptia.org/certifications/security#examdetails> <https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives>
<https://resources.infosecinstitute.com/topic/chain-of-custody-in-digital-forensics/>

NEW QUESTION 155

- (Exam Topic 2)

A security analyst is investigating network issues between a workstation and a company server. The workstation and server occasionally experience service disruptions, and employees are forced to reconnect to the server. In addition, some reports indicate sensitive information is being leaked from the server to the public.

The workstation IP address is 192.168.1.103, and the server IP address is 192.168.1.101. The analyst runs `arp -a` on a separate workstation and obtains the following results:

| Internet address | Physical address | Type |
|------------------|-------------------|---------|
| 192.168.1.101 | 27-4b-17-00-38-08 | dynamic |
| 192.168.1.102 | 8e-45-49-ac-67-b6 | dynamic |
| 192.168.1.103 | 27-4b-17-00-38-08 | dynamic |
| 192.168.1.105 | 1f-35-91-55-0f-39 | dynamic |
| 192.168.1.157 | 27-4b-17-00-38-08 | dynamic |
| 192.168.1.190 | 12-d6-cf-91-f6-3f | dynamic |

Which of the following is most likely occurring?

- A. Evil twin attack
- B. Domain hijacking attack
- C. On-path attack
- D. MAC flooding attack

Answer: C

Explanation:

An on-path attack is a type of attack where an attacker places themselves between two devices (such as a workstation and a server) and intercepts or modifies the communications between them. An on-path attacker can collect sensitive information, impersonate either device, or disrupt the service. In this scenario, the attacker is likely using an on-path attack to capture and alter the network traffic between the workstation and the server, causing service disruptions and data leakage.

NEW QUESTION 156

- (Exam Topic 2)

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

Answer: C

Explanation:

According to NIST Special Publication 1800-4B1, some of the security controls that can be used to protect mobile devices include:

- Root and jailbreak detection: ensures that the security architecture for a mobile device has not been compromised.
- Encryption: protects the data stored on the device and in transit from unauthorized access.
- Authentication: verifies the identity of the user and the device before granting access to enterprise resources.
- Remote wipe: allows the organization to erase the data on the device in case of loss or theft.
- Screen lock timer: sets a time limit for the device to lock itself after a period of inactivity.

NEW QUESTION 157

- (Exam Topic 2)

A company is moving to new location. The systems administrator has provided the following server room requirements to the facilities staff:

- Consistent power levels in case of brownouts or voltage spikes
- A minimum of 30 minutes runtime following a power outage
- Ability to trigger graceful shutdowns of critical systems

Which of the following would BEST meet the requirements?

- A. Maintaining a standby, gas-powered generator
- B. Using large surge suppressors on computer equipment
- C. Configuring managed PDUs to monitor power levels
- D. Deploying an appropriately sized, network-connected UPS device

Answer: D

Explanation:

A UPS (uninterruptible power supply) device is a battery backup system that can provide consistent power levels in case of brownouts or voltage spikes. It can also provide a minimum of 30 minutes runtime following a power outage, depending on the size and load of the device. A network-connected UPS device can also communicate with critical systems and trigger graceful shutdowns if the battery level is low or the power is not restored.

NEW QUESTION 161

- (Exam Topic 2)

A security analyst is reviewing packet capture data from a compromised host. In the packet capture, analyst locates packets that contain large amounts of text. Which of the following is most likely installed on the compromised host?

- A. Keylogger
- B. Spyware
- C. Trojan
- D. Ransomware

Answer: A

Explanation:

A keylogger is a type of malware that records the keystrokes of the user and sends them to a remote attacker. The attacker can use the keystrokes to steal the user's credentials, personal information, or other sensitive data. A keylogger can generate packets that contain large amounts of text, as the packet capture data shows.

NEW QUESTION 164

- (Exam Topic 2)

Given the following snippet of Python code:

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

```
#!/usr/bin/env python3
import logging
from pynput.keyboard import Key, Listener
logging.basicConfig(filename="output.txt", level=logging.DEBUG, format="%(asctime)s - %(message)s")
def on_press(key):
    logging.info(str(key))
with Listener(on_press=on_press) as listener:
    listener.join()
```

- 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.

References: <https://www.comptia.org/certifications/security#examdetails> <https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives>
<https://www.kaspersky.com/resource-center/definitions/logic-bomb>

NEW QUESTION 166

- (Exam Topic 2)

An organization's Chief Information Security Officer is creating a position that will be responsible for implementing technical controls to protect data, including ensuring backups are properly maintained. Which of the following roles would MOST likely include these responsibilities?

- A. Data protection officer
- B. Data owner
- C. Backup administrator
- D. Data custodian
- E. Internal auditor

Answer: C

Explanation:

The role that would most likely include the responsibilities of implementing technical controls to protect data and ensuring backups are properly maintained would be a Backup Administrator. A Backup Administrator is responsible for maintaining and managing an organization's backup systems and procedures, which includes ensuring that backups are properly configured, tested and securely stored. They are also responsible for the recovery of data in case of a disaster or data loss.

NEW QUESTION 168

- (Exam Topic 2)

Which of the following processes would most likely help an organization that has conducted an incident response exercise to improve performance and identify challenges?

- A. Lessons learned
- B. Identification
- C. Simulation
- D. Containment

Answer: A

Explanation:

Lessons learned is a process that would most likely help an organization that has conducted an incident response exercise to improve performance and identify challenges. Lessons learned is a process that involves reviewing and evaluating the incident response exercise to identify what went well, what went wrong, and what can be improved. Lessons learned can help an organization enhance its incident response capabilities, address any gaps or weaknesses, and update its incident response plan accordingly.

