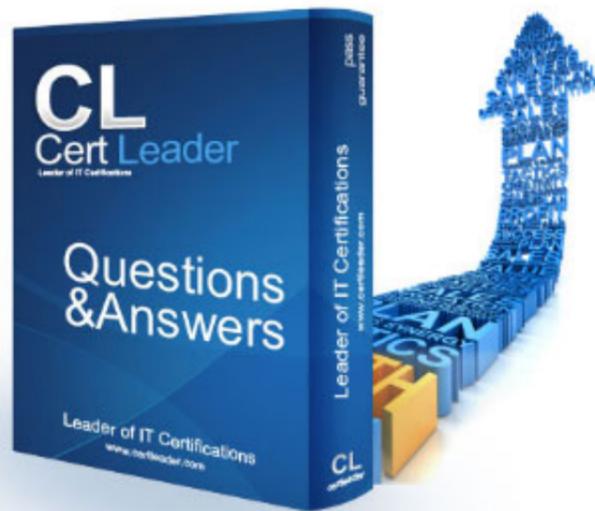


SY0-701 Dumps

CompTIA Security+ Exam

<https://www.certleader.com/SY0-701-dumps.html>



NEW QUESTION 1

Which of the following must be considered when designing a high-availability network? (Choose two).

- A. Ease of recovery
- B. Ability to patch
- C. Physical isolation
- D. Responsiveness
- E. Attack surface
- F. Extensible authentication

Answer: AE

Explanation:

A high-availability network is a network that is designed to minimize downtime and ensure continuous operation even in the event of a failure or disruption. A high-availability network must consider the following factors¹²:

? Ease of recovery: This refers to the ability of the network to restore normal functionality quickly and efficiently after a failure or disruption. Ease of recovery can be achieved by implementing backup and restore procedures, redundancy and failover mechanisms, fault tolerance and resilience, and disaster recovery plans.

? Attack surface: This refers to the amount of exposure and vulnerability of the network to potential threats and attacks. Attack surface can be reduced by implementing security controls such as firewalls, encryption, authentication, access control, segmentation, and hardening.

The other options are not directly related to high-availability network design:

? Ability to patch: This refers to the process of updating and fixing software components to address security issues, bugs, or performance improvements. Ability to patch is important for maintaining the security and functionality of the network, but it is not a specific factor for high-availability network design.

? Physical isolation: This refers to the separation of network components or devices from other networks or physical environments. Physical isolation can enhance the security and performance of the network, but it can also reduce the availability and accessibility of the network resources.

? Responsiveness: This refers to the speed and quality of the network's performance and service delivery. Responsiveness can be measured by metrics such as latency, throughput, jitter, and packet loss. Responsiveness is important for ensuring customer satisfaction and user experience, but it is not a specific factor for high-availability network design.

? Extensible authentication: This refers to the ability of the network to support multiple and flexible authentication methods and protocols. Extensible authentication can improve the security and convenience of the network, but it is not a specific factor for high-availability network design.

References = 1: CompTIA Security+ SY0-701 Certification Study Guide, page 972: High Availability – CompTIA Security+ SY0-701 – 3.4, video by Professor Messer.

NEW QUESTION 2

Which of the following can be used to identify potential attacker activities without affecting production servers?

- A. Honey pot
- B. Video surveillance
- C. Zero Trust
- D. Geofencing

Answer: A

Explanation:

A honey pot is a system or a network that is designed to mimic a real production server and attract potential attackers. A honey pot can be used to identify the attacker's methods, techniques, and objectives without affecting the actual production servers. A honey pot can also divert the attacker's attention from the real targets and waste their time and resources¹².

The other options are not effective ways to identify potential attacker activities without affecting production servers:

? Video surveillance: This is a physical security technique that uses cameras and monitors to record and observe the activities in a certain area. Video surveillance can help to deter, detect, and investigate physical intrusions, but it does not directly identify the attacker's activities on the network or the servers³.

? Zero Trust: This is a security strategy that assumes that no user, device, or network is trustworthy by default and requires strict verification and validation for every request and transaction. Zero Trust can help to improve the security posture and reduce the attack surface of an organization, but it does not directly identify the attacker's activities on the network or the servers⁴.

? Geofencing: This is a security technique that uses geographic location as a criterion to restrict or allow access to data or resources. Geofencing can help to protect the data sovereignty and compliance of an organization, but it does not directly identify the attacker's activities on the network or the servers⁵.

References = 1: CompTIA Security+ SY0-701 Certification Study Guide, page 542: Honeypots and Deception – SY0-601 CompTIA Security+ : 2.1, video by Professor Messer³; CompTIA Security+ SY0-701 Certification Study Guide, page 974: CompTIA Security+ SY0-701 Certification Study Guide, page 985: CompTIA Security+ SY0-701 Certification Study Guide, page 99.

NEW QUESTION 3

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

- A. Obtain the file's SHA-256 hash.
- B. Use hexdump on the file's contents.
- C. Check endpoint logs.
- D. Query the file's metadata.

Answer: D

Explanation:

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

References: 1: How do I get the meta-data of a video file? 2: How to check if an mp4 file contains malware? 3: [Hexdump - Wikipedia]

NEW QUESTION 4

Which of the following provides the details about the terms of a test with a third-party penetration tester?

- A. Rules of engagement
- B. Supply chain analysis
- C. Right to audit clause
- D. Due diligence

Answer: A

Explanation:

Rules of engagement are the detailed guidelines and constraints regarding the execution of information security testing, such as penetration testing. They define the scope, objectives, methods, and boundaries of the test, as well as the roles and responsibilities of the testers and the clients. Rules of engagement help to ensure that the test is conducted in a legal, ethical, and professional manner, and that the results are accurate and reliable. Rules of engagement typically include the following elements:

- ? The type and scope of the test, such as black box, white box, or gray box, and the target systems, networks, applications, or data.
- ? The client contact details and the communication channels for reporting issues, incidents, or emergencies during the test.
- ? The testing team credentials and the authorized tools and techniques that they can use.
- ? The sensitive data handling and encryption requirements, such as how to store, transmit, or dispose of any data obtained during the test.
- ? The status meeting and report schedules, formats, and recipients, as well as the confidentiality and non-disclosure agreements for the test results.
- ? The timeline and duration of the test, and the hours of operation and testing windows.
- ? The professional and ethical behavior expectations for the testers, such as avoiding unnecessary damage, disruption, or disclosure of information.

