CompTIA

Exam Questions SY0-701

CompTIA Security+ Exam

NEW QUESTION 1
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 2
An administrator notices that several users are logging in from suspicious IP addresses. After speaking with the users, the administrator determines that the employees were not logging in from those IP addresses and resets the affected users' passwords. Which of the following should the administrator implement to prevent this type of attack from succeeding in the future?

A. Multifactor authentication
B. Permissions assignment
C. Access management
D. Password complexity

Answer: A

Explanation:
The correct answer is A because multifactor authentication (MFA) is a method of verifying a user's identity by requiring more than one factor, such as something the user knows (e.g., password), something the user has (e.g., token), or something the user is (e.g., biometric). MFA can prevent unauthorized access even if the user's password is compromised, as the attacker would need to provide another factor to log in. The other options are incorrect because they do not address the root cause of the attack, which is weak authentication. Permissions assignment (B) is the process of granting or denying access to resources based on the user's role or identity. Access management © is the process of controlling who can access what and under what conditions. Password complexity (D) is the requirement of using strong passwords that are hard to guess or crack, but it does not prevent an attacker from using a stolen password. References = You can learn more about multifactor authentication and other security concepts in the following resources:
? CompTIA Security+ SY0-701 Certification Study Guide, Chapter 1: General Security Concepts1
? Professor Messer's CompTIA SY0-701 Security+ Training Course, Section 1.2: Security Concepts2
? Multi-factor Authentication – SY0-601 CompTIA Security+ : 2.43
? TOTAL: CompTIA Security+ Cert (SY0-701) | Udemy, Section 3: Identity and Access Management, Lecture 15: Multifactor Authentication4
? CompTIA Security+ Certification SY0-601: The Total Course [Video], Chapter 3: Identity and Account Management, Section 2: Enabling Multifactor Authentication5

NEW QUESTION 3
An organization disabled unneeded services and placed a firewall in front of a business- critical legacy system. Which of the following best describes the actions taken by the organization?

A. Exception
B. Segmentation
C. Risk transfer
D. Compensating controls

Answer: D

Explanation:
Compensating controls are alternative security measures that are implemented when the primary controls are not feasible, cost-effective, or sufficient to mitigate the risk. In this case, the organization used compensating controls to protect the legacy system from potential attacks by disabling unneeded services and placing a firewall in front of it. This reduced the attack surface and the likelihood of exploitation.
References:
? Official CompTIA Security+ Study Guide (SY0-701), page 29
? Security Controls - CompTIA Security+ SY0-701 - 1.1 1

NEW QUESTION 4
After a recent vulnerability scan, a security engineer needs to harden the routers within the corporate network. Which of the following is the most appropriate to disable?

A. Console access
B. Routing protocols
C. VLANs
D. Web-based administration

Answer: D

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

NEW QUESTION 5
Which of the following would be the best ways to ensure only authorized personnel can access a secure facility? (Select two).

A. Fencing
B. Video surveillance
C. Badge access
D. Access control vestibule
E. Sign-in sheet
F. Sensor

Answer: CD

Explanation:
Badge access and access control vestibule are two of the best ways to ensure only authorized personnel can access a secure facility. Badge access requires the personnel to present a valid and authenticated badge to a reader or scanner that grants or denies access based on predefined rules and permissions. Access control vestibule is a physical security measure that consists of a small room or chamber with two doors, one leading to the outside and one leading to the secure area. The personnel must enter the vestibule and wait for the first door to close and lock before the second door can be opened. This prevents tailgating or piggybacking by unauthorized individuals. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 4, pages 197-1981

NEW QUESTION 6
A company is required to use certified hardware when building networks. Which of the following best addresses the risks associated with procuring counterfeit hardware?

A. A thorough analysis of the supply chain
B. A legally enforceable corporate acquisition policy
C. A right to audit clause in vendor contracts and SOWs
D. An in-depth penetration test of all suppliers and vendors