References: <https://www.comptia.org/certifications/security#examdetails> <https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives>
<https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901>

NEW QUESTION 171

- (Exam Topic 2)

An organization needs to implement more stringent controls over administrator/root credentials and service accounts. Requirements for the project include:

- * Check-in/checkout of credentials
- * The ability to use but not know the password
- * Automated password changes
- * Logging of access to credentials

Which of the following solutions would meet the requirements?

- A. OAuth 2.0
- B. Secure Enclave
- C. A privileged access management system
- D. An OpenID Connect authentication system

Answer: C

Explanation:

A privileged access management (PAM) system is a solution that helps protect organizations against cyberthreats by monitoring, detecting, and preventing unauthorized privileged access to critical resources¹². A PAM system can meet the requirements of the project by providing features such as:

➤ Check-in/checkout of credentials: A PAM system can store and manage privileged credentials in a secure vault, and allow authorized users to check out credentials when needed and check them back in when done. This reduces the risk of credential theft, misuse, or sharing^{2g3}.

➤ The ability to use but not know the password: A PAM system can enable users to access privileged accounts or resources without revealing the actual password, using methods such as password injection, session proxy, or single sign-on²³. This prevents users from copying, changing, or sharing password^{2s}.

➤ Automated password changes: A PAM system can automatically rotate and update passwords for privileged accounts according to predefined policies, such as frequency, complexity, and uniqueness²³.

. This ensures that passwords are always strong and unpredictable, and reduces the risk of password reuse or compromise².

➤ Logging of access to credentials: A PAM system can record and audit all activities related to privileged access, such as who accessed what credentials, when, why, and what they did with them²³. This provides visibility and accountability for privileged access, and enables detection and investigation of anomalies or incidents².

A PAM system is different from OAuth 2.0, which is an authorization framework that enables third-party applications to obtain limited access to an HTTP service on behalf of a resource owner⁴. OAuth 2.0 does not provide the same level of control and security over privileged access as a PAM system does.

A PAM system is also different from a secure enclave, which is a hardware-based security feature that creates an isolated execution environment within a processor to protect sensitive data from unauthorized access or modification⁵. A secure enclave does not provide the same functionality as a PAM system for managing privileged credentials and access.

A PAM system is also different from an OpenID Connect authentication system, which is an identity layer on top of OAuth 2.0 that enables users to verify their identity across multiple websites using a single login⁶. OpenID Connect does not provide the same scope and granularity as a PAM system for controlling and monitoring privileged access.

NEW QUESTION 173

- (Exam Topic 2)

A company is focused on reducing risks from removable media threats. Due to certain primary applications, removable media cannot be entirely prohibited at this time. Which of the following best describes the company's approach?

- A. Compensating controls
- B. Directive control
- C. Mitigating controls
- D. Physical security controls

Answer: C

Explanation:

Mitigating controls are designed to reduce the impact or severity of an event that has occurred or is likely to occur. They do not prevent or detect the event, but rather limit the damage or consequences of it. For example, a backup system is a mitigating control that can help restore data after a loss or corruption. In this case, the company is focused on reducing risks from removable media threats, which are threats that can compromise data security, introduce malware infections, or cause media failure¹²³. Removable media threats can be used to bypass network defenses and target industrial/OT environments². The company cannot prohibit removable media entirely because of certain primary applications that require them, so it implements mitigating controls to lessen the potential harm from these threats.

Some examples of mitigating controls for removable media threats are:

- Encrypting data on removable media
- Scanning removable media for malware before use
- Restricting access to removable media ports
- Implementing policies and procedures for removable media usage and disposal
- Educating users on the risks and best practices of removable media

NEW QUESTION 175

- (Exam Topic 2)

An organization wants to secure a LAN/WLAN so users can authenticate and transport data securely. The solution needs to prevent on-path attacks and evil twin attacks. Which of the following will best meet the organization's need?

- A. MFA
- B. 802.1X
- C. WPA2
- D. TACACS

Answer: B

Explanation:

* 802.1 X is a standard for network access control that provides authentication and encryption for devices that connect to a LAN/WLAN. 802.1X uses the Extensible Authentication Protocol (EAP) to exchange authentication messages between a supplicant (the device requesting access), an authenticator (the device granting access), and an authentication server (the device verifying credentials). 802.1X can prevent on-path attacks and evil twin attacks by requiring users to provide valid credentials before accessing the network and encrypting the data transmitted over the network. On-path attacks are attacks that involve intercepting or modifying network traffic between two endpoints. An on-path attacker can eavesdrop on sensitive information, alter or inject malicious data, or redirect traffic to malicious destinations. On-path attacks are frequently perpetrated over WiFi network^{1s}. Evil twin attacks are attacks that involve setting up a fake WiFi access point that mimics a legitimate one. An evil twin attacker can trick users into connecting to the fake network and then monitor or manipulate their online activity. Evil twin attacks are more common on public WiFi networks that are unsecured and leave personal data vulnerable²³.

NEW QUESTION 180

- (Exam Topic 2)

An engineer recently deployed a group of 100 web servers in a cloud environment. Per the security policy, all web-server ports except 443 should be disabled. Which of the following can be used to accomplish this task?