Supply chain analysis, right to audit clause, and due diligence are not related to the terms of a test with a third-party penetration tester. Supply chain analysis is the process of evaluating the security and risk posture of the suppliers and partners in a business network. Right to audit clause is a provision in a contract that gives one party the right to audit another party to verify their compliance with the contract terms and conditions. Due diligence is the process of identifying and addressing the cyber risks that a potential vendor or partner brings to an organization.

References = <https://www.yeahhub.com/every-penetration-tester-you-should-know-about-this-rules-of-engagement/>
<https://bing.com/search?q=rules+of+engagement+penetration+testing>

NEW QUESTION 5

A company is adding a clause to its AUP that states employees are not allowed to modify the operating system on mobile devices. Which of the following vulnerabilities is the organization addressing?

- A. Cross-site scripting
- B. Buffer overflow
- C. Jailbreaking
- D. Side loading

Answer: C

Explanation:

Jailbreaking is the process of removing the restrictions imposed by the manufacturer or carrier on a mobile device, such as an iPhone or iPad. Jailbreaking allows users to install unauthorized applications, modify system settings, and access root privileges. However, jailbreaking also exposes the device to potential security risks, such as malware, spyware, unauthorized access, data loss, and voided warranty. Therefore, an organization may prohibit employees from jailbreaking their mobile devices to prevent these vulnerabilities and protect the corporate data and network. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 10: Mobile Device Security, page 507 2

NEW QUESTION 6

A bank insists all of its vendors must prevent data loss on stolen laptops. Which of the following strategies is the bank requiring?

- A. Encryption at rest
- B. Masking
- C. Data classification
- D. Permission restrictions

Answer: A

Explanation:

Encryption at rest is a strategy that protects data stored on a device, such as a laptop, by converting it into an unreadable format that can only be accessed with a decryption key or password. Encryption at rest can prevent data loss on stolen laptops by preventing unauthorized access to the data, even if the device is physically compromised.

Encryption at rest can also help comply with data privacy regulations and standards that require data protection. Masking, data classification, and permission restrictions are other strategies that can help protect data, but they may not be sufficient or applicable for data stored on laptops. Masking is a technique that obscures sensitive data elements, such as credit card numbers, with random characters or symbols, but it is usually used for data in transit or in use, not at rest. Data classification is a process that assigns labels to data based on its sensitivity and business impact, but it does not protect the data itself. Permission restrictions are rules that define who can access, modify, or delete data, but they may not prevent unauthorized access if the laptop is stolen and the security controls are bypassed. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 17-18, 372-373

NEW QUESTION 7

A systems administrator works for a local hospital and needs to ensure patient data is protected and secure. Which of the following data classifications should be used to secure patient data?

- A. Private
- B. Critical
- C. Sensitive
- D. Public

Answer: C

Explanation:

Data classification is a process of categorizing data based on its level of sensitivity, value, and impact to the organization if compromised. Data classification helps to determine the appropriate security controls and policies to protect the data from unauthorized access, disclosure, or modification. Different organizations may use different data classification schemes, but a common one is the four-tier model, which consists of the following categories: public, private, sensitive, and critical. Public data is data that is intended for public access and disclosure, and has no impact to the organization if compromised. Examples of public data include marketing materials, press releases, and public web pages.

Private data is data that is intended for internal use only, and has a low to moderate impact to the organization if compromised. Examples of private data include employee records, financial reports, and internal policies.

Sensitive data is data that is intended for authorized use only, and has a high impact to the organization if compromised. Examples of sensitive data include personal information, health records, and intellectual property.

Critical data is data that is essential for the organization's operations and survival, and has a severe impact to the organization if compromised. Examples of critical data include encryption keys, disaster recovery plans, and system backups.

Patient data is a type of sensitive data, as it contains personal and health information that is protected by law and ethical standards. Patient data should be used only by authorized personnel for legitimate purposes, and should be secured from unauthorized access, disclosure, or modification. Therefore, the systems administrator should use the sensitive data classification to secure patient data.

References = CompTIA Security+ SY0-701 Certification Study Guide, page 90-91; Professor Messer's CompTIA SY0-701 Security+ Training Course, video 5.5 - Data Classifications, 0:00 - 4:30.

NEW QUESTION 8

After a security awareness training session, a user called the IT help desk and reported a suspicious call. The suspicious caller stated that the Chief Financial Officer wanted credit card information in order to close an invoice. Which of the following topics did the user recognize from the training?

- A. Insider threat
- B. Email phishing
- C. Social engineering
- D. Executive whaling

Answer: C

Explanation:

Social engineering is the practice of manipulating people into performing actions or divulging confidential information, often by impersonating someone else or creating a sense of urgency or trust. The suspicious caller in this scenario was trying to use social engineering to trick the user into giving away credit card information by pretending to be the CFO and asking for a payment. The user recognized this as a potential scam and reported it to the IT help desk. The other topics are not relevant to this

situation. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 19 1

NEW QUESTION 9

A security analyst reviews domain activity logs and notices the following:

```
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
```

Which of the following is the best explanation for what the security analyst has discovered?

- A. The user jsmith's account has been locked out.
- B. A keylogger is installed on [smith's workstation
- C. An attacker is attempting to brute force ismith's account.
- D. Ransomware has been deployed in the domain.

Answer: C

Explanation:

Brute force is a type of attack that tries to guess the password or other credentials of a user account by using a large number of possible combinations. An attacker can use automated tools or scripts to perform a brute force attack and gain unauthorized access to the account. The domain activity logs show that the user ismith has failed to log in 10 times in a row within a short period of time, which is a strong indicator of a brute force attack. The logs also show that the source IP address of the failed logins is different from the usual IP address of ismith, which suggests that the attacker is using a different device or location to launch the attack. The security analyst should take immediate action to block the attacker's IP address, reset ismith's password, and notify ismith of the incident. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 1, page 14. CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 1.1, page 2. Threat Actors and Attributes – SY0-601 CompTIA Security+ : 1.1

NEW QUESTION 10

Which of the following must be considered when designing a high-availability network? (Select two).

- A. Ease of recovery
- B. Ability to patch
- C. Physical isolation
- D. Responsiveness
- E. Attack surface
- F. Extensible authentication

Answer: AE

Explanation:

A high-availability network is a network that is designed to minimize downtime and ensure continuous operation of critical services and applications. To achieve this goal, a high-availability network must consider two important factors: ease of recovery and attack surface.