- A. Application allow list
- B. Load balancer
- C. Host-based firewall
- D. VPN

Answer: C

Explanation:

A host-based firewall is a software application that runs on each individual host and controls the incoming and outgoing network traffic based on a set of rules. A host-based firewall can be used to block or allow specific ports, protocols, IP addresses, or applications. An engineer can use a host-based firewall to accomplish the task of disabling all web-server ports except 443 on a group of 100 web servers in a cloud

environment. The engineer can configure the firewall rules on each web server to allow only HTTPS traffic on port 443 and deny any other traffic. Alternatively, the engineer can use a centralized management tool to deploy and enforce the firewall rules across all web servers.

NEW QUESTION 185

- (Exam Topic 2)

Which of the following would be best to ensure data is saved to a location on a server, is easily scaled, and is centrally monitored?

- A. Edge computing
- B. Microservices
- C. Containers
- D. Thin client

Answer: C

Explanation:

Containers are a method of virtualization that allow you to run multiple isolated applications on a single server. Containers are lightweight, portable, and scalable, which means they can save resources, improve performance, and simplify deployment. Containers also enable centralized monitoring and management of the applications running on them, using tools such as Docker or Kubernetes. Containers are different from edge computing, which is a distributed computing paradigm that brings computation and data storage closer to the location where it is needed. Microservices are a software architecture style that breaks down complex applications into smaller, independent services that communicate with each other. Thin clients are devices that rely on a server to perform most of the processing tasks and only provide a user interface.

NEW QUESTION 186

- (Exam Topic 2)

A company would like to protect credit card information that is stored in a database from being exposed and reused. However, the current POS system does not support encryption. Which of the following would be BEST suited to secure this information?

(Give me related explanation and references from CompTIA Security+ SY0-601 documents for Correct answer option)

- A. Masking
- B. Tokenization
- C. DLP
- D. SSL/TLS

Answer: B

Explanation:

Tokenization replaces sensitive data with non-sensitive data, such as a unique identifier. This means that the data is still present in the system, but the sensitive information itself is replaced with the token. Tokenization is more secure than masking, which only obscures the data but does not eliminate it. DLP is not suitable for this task, as it is designed to prevent the loss or leakage of data from the system. SSL/TLS can be used to secure the transmission of data, but it cannot prevent the data itself from being exposed or reused. For more information, please refer to CompTIA Security+ SY0-601 Exam Objectives, Section 3.3: Explain the security purpose of authentication, authorization and accounting (AAA) services, and Section 4.7: Explain the purpose and characteristics of various types of encryption.

NEW QUESTION 187

- (Exam Topic 2)

A security administrator installed a new web server. The administrator did this to increase the capacity for an application due to resource exhaustion on another server. Which of the following algorithms should the administrator use to split the number of the connections on each server in half?

- A. Weighted response
- B. Round-robin
- C. Least connection
- D. Weighted least connection

Answer: B

Explanation:

Round-robin is a type of load balancing algorithm that distributes traffic to a list of servers in rotation. It is a static algorithm that does not take into account the state of the system for the distribution of tasks. It assumes that all servers have equal capacity and can handle an equal amount of traffic.

NEW QUESTION 189

- (Exam Topic 2)

A security team will be outsourcing several key functions to a third party and will require that:

- Several of the functions will carry an audit burden.
- Attestations will be performed several times a year.
- Reports will be generated on a monthly basis.

Which of the following BEST describes the document that is used to define these requirements and stipulate how and when they are performed by the third party?

- A. MOU
- B. AUP
- C. SLA
- D. MSA

Answer: C

Explanation:

A service level agreement (SLA) is a contract between a service provider and a customer that outlines the services that are to be provided and the expected levels of performance. It is used to define the requirements for the service, including any attestations and reports that must be generated, and the timescales in which these must be completed. It also outlines any penalties for failing to meet these requirements. SLAs are essential for ensuring that third-party services are meeting the agreed upon performance levels.

Reference: CompTIA Security+ Study Guide: SY0-601 by Emmett Dulaney, Chuck Easttom <https://www.wiley.com/en-us/CompTIA+Security%2B+Study+Guide%3A+SY0-601-p-9781119515968>
CompTIA Security+ Get Certified Get Ahead: SY0-601 Study Guide by Darril Gibson <https://www.amazon.com/CompTIA-Security-Certified-Ahead-SY0-601/dp/1260117558>
Note: SLA is the best document that is used to define these requirements and stipulate how and when they are performed by the third party.

NEW QUESTION 191

- (Exam Topic 2)

A small, local company experienced a ransomware attack. The company has one web-facing server and a few workstations. Everything is behind an ISP firewall. A single web-facing server is set up on the router to forward all ports so that the server is viewable from the internet. The company uses an older version of third-party software to manage the website. The assets were never patched. Which of the following should be done to prevent an attack like this from happening again? (Select three).

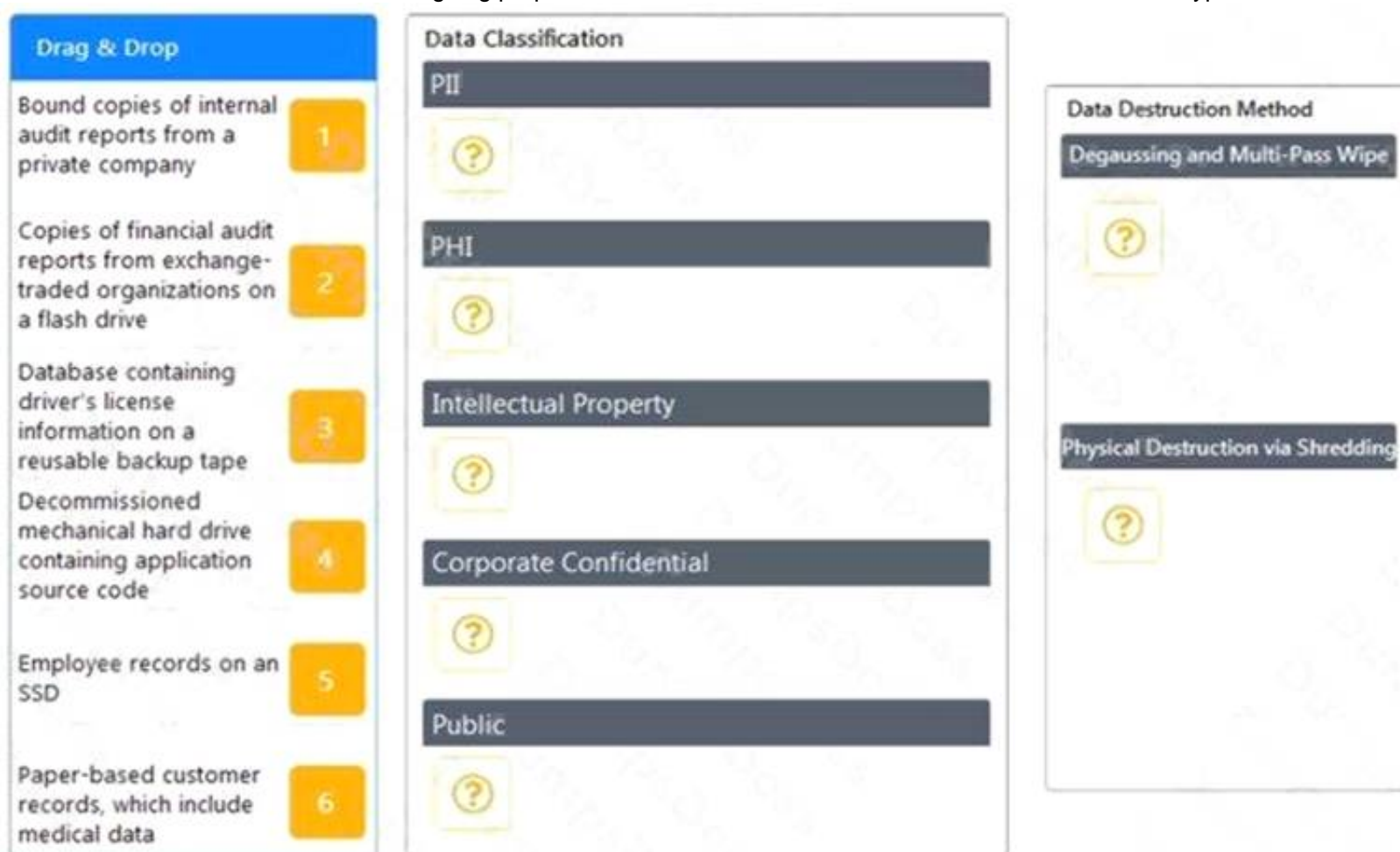
- A. Install DLP software to prevent data loss.
- B. Use the latest version of software.
- C. Install a SIEM device.
- D. Implement MDM.
- E. Implement a screened subnet for the web server.
- F. Install an endpoint security solution.
- G. Update the website certificate and revoke the existing ones.
- H. Deploy additional network sensors.

Answer: BEF

NEW QUESTION 196

- (Exam Topic 2)

A data owner has been tasked with assigning proper data classifications and destruction methods for various types of data contained within the environment.



The screenshot shows a drag-and-drop interface for data classification and destruction methods. On the left, under 'Drag & Drop', there are six items with numbered orange buttons: 1. Bound copies of internal audit reports from a private company, 2. Copies of financial audit reports from exchange-traded organizations on a flash drive, 3. Database containing driver's license information on a reusable backup tape, 4. Decommissioned mechanical hard drive containing application source code, 5. Employee records on an SSD, and 6. Paper-based customer records, which include medical data. In the center, under 'Data Classification', there are five categories: PII, PHI, Intellectual Property, Corporate Confidential, and Public, each with a yellow question mark icon. On the right, under 'Data Destruction Method', there are two methods: Degaussing and Multi-Pass Wipe, and Physical Destruction via Shredding, each with a yellow question mark icon.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, application Description automatically generated

NEW QUESTION 201

- (Exam Topic 2)

A network administrator needs to determine the sequence of a server farm's logs. Which of the following should the administrator consider? (Select TWO).

- A. Chain of custody
- B. Tags
- C. Reports
- D. Time stamps
- E. Hash values
- F. Time offset

Answer: DF

Explanation:

A server farm's logs are records of events that occur on a group of servers that provide the same service or function. Logs can contain information such as date, time, source, destination, message, error code, and severity level. Logs can help administrators monitor the performance, security, and availability of the servers and troubleshoot any issues.

To determine the sequence of a server farm's logs, the administrator should consider the following factors:

➤ Time stamps: Time stamps are indicators of when an event occurred on a server. Time stamps can help administrators sort and correlate events across different servers based on chronological order. However, time stamps alone may not be sufficient to determine the sequence of events if the servers have different time zones or clock settings.

➤ Time offset: Time offset is the difference between the local time of a server and a reference time, such as Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT). Time offset can help administrators adjust and synchronize the time stamps of different servers to a common reference time and eliminate any discrepancies caused by time zones or clock settings.