Ease of recovery refers to the ability of a network to quickly restore normal functionality after a failure, disruption, or disaster. A high-availability network should

have mechanisms such as redundancy, failover, backup, and restore to ensure that any single point of failure does not cause a complete network outage. A high-availability network should also have procedures and policies for incident response, disaster recovery, and business continuity to minimize the impact of any network issue on the organization's operations and reputation. Attack surface refers to the exposure of a network to potential threats and vulnerabilities. A high-availability network should have measures such as encryption, authentication, authorization, firewall, intrusion detection and prevention, and patch management to protect the network from unauthorized access, data breaches, malware, denial-of-service attacks, and other cyberattacks. A high-availability network should also have processes and tools for risk assessment, threat intelligence, vulnerability scanning, and penetration testing to identify and mitigate any weaknesses or gaps in the network security. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 4: Architecture and Design, pages 164-1651. CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 4: Architecture and Design, pages 164-1652.

NEW QUESTION 10

A company decided to reduce the cost of its annual cyber insurance policy by removing the coverage for ransomware attacks. Which of the following analysis elements did the company most likely use in making this decision?

- A. IMTTR
- B. RTO
- C. ARO
- D. MTBF

Answer: C

Explanation:

ARO (Annualized Rate of Occurrence) is an analysis element that measures the frequency or likelihood of an event happening in a given year. ARO is often used in risk assessment and management, as it helps to estimate the potential loss or impact of an event. A company can use ARO to calculate the annualized loss expectancy (ALE) of an event, which is the product of ARO and the single loss expectancy (SLE). ALE represents the expected cost of an event per year, and can be used to compare with the cost of implementing a security control or purchasing an insurance policy.

The company most likely used ARO in making the decision to remove the coverage for ransomware attacks from its cyber insurance policy. The company may have estimated the ARO of ransomware attacks based on historical data, industry trends, or threat intelligence, and found that the ARO was low or negligible. The company may have also calculated the ALE of ransomware attacks, and found that the ALE was lower than the cost of the insurance policy. Therefore, the company decided to reduce the cost of its annual cyber insurance policy by removing the coverage for ransomware attacks, as it deemed the risk to be acceptable or manageable.

IMTTR (Incident Management Team Training and Readiness), RTO (Recovery Time Objective), and MTBF (Mean Time Between Failures) are not analysis elements that the company most likely used in making the decision to remove the coverage for ransomware attacks from its cyber insurance policy. IMTTR is a process of preparing and training the incident management team to respond effectively to security incidents. IMTTR does not measure the frequency or impact of an event, but rather the capability and readiness of the team. RTO is a metric that defines the maximum acceptable time for restoring a system or service after a disruption. RTO does not measure the frequency or impact of an event, but rather the availability and continuity of the system or service. MTBF is a metric that measures the average time between failures of a system or component. MTBF does not measure the frequency or impact of an event, but rather the reliability and performance of the system or component.

References = CompTIA Security+ SY0-701 Certification Study Guide, page 97-

98; Professor Messer's CompTIA SY0-701 Security+ Training Course, video 5.2 - Risk Management, 0:00 - 3:00.

NEW QUESTION 14

A company's web filter is configured to scan the URL for strings and deny access when matches are found. Which of the following search strings should an analyst employ to prohibit access to non-encrypted websites?

- A. encryption=off\
- B. http://
- C. www*.com
- D. :443

Answer: B

Explanation:

A web filter is a device or software that can monitor, block, or allow web traffic based on predefined rules or policies. One of the common methods of web filtering is to scan the URL for strings and deny access when matches are found. For example, a web filter can block access to websites that contain the words "gambling", "porn", or "malware" in their URLs. A URL is a uniform resource locator that identifies the location and protocol of a web resource. A URL typically consists of the following components: protocol://domain:port/path?query#fragment. The protocol specifies the communication method used to access the web resource, such as HTTP, HTTPS, FTP, or SMTP. The domain is the name of the web server that hosts the web resource, such as www.google.com or www.bing.com. The port is an optional number that identifies the specific service or application running on the web server, such as 80 for HTTP or 443 for HTTPS. The path is the specific folder or file name of the web resource, such as /index.html or /images/logo.png. The query is an optional string that contains additional information or parameters for the web resource, such as ?q=security or ?lang=en. The fragment is an optional string that identifies a specific part or section of the web resource, such as #introduction or #summary.

To prohibit access to non-encrypted websites, an analyst should employ a search string that matches the protocol of non-encrypted web traffic, which is HTTP. HTTP stands for hypertext transfer protocol, and it is a standard protocol for transferring data between web servers and web browsers. However, HTTP does not provide any encryption or security for the data, which means that anyone who intercepts the web traffic can read or modify the data. Therefore, non-encrypted websites are vulnerable to eavesdropping, tampering, or spoofing attacks. To access a non-encrypted website, the URL usually starts with http://, followed by the domain name and optionally the port number. For example, http://www.example.com or http://www.example.com:80. By scanning the URL for the string http://, the web filter can identify and block non-encrypted websites.

The other options are not correct because they do not match the protocol of non-encrypted web traffic. Encryption=off is a possible query string that indicates the encryption status of the web resource, but it is not a standard or mandatory parameter. https:// is the protocol of encrypted web traffic, which uses hypertext transfer protocol secure (HTTPS) to provide encryption and security for the data. www*.com is a possible domain name that matches any website that starts with www and ends with .com, but it does not specify the protocol.

:443 is the port number of HTTPS, which is the protocol of encrypted web traffic. References = CompTIA Security+ Study Guide (SY0-701), Chapter 2: Securing Networks, page 69. Professor Messer's CompTIA SY0-701 Security+ Training Course, Section 2.1: Network Devices and Technologies, video: Web Filter (5:16).

NEW QUESTION 18

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

- A. Virtualization
- B. Firmware

- C. Application
- D. Operating system

Answer: B

Explanation:

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

NEW QUESTION 19

A newly identified network access vulnerability has been found in the OS of legacy IoT devices. Which of the following would best mitigate this vulnerability quickly?

- A. Insurance
- B. Patching
- C. Segmentation
- D. Replacement

Answer: C

Explanation:

Segmentation is a technique that divides a network into smaller subnetworks or segments, each with its own security policies and controls. Segmentation can help mitigate network access vulnerabilities in legacy IoT devices by isolating them from other devices and systems, reducing their attack surface and limiting the potential impact of a breach. Segmentation can also improve network performance and efficiency by reducing congestion and traffic. Patching, insurance, and replacement are other possible strategies to deal with network access vulnerabilities, but they may not be feasible or effective in the short term. Patching may not be available or compatible for legacy IoT devices, insurance may not cover the costs or damages of a cyberattack, and replacement may be expensive and time-consuming. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 142-143

NEW QUESTION 22

A systems administrator is working on a solution with the following requirements:

- Provide a secure zone.
- Enforce a company-wide access control policy.
- Reduce the scope of threats.

Which of the following is the systems administrator setting up?

- A. Zero Trust
- B. AAA
- C. Non-repudiation
- D. CIA

Answer: A

Explanation:

Zero Trust is a security model that assumes no trust for any entity inside or outside the network perimeter and requires continuous verification of identity and permissions. Zero Trust can provide a secure zone by isolating and protecting sensitive data and resources from unauthorized access. Zero Trust can also enforce a company-wide access control policy by applying the principle of least privilege and granular segmentation for users, devices, and applications. Zero Trust can reduce the scope of threats by preventing lateral movement and minimizing the attack surface.

References:

? 5: This source explains the concept and benefits of Zero Trust security and how it differs from traditional security models.

? 8: This source provides an overview of Zero Trust identity security and how it can help verify the identity and integrity of users and devices.

NEW QUESTION 27

A company needs to provide administrative access to internal resources while minimizing the traffic allowed through the security boundary. Which of the following methods is most secure?

- A. Implementing a bastion host
- B. Deploying a perimeter network
- C. Installing a WAF
- D. Utilizing single sign-on

Answer: A

Explanation:

A bastion host is a special-purpose server that is designed to withstand attacks and provide secure access to internal resources. A bastion host is usually placed on the edge of a network, acting as a gateway or proxy to the internal network. A bastion host can be configured to allow only certain types of traffic, such as SSH or HTTP, and block all other traffic. A bastion host can also run security software such as firewalls, intrusion detection systems, and antivirus programs to monitor and filter incoming and outgoing traffic. A bastion host can provide administrative access to internal resources by requiring strong authentication and encryption, and by logging all activities for auditing purposes¹².

A bastion host is the most secure method among the given options because it minimizes the traffic allowed through the security boundary and provides a single point of control and defense. A bastion host can also isolate the internal network from direct exposure to the internet or other untrusted networks, reducing the attack surface and the risk of compromise³.

Deploying a perimeter network is not the correct answer, because a perimeter network is a network segment that separates the internal network from the external network. A perimeter network usually hosts public-facing services such as web servers, email servers, or DNS servers that need to be accessible from the internet. A perimeter network does not provide administrative access to internal resources, but rather protects them from unauthorized access. A perimeter network can also increase the complexity and cost of network management and security⁴.

Installing a WAF is not the correct answer, because a WAF is a security tool that protects web applications from common web-based attacks by monitoring,

filtering, and blocking HTTP traffic. A WAF can prevent attacks such as cross-site scripting, SQL injection, or file inclusion, among others. A WAF does not provide administrative access to internal resources, but rather protects them from web application vulnerabilities. A WAF is also not a comprehensive solution for network security, as it only operates at the application layer and does not protect against other types of attacks or threats⁵.

Utilizing single sign-on is not the correct answer, because single sign-on is a method of authentication that allows users to access multiple sites, services, or applications with one username and password. Single sign-on can simplify the sign-in process for users and reduce the number of passwords they have to remember and manage. Single sign-on does not provide administrative access to internal resources, but rather enables access to various resources that the user is authorized to use. Single sign-on can also introduce security risks if the user's credentials are compromised or if the single sign-on provider is breached⁶. References = 1: Bastion host - Wikipedia, 2: 14 Best Practices to Secure SSH Bastion Host - goteleport.com, 3: The Importance Of Bastion Hosts In Network

Security, 4: What is the network perimeter? | Cloudflare, 5: What is a WAF? | Web Application Firewall explained, 6: [What is single sign-on (SSO)? - Definition from WhatIs.com]

NEW QUESTION 31

A company is developing a business continuity strategy and needs to determine how many staff members would be required to sustain the business in the case of a disruption. Which of the following best describes this step?

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

Answer: A

Explanation:

Capacity planning is the process of determining the resources needed to meet the current and future demands of an organization. Capacity planning can help a company develop a business continuity strategy by estimating how many staff members would be required to sustain the business in the case of a disruption, such as a natural disaster, a cyberattack, or a pandemic. Capacity planning can also help a company optimize the use of its resources, reduce costs, and improve performance. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 4, page 184. CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 4.1, page 14. Business Continuity – SY0-601 CompTIA Security+ : 4.1

NEW QUESTION 32

Which of the following involves an attempt to take advantage of database misconfigurations?

- A. Buffer overflow
- B. SQL injection
- C. VM escape
- D. Memory injection

Answer: B

Explanation:

SQL injection is a type of attack that exploits a database misconfiguration or a flaw in the application code that interacts with the database. An attacker can inject malicious SQL statements into the user input fields or the URL parameters that are sent to the database server. These statements can then execute unauthorized commands, such as reading, modifying, deleting, or creating data, or even taking over the database server. SQL injection can compromise the confidentiality, integrity, and availability of the data and the system. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 215 1

NEW QUESTION 33

A newly appointed board member with cybersecurity knowledge wants the board of directors to receive a quarterly report detailing the number of incidents that impacted the organization. The systems administrator is creating a way to present the data to the board of directors. Which of the following should the systems administrator use?

- A. Packet captures
- B. Vulnerability scans
- C. Metadata
- D. Dashboard

Answer: D

Explanation:

A dashboard is a graphical user interface that provides a visual representation of key performance indicators, metrics, and trends related to security events and incidents. A dashboard can help the board of directors to understand the number and impact of incidents that affected the organization in a given period, as well as the status and effectiveness of the security controls and processes. A dashboard can also allow the board of directors to drill down into specific details or filter the data by various criteria¹².

A packet capture is a method of capturing and analyzing the network traffic that passes through a device or a network segment. A packet capture can provide detailed information about the source, destination, protocol, and content of each packet, but it is not a suitable way to present a summary of incidents to the board of directors¹³.