References: <https://www.comptia.org/certifications/security#examdetails> <https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives>
<https://docs.microsoft.com/en-us/windows-server/administration/server-manager/view-event-logs>

NEW QUESTION 202

- (Exam Topic 2)

An air traffic controller receives a change in flight plan for an morning aircraft over the phone. The air traffic controller compares the change to what appears on radar and determines the information to be false. As a result, the air traffic controller is able to prevent an incident from occurring. Which of the following is this scenario an example of?

- A. Mobile hijacking
- B. Vishing
- C. Unsecure VoIP protocols
- D. SPIM attack

Answer: B

Explanation:

Vishing is a form of phishing that uses voice calls or voice messages to trick victims into revealing personal information, such as credit card numbers, bank details, or passwords. Vishing often uses spoofed phone numbers, voice-altering software, or social engineering techniques to impersonate legitimate organizations or authorities. In this scenario, the caller pretended to be someone who could change the flight plan of an aircraft, which could have caused a serious incident.

NEW QUESTION 207

- (Exam Topic 2)

A network administrator needs to determine the sequence of a server farm's logs. Which of the following should the administrator consider? (Select two).

- A. Chain of custody
- B. Tags
- C. Reports
- D. Time stamps
- E. Hash values
- F. Time offset

Answer: DF

Explanation:

A server farm's logs are records of events that occur on a group of servers that provide the same service or function. Logs can contain information such as date, time, source, destination, message, error code, and severity level. Logs can help administrators monitor the performance, security, and availability of the servers and troubleshoot any issues.

To determine the sequence of a server farm's logs, the administrator should consider the following factors:

➤ Time stamps: Time stamps are indicators of when an event occurred on a server. Time stamps can help administrators sort and correlate events across different servers based on chronological order. However, time stamps alone may not be sufficient to determine the sequence of events if the servers have different time zones or clock settings.

➤ Time offset: Time offset is the difference between the local time of a server and a reference time, such as Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT). Time offset can help administrators adjust and synchronize the time stamps of different servers to a common reference time and eliminate any discrepancies caused by time zones or clock settings.

References: <https://www.comptia.org/certifications/security#examdetails> <https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives>
<https://docs.microsoft.com/en-us/windows-server/administration/server-manager/view-event-logs>

NEW QUESTION 209

- (Exam Topic 2)

A security analyst received the following requirements for the deployment of a security camera solution:

- * The cameras must be viewable by the on-site security guards.
 - * The cameras must be able to communicate with the video storage server.
 - * The cameras must have the time synchronized automatically.
 - * The cameras must not be reachable directly via the internet.
 - * The servers for the cameras and video storage must be available for remote maintenance via the company VPN.
- Which of the following should the security analyst recommend to securely meet the remote connectivity requirements?

- A. Creating firewall rules that prevent outgoing traffic from the subnet the servers and cameras reside on
- B. Deploying a jump server that is accessible via the internal network that can communicate with the servers
- C. Disabling all unused ports on the switch that the cameras are plugged into and enabling MAC filtering
- D. Implementing a WAF to allow traffic from the local NTP server to the camera server

Answer: B

Explanation:

A jump server is a system that is used to manage and access systems in a separate security zone. It acts as a bridge between two different security zones and provides a controlled and secure way of accessing systems between them¹². A jump server can also be used for auditing traffic and user activity for real-time

surveillance 3. By deploying a jump server that is accessible via the internal network, the security analyst can securely meet the remote connectivity requirements for the servers and cameras without exposing them directly to the internet or allowing outgoing traffic from their subnet. The other options are not suitable because:

- A. Creating firewall rules that prevent outgoing traffic from the subnet the servers and cameras reside on would not allow remote maintenance via the company VPN.
- C. Disabling all unused ports on the switch that the cameras are plugged into and enabling MAC filtering would not prevent direct internet access to the cameras or servers.
- D. Implementing a WAF to allow traffic from the local NTP server to the camera server would not address the remote connectivity requirements or protect the servers from internet access.

References:

1: <https://www.thesecuritybuddy.com/network-security/what-is-a-jump-server/> 3:
<https://www.ssh.com/academy/iam/jump-server> 2: https://en.wikipedia.org/wiki/Jump_server

NEW QUESTION 210

- (Exam Topic 2)

A Chief Information Security Officer (CISO) wants to implement a new solution that can protect against certain categories of websites, whether the employee is in the office or away. Which of the following solutions should the CISO implement?

- A. VAF
- B. SWG
- C. VPN
- D. WDS

Answer: B

Explanation:

A secure web gateway (SWG) is a solution that can filter and block malicious or inappropriate web traffic based on predefined policies. It can protect users from web-based threats, such as malware, phishing, or ransomware, whether they are in the office or away. An SWG can be deployed as a hardware appliance, a software application, or a cloud service. References: <https://www.comptia.org/content/guides/what-is-a-secure-web-gateway>

NEW QUESTION 214

- (Exam Topic 2)

A security engineer is concerned the strategy for detection on endpoints is too heavily dependent on previously defined attacks. The engineer wants a tool that can monitor for changes to key files and network traffic for the device. Which of the following tools should the engineer select?

- A. HIDS
- B. AV
- C. NGF-W
- D. DLP

Answer: A

Explanation:

The security engineer should select a Host Intrusion Detection System (HIDS) to address the concern. HIDS monitors and analyzes the internals of a computing system, such as key files and network traffic, for any suspicious activity. Unlike antivirus software (AV), which relies on known signatures of malware, HIDS can detect anomalies, policy violations, and previously undefined attacks by monitoring system behavior and the network traffic of the device.