A vulnerability scan is a process of identifying and assessing the weaknesses and exposures in a system or a network that could be exploited by attackers. A vulnerability scan can help the organization to prioritize and remediate the risks and improve the security posture, but it is not a relevant way to report the number of incidents that occurred in a quarter¹⁴.

Metadata is data that describes other data, such as its format, origin, structure, or context. Metadata can provide useful information about the characteristics and properties of data, but it is not a meaningful way to communicate the impact and frequency of incidents to the board of directors. References = 1: CompTIA Security+ SY0-701 Certification Study Guide, page 3722: SIEM Dashboards – SY0-601 CompTIA Security+ : 4.3, video by Professor Messer³: CompTIA Security+ SY0-701 Certification Study Guide, page 3464: CompTIA Security+ SY0-701 Certification Study Guide, page 362. : CompTIA Security+ SY0-701 Certification Study Guide, page 97.

NEW QUESTION 37

Which of the following best practices gives administrators a set period to perform changes to an operational system to ensure availability and minimize business impacts?

- A. Impact analysis
- B. Scheduled downtime
- C. Backout plan
- D. Change management boards

Answer: B

Explanation:

Scheduled downtime is a planned period of time when a system or service is unavailable for maintenance, updates, upgrades, or other changes. Scheduled downtime gives administrators a set period to perform changes to an operational system without disrupting the normal business operations or affecting the availability of the system or service. Scheduled downtime also allows administrators to inform the users and stakeholders about the expected duration and impact of the changes. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 12: Security Operations and Administration, page 579 1

NEW QUESTION 41

Which of the following is used to quantitatively measure the criticality of a vulnerability?

- A. CVE
- B. CVSS
- C. CIA
- D. CERT

Answer: B

Explanation:

CVSS stands for Common Vulnerability Scoring System, which is a framework that provides a standardized way to assess and communicate the severity and risk of vulnerabilities. CVSS uses a set of metrics and formulas to calculate a numerical score ranging from 0 to 10, where higher scores indicate higher criticality. CVSS can help organizations prioritize remediation efforts and compare vulnerabilities across different systems and vendors. The other options are not used to measure the criticality of a vulnerability, but rather to identify, classify, or report them. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 39

NEW QUESTION 45

During a security incident, the security operations team identified sustained network traffic from a malicious IP address: 10.1.4.9. A security analyst is creating an inbound firewall rule to block the IP address from accessing the organization's network. Which of the following fulfills this request?

- A. access-list inbound deny ig source 0.0.0.0/0 destination 10.1.4.9/32
- B. access-list inbound deny ig source 10.1.4.9/32 destination 0.0.0.0/0
- C. access-list inbound permit ig source 10.1.4.9/32 destination 0.0.0.0/0
- D. access-list inbound permit ig source 0.0.0.0/0 destination 10.1.4.9/32

Answer: B

Explanation:

A firewall rule is a set of criteria that determines whether to allow or deny a packet to pass through the firewall. A firewall rule consists of several elements, such as the action, the protocol, the source address, the destination address, and the port number. The syntax of a firewall rule may vary depending on the type and vendor of the firewall, but the basic logic is the same. In this question, the security analyst is creating an inbound firewall rule to block the IP address 10.1.4.9 from accessing the organization's network. This means that the action should be deny, the protocol should be any (or ig for IP), the source address should be 10.1.4.9/32 (which means a single IP address), the destination address should be 0.0.0.0/0 (which means any IP address), and the port number should be any. Therefore, the correct firewall rule is:

```
access-list inbound deny ig source 10.1.4.9/32 destination 0.0.0.0/0
```

This rule will match any packet that has the source IP address of 10.1.4.9 and drop it. The other options are incorrect because they either have the wrong action, the wrong source address, or the wrong destination address. For example, option A has the source and destination addresses reversed, which means that it will block any packet that has the destination IP address of 10.1.4.9, which is not the intended goal. Option C has the wrong action, which is permit, which means that it will allow the packet to pass through the firewall, which is also not the intended goal. Option D has the same problem as option A, with the source and destination addresses reversed.

References = Firewall Rules – CompTIA Security+ SY0-401: 1.2, Firewalls – SY0-601 CompTIA Security+ : 3.3, Firewalls – CompTIA Security+ SY0-501, Understanding Firewall Rules – CompTIA Network+ N10-005: 5.5, Configuring Windows Firewall – CompTIA A+ 220-1102 – 1.6.

NEW QUESTION 49

An enterprise has been experiencing attacks focused on exploiting vulnerabilities in older browser versions with well-known exploits. Which of the following security solutions should be configured to best provide the ability to monitor and block these known signature-based attacks?

- A. ACL
- B. DLP
- C. IDS
- D. IPS

Answer: D

Explanation:

An intrusion prevention system (IPS) is a security device that monitors network traffic and blocks or modifies malicious packets based on predefined rules or signatures. An IPS can prevent attacks that exploit known vulnerabilities in older browser versions by detecting and dropping the malicious packets before they reach the target system. An IPS can also perform other functions, such as rate limiting, encryption, or redirection. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 3: Securing Networks, page 132.

NEW QUESTION 53

A security analyst is reviewing alerts in the SIEM related to potential malicious network traffic coming from an employee's corporate laptop. The security analyst has determined that additional data about the executable running on the machine is necessary to continue the investigation. Which of the following logs should the analyst use as a data source?

- A. Application
- B. IPS/IDS
- C. Network
- D. Endpoint

Answer: D

Explanation:

An endpoint log is a file that contains information about the activities and events that occur on an end-user device, such as a laptop, desktop, tablet, or smartphone. Endpoint logs can provide valuable data for security analysts, such as the processes running on the device, the network connections established, the files accessed or modified, the user actions performed, and the applications installed or updated. Endpoint logs can also record the details of any executable files running on the device, such as the name, path, size, hash, signature, and permissions of the executable.

An application log is a file that contains information about the events that occur within a software application, such as errors, warnings, transactions, or performance metrics. Application logs can help developers and administrators troubleshoot issues, optimize performance, and monitor user behavior. However, application logs may not provide enough information about the executable files running on the device, especially if they are malicious or unknown.

An IPS/IDS log is a file that contains information about the network traffic that is monitored and analyzed by an intrusion prevention system (IPS) or an intrusion detection system (IDS). IPS/IDS logs can help security analysts identify and block potential attacks, such as exploit attempts, denial-of-service (DoS) attacks, or malicious scans. However, IPS/IDS logs may not provide enough information about the executable files running on the device, especially if they are encrypted, obfuscated, or use legitimate protocols.