References:

- * 1. CompTIA Security+ Certification Exam Objectives (SY0-601): <https://www.comptia.jp/pdf/Security%2B%20SY0-601%20Exam%20Objectives.pdf>
- * 2. Scarfone, K., & Mell, P. (2007). Guide to Intrusion Detection and Prevention Systems (IDPS): Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-94. <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf>

NEW QUESTION 218

- (Exam Topic 2)

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

Answer: C

Explanation:

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>

NEW QUESTION 222

- (Exam Topic 2)

A security administrator is integrating several segments onto a single network. One of the segments, which includes legacy devices, presents a significant amount of risk to the network.

Which of the following would allow users to access the legacy devices without compromising the security of the entire network?

- A. NIDS
- B. MAC filtering
- C. Jump server

- D. IPSec
- E. NAT gateway

Answer: C

Explanation:

A jump server is a device that acts as an intermediary between users and other devices on a network. A jump server can provide a secure and controlled access point to the legacy devices without exposing them directly to the network. A jump server can also enforce authentication, authorization, logging, and auditing policies.

NEW QUESTION 225

- (Exam Topic 2)

Which of the following should be addressed first on security devices before connecting to the network?

- A. Open permissions
- B. Default settings
- C. API integration configuration
- D. Weak encryption

Answer: B

Explanation:

Before connecting security devices to the network, it is crucial to address default settings first. Manufacturers often ship devices with default settings that include default usernames, passwords, and configurations. These settings are widely known and can be easily exploited by attackers. Changing default settings helps to secure the device and prevent unauthorized access. Reference: CompTIA Security+ SY0-501 Exam Objectives, Section 3.2: "Given a scenario, implement secure systems design." (<https://www.comptia.jp/pdf/Security%2B%20SY0-501%20Exam%20Objectives.pdf>)

NEW QUESTION 229

- (Exam Topic 2)

A company recently upgraded its authentication infrastructure and now has more computing power. Which of the following should the company consider using to ensure user credentials are being transmitted and stored more securely?

- A. Blockchain
- B. Salting
- C. Quantum
- D. Digital signature

Answer: B

Explanation:

Salting is a technique that adds random data to user credentials before hashing them. This makes the hashed credentials more secure and resistant to brute-force attacks or rainbow table attacks. Salting also ensures that two users with the same password will have different hashed credentials.

A company that has more computing power can consider using salting to ensure user credentials are being transmitted and stored more securely. Salting can increase the complexity and entropy of the hashed credentials, making them harder to crack or reverse.

NEW QUESTION 230

- (Exam Topic 2)

Audit logs indicate an administrative account that belongs to a security engineer has been locked out multiple times during the day. The security engineer has been on vacation (or a few days). Which of the following attacks can the account lockout be attributed to?

- A. Backdoor
- B. Brute-force
- C. Rootkit
- D. Trojan

Answer: B

Explanation:

The account lockout can be attributed to a brute-force attack. A brute-force attack is a type of attack where an attacker attempts to guess a user's password by continually trying different combinations of characters. In this case, it is likely that the security engineer's account was locked out due to an attacker attempting to guess their password. Backdoor, rootkit, and Trojan attacks are not relevant in this scenario.

NEW QUESTION 234

- (Exam Topic 2)

Which of the following models offers third-party-hosted, on-demand computing resources that can be shared with multiple organizations over the internet?

- A. Public cloud
- B. Hybrid cloud
- C. Community cloud
- D. Private cloud

Answer: A

Explanation:

There are three main models for cloud computing: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS)¹². Each model represents a different part of the cloud computing stack and provides different levels of control, flexibility, and management.

According to one source¹, a public cloud is a type of cloud deployment where the cloud resources (such as servers and storage) are owned and operated by a

third-party cloud service provider and delivered over the Internet. A public cloud can be shared with multiple organizations or users who pay for the service on a subscription or pay-as-you-go basis.

NEW QUESTION 235

- (Exam Topic 2)

Which of the following incident response phases should the proper collection of the detected 'ocs and establishment of a chain of custody be performed before?

- A. Containment
- B. Identification
- C. Preparation
- D. Recovery

Answer: A

Explanation:

Containment is the phase where the incident response team tries to isolate and stop the spread of the incident¹². Before containing the incident, the team should collect and preserve any evidence that may be useful for analysis and investigation¹². This includes documenting the incident details, such as date, time, location, source, and impact¹². It also includes establishing a chain of custody, which is a record of who handled the evidence, when, where, how, and why³. A chain of custody ensures the integrity and admissibility of the evidence in court or other legal proceedings³.

NEW QUESTION 236

- (Exam Topic 2)

A network security manager wants to implement periodic events that will test the security team's preparedness for incidents in a controlled and scripted manner, Which of the following concepts describes this scenario?

- A. Red-team exercise
- B. Business continuity plan testing
- C. Tabletop exercise
- D. Functional exercise

Answer: C

Explanation:

A tabletop exercise is a type of security exercise that involves a simulated scenario of a security incident and a discussion of how the security team would respond to it¹. A tabletop exercise is a low-impact and cost-effective way to test the security team's preparedness, identify gaps and areas for improvement, and enhance communication and coordination among team members². A tabletop exercise is different from a red-team exercise, which is a simulated attack by an authorized group of ethical hackers to test the security defenses and response capabilities of an organization³. A business continuity plan testing is a process of verifying that an organization can continue its essential functions and operations in the event of a disaster or disruption⁴. A functional exercise is a type of security exercise that involves a realistic simulation of a security incident and requires the security team to perform their roles and responsibilities as if it were a real event.