A network log is a file that contains information about the network activity and communication that occurs between devices, such as IP addresses, ports, protocols, packets, or bytes. Network logs can help security analysts understand the network topology, traffic patterns, and bandwidth usage. However, network logs may not provide enough information about the executable files running on the device, especially if they are hidden, spoofed, or use proxy servers.

Therefore, the best log type to use as a data source for additional information about the executable running on the machine is the endpoint log, as it can provide the most relevant and detailed data about the executable file and its behavior.

References = <https://www.crowdstrike.com/cybersecurity-101/observability/application-log/>

<https://owasp.org/www-project-proactive-controls/v3/en/c9-security-logging>

NEW QUESTION 54

A client demands at least 99.99% uptime from a service provider's hosted security services. Which of the following documents includes the information the service provider should return to the client?

- A. MOA
- B. SOW
- C. MOU
- D. SLA

Answer: D

Explanation:

A service level agreement (SLA) is a document that defines the level of service expected by a customer from a service provider, indicating the metrics by which that service is measured, and the remedies or penalties, if any, should the agreed-upon levels not be achieved. An SLA can specify the minimum uptime or availability of a service, such as 99.99%, and the consequences for failing to meet that standard. A memorandum of agreement (MOA), a statement of work (SOW), and a memorandum of understanding (MOU) are other types of documents that can be used to establish a relationship between parties, but they do not typically include the details of service levels and performance metrics that an SLA does. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 16-17

NEW QUESTION 55

An organization wants a third-party vendor to do a penetration test that targets a specific device. The organization has provided basic information about the device. Which of the following best describes this kind of penetration test?

- A. Partially known environment
- B. Unknown environment
- C. Integrated
- D. Known environment

Answer: A

Explanation:

A partially known environment is a type of penetration test where the tester has some information about the target, such as the IP address, the operating system, or the device type. This can help the tester focus on specific vulnerabilities and reduce the scope of the test. A partially known environment is also called a gray box test¹. References: CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 10, page 543.

NEW QUESTION 59

Which of the following is a hardware-specific vulnerability?

- A. Firmware version
- B. Buffer overflow
- C. SQL injection
- D. Cross-site scripting

Answer: A

Explanation:

Firmware is a type of software that is embedded in a hardware device, such as a router, a printer, or a BIOS chip. Firmware controls the basic functions and operations of the device, and it can be updated or modified by the manufacturer or the user. Firmware version is a hardware-specific vulnerability, as it can expose the device to security risks if it is outdated, corrupted, or tampered with. An attacker can exploit firmware vulnerabilities to gain unauthorized access, modify device settings, install malware, or cause damage to the device or the network. Therefore, it is important to keep firmware updated and verify its integrity and authenticity. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 2, page 67. CompTIA Security+ SY0-701 Exam Objectives, Domain 2.1, page 10.

NEW QUESTION 63

A company is planning to set up a SIEM system and assign an analyst to review the logs on a weekly basis. Which of the following types of controls is the company setting up?

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

Answer: C

Explanation:

A detective control is a type of control that monitors and analyzes the events and activities in a system or a network, and alerts or reports when an incident or a violation occurs. A SIEM (Security Information and Event Management) system is a tool that collects, correlates, and analyzes the logs from various sources, such as firewalls, routers, servers, or applications, and provides a centralized view of the security status and incidents. An analyst who reviews the logs on a weekly basis can identify and investigate any anomalies, trends, or patterns that indicate a potential threat or a breach. A detective control can help the company to respond quickly and effectively to the incidents, and to improve its security posture and resilience. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 1, page 23. CompTIA Security+ SY0-701 Exam Objectives, Domain 4.3, page 14.

NEW QUESTION 65

A systems administrator is creating a script that would save time and prevent human error when performing account creation for a large number of end users. Which of the following would be a good use case for this task?

- A. Off-the-shelf software
- B. Orchestration
- C. Baseline
- D. Policy enforcement

Answer: B

Explanation:

Orchestration is the process of automating multiple tasks across different systems and applications. It can help save time and reduce human error by executing predefined workflows and scripts. In this case, the systems administrator can use orchestration to create accounts for a large number of end users without having to manually enter their information and assign permissions. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 457 1

NEW QUESTION 67

Which of the following is the phase in the incident response process when a security analyst reviews roles and responsibilities?

- A. Preparation
- B. Recovery
- C. Lessons learned
- D. Analysis

Answer: A

Explanation:

Preparation is the phase in the incident response process when a security analyst reviews roles and responsibilities, as well as the policies and procedures for handling incidents. Preparation also involves gathering and maintaining the necessary tools, resources, and contacts for responding to incidents. Preparation can help a security analyst to be ready and proactive when an incident occurs, as well as to reduce the impact and duration of the incident.

Some of the activities that a security analyst performs during the preparation phase are:

? Defining the roles and responsibilities of the incident response team members, such as the incident manager, the incident coordinator, the technical lead, the communications lead, and the legal advisor.

? Establishing the incident response plan, which outlines the objectives, scope, authority, and procedures for responding to incidents, as well as the escalation and reporting mechanisms.

? Developing the incident response policy, which defines the types and categories of incidents, the severity levels, the notification and reporting requirements, and the roles and responsibilities of the stakeholders.

? Creating the incident response playbook, which provides the step-by-step guidance and checklists for handling specific types of incidents, such as denial-of-service, ransomware, phishing, or data breach.

? Acquiring and testing the incident response tools, such as network and host-based scanners, malware analysis tools, forensic tools, backup and recovery tools, and communication and collaboration tools.

? Identifying and securing the incident response resources, such as the incident response team, the incident response location, the evidence storage, and the external support.

? Building and maintaining the incident response contacts, such as the internal and external stakeholders, the law enforcement agencies, the regulatory bodies, and the media.

References:

? CompTIA Security+ SY0-701 Certification Study Guide, Chapter 6: Architecture and Design, Section 6.4: Secure Systems Design, p. 279-280

? CompTIA Security+ SY0-701 Certification Exam Objectives, Domain 3: Architecture and Design, Objective 3.5: Given a scenario, implement secure network architecture concepts, Sub-objective: Incident response, p. 16

NEW QUESTION 72

A security manager created new documentation to use in response to various types of security incidents. Which of the following is the next step the manager should take?