References: 1:

<https://www.isaca.org/resources/isaca-journal/issues/2022/volume-1/cybersecurity-incident-response-exercise-g>

2: <https://www.linuxjournal.com/content/security-exercises> 3:

<https://www.imperva.com/learn/application-security/red-team-blue-team/> 4: <https://www.ready.gov/business-continuity-plan> : <https://www.ready.gov/exercises>

NEW QUESTION 237

- (Exam Topic 2)

An organization recently released a zero-trust policy that will enforce who is able to remotely access certain data. Authenticated users who access the data must have a need to know, depending on their level of permissions.

Which of the following is the first step the organization should take when implementing the policy?

- A. Determine a quality CASB solution.
- B. Configure the DLP policies by user groups.
- C. Implement agentless NAC on boundary devices.
- D. Classify all data on the file servers.

Answer: D

Explanation:

zero trust is a security strategy that assumes breach and verifies each request as though it originates from an untrusted network¹². A zero trust policy is a set of "allow rules" that specify conditions for accessing certain resources³.

According to one source⁴, the first step in implementing a zero trust policy is to identify and classify all data and assets in the organization. This helps to determine the level of sensitivity and risk associated with each resource and apply appropriate access controls.

Classifying all data on the file servers is the first step in implementing a zero trust policy because it helps to

determine the level of sensitivity and risk associated with each resource and apply appropriate access controls. Reference: Zero Trust implementation guidance | Microsoft Learn

NEW QUESTION 240

- (Exam Topic 2)

A security analyst needs to recommend a solution that will allow current Active Directory accounts and groups to be used for access controls on both network and remote-access devices. Which of the following should the analyst recommend? (Select two).

- A. TACACS+
- B. RADIUS
- C. OAuth
- D. OpenID
- E. Kerberos
- F. CHAP

Answer: BE

Explanation:

RADIUS and Kerberos are two protocols that can be used to integrate Active Directory accounts and groups with network and remote-access devices. RADIUS is a protocol that provides centralized authentication, authorization, and accounting for network access. It can use Active Directory as a backend database to store user credentials and group memberships. Kerberos is a protocol that provides secure authentication and encryption for network services. It is the default authentication protocol for Active Directory and can be used by remote-access devices that support it.

NEW QUESTION 243

- (Exam Topic 2)

A cybersecurity analyst at Company A is working to establish a secure communication channel with a counter part at Company B, which is 3,000 miles (4.828 kilometers) away. Which of the following concepts would help the analyst meet this goal in a secure manner?

- A. Digital signatures
- B. Key exchange
- C. Salting
- D. PPTP

Answer: B

Explanation:

Key exchange Short explanation

Key exchange is the process of securely sharing cryptographic keys between two parties over a public network. This allows them to establish a secure communication channel and encrypt their messages. There are different methods of key exchange, such as Diffie-Hellman or RSA. References:

<https://www.comptia.org/content/guides/what-is-encryption>

NEW QUESTION 247

- (Exam Topic 2)

A company wants to enable BYOD for checking email and reviewing documents. Many of the documents contain sensitive organizational information. Which of the following should be deployed first before allowing the use of personal devices to access company data?

- A. MDM
- B. RFID
- C. DLR
- D. SIEM

Answer: A

Explanation:

MDM stands for Mobile Device Management, which is a solution that can be used to manage and secure personal devices that access company data. MDM can enforce policies and rules, such as password protection, encryption, remote wipe, device lock, application control, and more. MDM can help a company enable BYOD (Bring Your Own Device) while protecting sensitive organizational information.

NEW QUESTION 252

- (Exam Topic 2)

A retail store has a business requirement to deploy a kiosk computer in an open area. The kiosk computer's operating system has been hardened and tested. A security engineer is concerned that someone could use removable media to install a rootkit. Which of the following should the security engineer configure to BEST protect the kiosk computer?

- A. Measured boot
- B. Boot attestation
- C. UEFI
- D. EDR

Answer: B

Explanation:

Boot attestation is a security feature that enables the computer to verify the integrity of its operating system before it boots. It does this by performing a hash of the operating system and comparing it to the expected hash of the operating system. If the hashes do not match, the computer will not boot and the rootkit will not be allowed to run. This process is also known as measured boot or secure boot.

According to the CompTIA Security+ Study Guide, "Secure Boot is a feature of Unified Extensible Firmware Interface (UEFI) that ensures that code that is executed during the boot process has been authenticated by a cryptographic signature. Secure Boot prevents malicious code from running at boot time, thus providing assurance that the system is executing only code that is legitimate. This provides a measure of protection against rootkits and other malicious code that is designed to run at boot time."

NEW QUESTION 257

- (Exam Topic 2)

A security analyst is assisting a team of developers with best practices for coding. The security analyst would like to defend against the use of SQL injection attacks. Which of the following should the security analyst recommend first?

- A. Tokenization
- B. Input validation
- C. Code signing
- D. Secure cookies

Answer: B

Explanation:

Input validation is a technique that involves checking the user input for any malicious or unexpected characters or commands that could be used to perform SQL injection attacks. Input validation can be done by using allow-lists or deny-lists to filter out the input based on predefined criteria. Input validation can prevent SQL injection attacks by ensuring that only valid and expected input is passed to the database queries.

NEW QUESTION 259

- (Exam Topic 2)

Which of the following can be used by an authentication application to validate a user's credentials without the need to store the actual sensitive data?

- A. Salt string
- B. Private Key
- C. Password hash
- D. Cipher stream

Answer: C

Explanation:

Password hash is a method of storing a user's credentials without the need to store the actual sensitive data. A password hash is a one-way function that transforms the user's password into a fixed-length string of characters that cannot be reversed. The authentication application can then compare the password hash with the stored hash to validate the user's credentials without revealing the original password. References: 1

CompTIA Security+ Certification Exam Objectives, page 15, Domain 3.0: Implementation, Objective 3.5:

Implement secure authentication mechanisms 2

CompTIA Security+ Certification Exam Objectives, page 16,

Domain 3.0: Implementation, Objective 3.6: Implement identity and account management best practices 3

<https://www.comptia.org/blog/what-is-password-hashing>

NEW QUESTION 264

- (Exam Topic 2)

A security analyst is using OSINT to gather information to verify whether company data is available publicly. Which of the following is the BEST application for the analyst to use?

- A. theHarvester
- B. Cuckoo
- B. Nmap
- C. Nessus

Answer: A

Explanation:

TheHarvester is a reconnaissance tool that is used to gather information about a target organization, such as email addresses, subdomains, and IP addresses. It can also be used to gather information about a target individual, such as email addresses, phone numbers, and social media profiles. TheHarvester is specifically designed for OSINT (Open-Source Intelligence) and it can be used to discover publicly available information about a target organization or individual.

NEW QUESTION 269

- (Exam Topic 2)

A security engineer is investigating a penetration test report that states the company website is vulnerable to a web application attack. While checking the web logs from the time of the test, the engineer notices several invalid web form submissions using an unusual address: "SELECT * FROM customername". Which of the following is most likely being attempted?

- A. Directory traversal
- B. SQL injection
- C. Privilege escalation
- D. Cross-site scripting

Answer: B

Explanation:

SQL injection is a web application attack that involves inserting malicious SQL statements into an input field, such as a web form, to manipulate or access the database behind the application. SQL injection can be used to perform various actions, such as reading, modifying, or deleting data, executing commands on the database server, or bypassing authentication. In this scenario, the attacker is trying to use a SQL statement "SELECT * FROM customername" to retrieve all data from the customername table in the database.

NEW QUESTION 273

- (Exam Topic 2)

A network architect wants a server to have the ability to retain network availability even if one of the network switches it is connected to goes down. Which of the following should the architect implement on the server to achieve this goal?

- A. RAID
- B. UPS
- C. NIC teaming
- D. Load balancing

Answer: C

Explanation:

NIC Teaming is a feature that allows a server to be connected to multiple network switches, providing redundancy and increased network availability. If one of the switches goes down, the server will still be able to send and receive data through one of the other switches. To configure NIC Teaming in Windows Server, see Microsoft's documentation:

<https://docs.microsoft.com/en-us/windows-server/networking/technologies/nic-teaming>. For more information on NIC Teaming and other network redundancy features, refer to the CompTIA Security+ SY0-601 Official Text Book and Resources.

NEW QUESTION 275

- (Exam Topic 2)

Which of the following describes software on network hardware that needs to be updated on a rou-tine basis to help address possible vulnerabilities?

- A. Vendor management
- B. Application programming interface
- C. Vanishing
- D. Encryption strength
- E. Firmware

Answer: E

Explanation:

Firmware is software that allows your computer to communicate with hardware devices, such as network routers, switches, or firewalls. Firmware updates can fix bugs, improve performance, and enhance security features. Without firmware updates, the devices you connect to your network might not work properly or might be vulnerable to attacks¹. You can have Windows automatically download recommended drivers and firmware updates for your hardware devices¹, or you can use a network monitoring software to keep track of the firmware status of your devices². You should also follow the best practices for keeping devices and software up to date, such as enforcing automatic updates, monitoring update status, and testing updates before deploying them

NEW QUESTION 280

- (Exam Topic 2)

A user's laptop constantly disconnects from the Wi-Fi network. Once the laptop reconnects, the user can reach the internet but cannot access shared folders or other network resources. Which of the following types of attacks is the user MOST likely experiencing?

- A. Bluejacking
- B. Jamming
- C. Rogue access point
- D. Evil twin

Answer: D

Explanation:

An evil twin attack is when an attacker sets up a fake Wi-Fi network that looks like a legitimate network, but is designed to capture user data that is sent over the network. In this case, the user's laptop is constantly disconnecting and reconnecting to the Wi-Fi network, indicating that it is connecting to the fake network instead of the legitimate one. Once the user connects to the fake network, they are unable to access shared folders or other network resources, as those are only available on the legitimate network.

NEW QUESTION 283

- (Exam Topic 2)

A police department is using the cloud to share information city officials Which of the cloud models describes this scenario?

- A. Hybrid
- B. private
- C. pubic
- D. Community

Answer: D

Explanation:

A community cloud model describes a scenario where a cloud service is shared among multiple organizations that have common goals, interests, or requirements. A community cloud can be hosted by one of the organizations, a third-party provider, or a combination of both. A community cloud can offer benefits such as cost savings, security, compliance, and collaboration. A police department using the cloud to share information with city officials is an example of a community cloud model.

References: <https://www.comptia.org/certifications/security#examdetails> <https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives>
<https://www.ibm.com/cloud/learn/community-cloud>

NEW QUESTION 288

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

SY0-601 Practice Exam Features:

- * SY0-601 Questions and Answers Updated Frequently
- * SY0-601 Practice Questions Verified by Expert Senior Certified Staff
- * SY0-601 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * SY0-601 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The SY0-601 Practice Test Here](#)