- A. Set the maximum data retention policy.
- B. Securely store the documents on an air-gapped network.
- C. Review the documents' data classification policy.
- D. Conduct a tabletop exercise with the team.

Answer: D

Explanation:

A tabletop exercise is a simulated scenario that tests the effectiveness of a security incident response plan. It involves gathering the relevant stakeholders and walking through the steps of the plan, identifying any gaps or issues that need to be addressed. A tabletop exercise is a good way to validate the documentation created by the security manager and ensure that the team is prepared for various types of security incidents. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 6: Risk Management, page 2841. CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 6: Risk Management, page 2842.

NEW QUESTION 76

Which of the following would be the best way to handle a critical business application that is running on a legacy server?

- A. Segmentation
- B. Isolation
- C. Hardening
- D. Decommissioning

Answer: C

Explanation:

A legacy server is a server that is running outdated or unsupported software or hardware, which may pose security risks and compatibility issues. A critical business application is an application that is essential for the operation and continuity of the business, such as accounting, payroll, or inventory management. A legacy server running a critical business application may be difficult to replace or upgrade, but it should not be left unsecured or exposed to potential threats. One of the best ways to handle a legacy server running a critical business application is to harden it. Hardening is the process of applying security measures and configurations to a system to reduce its attack surface and vulnerability. Hardening a legacy server may involve steps such as:

? Applying patches and updates to the operating system and the application, if available

? Removing or disabling unnecessary services, features, or accounts

? Configuring firewall rules and network access control lists to restrict inbound and outbound traffic

? Enabling encryption and authentication for data transmission and storage

? Implementing logging and monitoring tools to detect and respond to anomalous or malicious activity

? Performing regular backups and testing of the system and the application

Hardening a legacy server can help protect the critical business application from unauthorized access, modification, or disruption, while maintaining its functionality and availability. However, hardening a legacy server is not a permanent solution, and it may not be sufficient to address all the security issues and challenges posed by the outdated or unsupported system. Therefore, it is advisable to plan for the eventual decommissioning or migration of the legacy server to a more secure and modern platform, as soon as possible. References: CompTIA Security+ SY0-701 Certification Study Guide, Chapter 3: Architecture and Design, Section 3.2: Secure System Design, Page 133 1; CompTIA Security+ Certification Exam Objectives, Domain 3: Architecture and Design, Objective 3.2: Explain the importance of secure system design, Subobjective: Legacy systems 2

NEW QUESTION 81

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

- A. RBAC
- B. ACL
- C. SAML
- D. GPO

Answer: A

Explanation:

RBAC stands for Role-Based Access Control, which is a method of restricting access to data and resources based on the roles or responsibilities of users. RBAC simplifies the management of permissions by assigning roles to users and granting access rights to roles, rather than to individual users. RBAC can help enforce the principle of least privilege and reduce the risk of unauthorized access or data leakage. The other options are not as suitable for the scenario as RBAC, as they either do not prevent access based on responsibilities, or do not apply a simplified format. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 133 1

NEW QUESTION 85

Which of the following describes the reason root cause analysis should be conducted as part of incident response?

- A. To gather IoCs for the investigation
- B. To discover which systems have been affected
- C. To eradicate any trace of malware on the network
- D. To prevent future incidents of the same nature

Answer: D

Explanation:

Root cause analysis is a process of identifying and resolving the underlying factors that led to an incident. By conducting root cause analysis as part of incident response, security professionals can learn from the incident and implement corrective actions to prevent future incidents of the same nature. For example, if the root cause of a data breach was a weak password policy, the security team can enforce a stronger password policy and educate users on the importance of password security. Root cause analysis can also help to improve security processes, policies, and procedures, and to enhance security awareness and culture within the organization. Root cause analysis is not meant to gather IoCs (indicators of compromise) for the investigation, as this is a task performed during the identification and analysis phases of incident response. Root cause analysis is also not meant to discover which systems have been affected or to eradicate any trace of malware on the network, as these are tasks performed during the containment and eradication phases of incident response. References = CompTIA Security+ SY0-701 Certification Study Guide, page 424-425; Professor Messer's CompTIA SY0-701 Security+ Training Course, video 5.1 - Incident Response, 9:55 - 11:18.

NEW QUESTION 87

Which of the following vulnerabilities is associated with installing software outside of a manufacturer's approved software repository?

- A. Jailbreaking

- B. Memory injection
- C. Resource reuse
- D. Side loading

Answer: D

Explanation:

Side loading is the process of installing software outside of a manufacturer's approved software repository. This can expose the device to potential vulnerabilities, such as malware, spyware, or unauthorized access. Side loading can also bypass security controls and policies that are enforced by the manufacturer or the organization. Side loading is often done by users who want to access applications or features that are not available or allowed on their devices. References = Sideload - CompTIA Security+ Video Training | Interface Technical Training, Security+ (Plus) Certification | CompTIA IT Certifications, Load Balancers – CompTIA Security+ SY0-501 – 2.1, CompTIA Security+ SY0-601 Certification Study Guide.

NEW QUESTION 92

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

- A. Concurrent session usage
- B. Secure DNS cryptographic downgrade
- C. On-path resource consumption
- D. Reflected denial of service

Answer: D

Explanation:

A reflected denial of service (RDoS) attack is a type of DDoS attack that uses spoofed source IP addresses to send requests to a third-party server, which then sends responses to the victim server. The attacker exploits the difference in size between the request and the response, which can amplify the amount of traffic sent to the victim server. The attacker also hides their identity by using the victim's IP address as the source. A RDoS attack can target DNS servers by sending forged DNS queries that generate large DNS responses. This can flood the network interface of the DNS server and prevent it from serving legitimate requests from end users. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 215-216 1

NEW QUESTION 93

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

- A. Deploying a SASE solution to remote employees
- B. Building a load-balanced VPN solution with redundant internet
- C. Purchasing a low-cost SD-WAN solution for VPN traffic
- D. Using a cloud provider to create additional VPN concentrators

Answer: A

Explanation:

SASE stands for Secure Access Service Edge. It is a cloud-based service that combines network and security functions into a single integrated solution. SASE can help reduce traffic on the VPN and internet circuit by providing secure and optimized access to the data center and cloud applications for remote employees. SASE can also monitor and enforce security policies on the remote employee internet traffic, regardless of their location or device. SASE can offer benefits such as lower costs, improved performance, scalability, and flexibility compared to traditional VPN solutions. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 457-458 1

NEW QUESTION 98

An organization would like to store customer data on a separate part of the network that is not accessible to users on the main corporate network. Which of the following should the administrator use to accomplish this goal?

- A. Segmentation
- B. Isolation
- C. Patching
- D. Encryption

Answer: A

Explanation:

Segmentation is a network design technique that divides the network into smaller and isolated segments based on logical or physical boundaries. Segmentation can help improve network security by limiting the scope of an attack, reducing the attack surface, and enforcing access control policies. Segmentation can also enhance network performance, scalability, and manageability. To accomplish the goal of storing customer data on a separate part of the network, the administrator can use segmentation technologies such as subnetting, VLANs, firewalls, routers, or switches. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 308-309 1

NEW QUESTION 101

After reviewing the following vulnerability scanning report:

Server:192.168.14.6

Service: Telnet

Port: 23 Protocol: TCP Status: Open Severity: High

Vulnerability: Use of an insecure network protocol

A security analyst performs the following test: `nmap -p 23 192.168.14.6 --script telnet-encryption PORT STATE SERVICE REASON`

`23/tcp open telnet syn-ack | telnet encryption:`

`|_ Telnet server supports encryption`

Which of the following would the security analyst conclude for this reported vulnerability?

- A. It is a false positive.
- B. A rescan is required.
- C. It is considered noise.
- D. Compensating controls exist.

Answer: A

Explanation:

A false positive is a result that indicates a vulnerability or a problem when there is none. In this case, the vulnerability scanning report shows that the telnet service on port 23 is open and uses an insecure network protocol. However, the security analyst performs a test using nmap and a script that checks for telnet encryption support. The result shows that the telnet server supports encryption, which means that the data transmitted between the client and the server can be protected from eavesdropping. Therefore, the reported vulnerability is a false positive and does not reflect the actual security posture of the server. The security analyst should verify the encryption settings of the telnet server and client and ensure that they are configured properly³. References: 3: Telnet Protocol - Can You Encrypt Telnet?

NEW QUESTION 105

The management team notices that new accounts that are set up manually do not always have correct access or permissions. Which of the following automation techniques should a systems administrator use to streamline account creation?

- A. Guard rail script
- B. Ticketing workflow
- C. Escalation script
- D. User provisioning script

Answer: D

Explanation:

A user provisioning script is an automation technique that uses a predefined set of instructions or commands to create, modify, or delete user accounts and assign appropriate access or permissions. A user provisioning script can help to streamline account creation by reducing manual errors, ensuring consistency and compliance, and saving time and resources¹².

The other options are not automation techniques that can streamline account creation:

? Guard rail script: This is a script that monitors and enforces the security policies and rules on a system or a network. A guard rail script can help to prevent unauthorized or malicious actions, such as changing security settings, accessing restricted resources, or installing unwanted software³.

? Ticketing workflow: This is a process that tracks and manages the requests, issues, or incidents that are reported by users or customers. A ticketing workflow can help to improve the communication, collaboration, and resolution of problems, but it does not automate the account creation process⁴.

? Escalation script: This is a script that triggers an alert or a notification when a certain condition or threshold is met or exceeded. An escalation script can help to inform the relevant parties or authorities of a critical situation, such as a security breach, a performance degradation, or a service outage.

References = 1: CompTIA Security+ SY0-701 Certification Study Guide, page 1022: User Provisioning – CompTIA Security+ SY0-701 – 5.1, video by Professor Messer³: CompTIA Security+ SY0-701 Certification Study Guide, page 1034: CompTIA Security+ SY0-701 Certification Study Guide, page 104. : CompTIA Security+ SY0-701 Certification Study Guide, page 105.

NEW QUESTION 109

A penetration tester begins an engagement by performing port and service scans against the client environment according to the rules of engagement. Which of the following reconnaissance types is the tester performing?

- A. Active
- B. Passive
- C. Defensive
- D. Offensive

Answer: A

Explanation:

Active reconnaissance is a type of reconnaissance that involves sending packets or requests to a target and analyzing the responses. Active reconnaissance can reveal information such as open ports, services, operating systems, and vulnerabilities. However, active reconnaissance is also more likely to be detected by the target or its security devices, such as firewalls or intrusion detection systems. Port and service scans are examples of active reconnaissance techniques, as they involve probing the target for specific information. References = CompTIA Security+ Certification Exam Objectives, Domain 1.1: Given a scenario, conduct reconnaissance using appropriate techniques and tools. CompTIA Security+ Study Guide (SY0-701), Chapter 2: Reconnaissance and Intelligence Gathering, page 47. CompTIA Security+ Certification Exam SY0-701 Practice Test 1, Question 1.

NEW QUESTION 113

Which of the following is required for an organization to properly manage its restore process in the event of system failure?

- A. IRP
- B. DRP
- C. RPO
- D. SDLC

Answer: B

Explanation:

A disaster recovery plan (DRP) is a set of policies and procedures that aim to restore the normal operations of an organization in the event of a system failure, natural disaster, or other emergency. A DRP typically includes the following elements:

? A risk assessment that identifies the potential threats and impacts to the organization's critical assets and processes.

? A business impact analysis that prioritizes the recovery of the most essential functions and data.

? A recovery strategy that defines the roles and responsibilities of the recovery team, the resources and tools needed, and the steps to follow to restore the system.

? A testing and maintenance plan that ensures the DRP is updated and validated regularly. A DRP is required for an organization to properly manage its restore process in the event of system failure, as it provides a clear and structured framework for recovering from a disaster and minimizing the downtime and data loss.

References = CompTIA Security+ Study Guide (SY0-701), Chapter 7: Resilience and Recovery, page 325.

NEW QUESTION 117

An analyst is evaluating the implementation of Zero Trust principles within the data plane. Which of the following would be most relevant for the analyst to evaluate?

- A. Secured zones
- B. Subject role
- C. Adaptive identity
- D. Threat scope reduction

Answer: A

Explanation:

Secured zones are a key component of the Zero Trust data plane, which is the layer where data is stored, processed, and transmitted. Secured zones are logical or physical segments of the network that isolate data and resources based on their sensitivity and risk. Secured zones enforce granular policies and controls to prevent unauthorized access and lateral movement within the network¹.

References: CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 5, page 255.

NEW QUESTION 120

.....

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 SY0-701 Exam with Our Prep Materials Via below:

<https://www.certleader.com/SY0-701-dumps.html>