Answer: A

Explanation:
Counterfeit hardware is hardware that is built or modified without the authorization of the original equipment manufacturer (OEM). It can pose serious risks to network quality, performance, safety, and reliability12. Counterfeit hardware can also contain malicious components that can compromise the security of the network and the data that flows through it3. To address the risks associated with procuring counterfeit hardware, a company should conduct a thorough analysis of the supply chain, which is the network of entities involved in the production, distribution, and delivery of the hardware. By analyzing the supply chain, the company can verify the origin, authenticity, and integrity of the hardware, and identify any potential sources of counterfeit or tampered products. A thorough analysis of the supply chain can include the following steps:
? Establishing a trusted relationship with the OEM and authorized resellers
? Requesting documentation and certification of the hardware from the OEM or authorized resellers
? Inspecting the hardware for any signs of tampering, such as mismatched labels, serial numbers, or components
? Testing the hardware for functionality, performance, and security
? Implementing a tracking system to monitor the hardware throughout its lifecycle
? Reporting any suspicious or counterfeit hardware to the OEM and law enforcement agencies References = 1: Identify Counterfeit and Pirated Products - Cisco, 2: What Is Hardware Security? Definition, Threats, and Best Practices, 3: Beware of Counterfeit Network Equipment - TechNewsWorld, : Counterfeit Hardware: The Threat and How to Avoid It

NEW QUESTION 7
A healthcare organization wants to provide a web application that allows individuals to digitally report health emergencies.
Which of the following is the most important consideration during development?

A. Scalability
B. Availability
C. Cost
D. Ease of deployment

Answer: B

Explanation:
Availability is the ability of a system or service to be accessible and usable when needed. For a web application that allows individuals to digitally report health emergencies, availability is the most important consideration during development, because any downtime or delay could have serious consequences for the health and safety of the users. The web application should be designed to handle high traffic, prevent denial-of- service attacks, and have backup and recovery plans in case of failures2.
References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 2, page 41.

NEW QUESTION 8

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 9
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 10
An organization is building a new backup data center with cost-benefit as the primary requirement and RTO and RPO values around two days. Which of the following types of sites is the best for this scenario?

A. Real-time recovery
B. Hot
C. Cold
D. Warm

Answer: C

Explanation:
A cold site is a type of backup data center that has the necessary infrastructure to support IT operations, but does not have any pre-configured hardware or software. A cold site is the cheapest option among the backup data center types, but it also has the longest recovery time objective (RTO) and recovery point objective (RPO) values. A cold site is suitable for scenarios where the cost-benefit is the primary requirement and the RTO and RPO values are not very stringent. A cold site can take up to two days or more to restore the normal operations after a disaster. References = CompTIA Security+ SY0-701 Certification Study Guide, page 387; Backup Types – SY0-601 CompTIA Security+ : 2.5, video at 4:50.

NEW QUESTION 11
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 12
An enterprise is trying to limit outbound DNS traffic originating from its internal network. Outbound DNS requests will only be allowed from one device with the IP address 10.50.10.25. Which of the following firewall ACLs will accomplish this goal?

A. Access list outbound permit 0.0.0.0 0 0.0.0.0/0 port 53 Access list outbound deny 10.50.10.25 32 0.0.0.0/0 port 53
B. Access list outbound permit 0.0.0.0/0 10.50.10.25 32 port 53 Access list outbound deny 0.0.0.0 0 0.0.0.0/0 port 53
C. Access list outbound permit 0.0.0.0 0 0.0.0.0/0 port 53 Access list outbound deny 0.0.0.0/0 10.50.10.25 32 port 53
D. Access list outbound permit 10.50.10.25 32 0.0.0.0/0 port 53 Access list outbound deny 0.0.0.0.0.0.0.0/0 port 53

Answer: D

Explanation:
 The correct answer is D because it allows only the device with the IP address 10.50.10.25 to send outbound DNS requests on port 53, and denies all other devices from doing so. The other options are incorrect because they either allow all devices to send outbound DNS requests (A and C), or they allow no devices to send outbound DNS requests (B). References = You can learn more about firewall ACLs and DNS in the following resources:
? CompTIA Security+ SY0-701 Certification Study Guide, Chapter 4: Network Security1
? Professor Messer's CompTIA SY0-701 Security+ Training Course, Section 3.2: Firewall Rules2
? TOTAL: CompTIA Security+ Cert (SY0-701) | Udemy, Section 6: Network Security, Lecture 28: Firewall Rules3

NEW QUESTION 13
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 14
An administrator discovers that some files on a database server were recently encrypted. The administrator sees from the security logs that the data was last accessed by a domain user. Which of the following best describes the type of attack that occurred?

A. Insider threat
B. Social engineering
C. Watering-hole
D. Unauthorized attacker

Answer: A

Explanation:
 An insider threat is a type of attack that originates from someone who has legitimate access to an organization's network, systems, or data. In this case, the domain user who encrypted the files on the database server is an example of an insider threat, as they abused their access privileges to cause harm to the organization. Insider threats can be motivated by various factors, such as financial gain, revenge, espionage, or sabotage. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 1: General Security Concepts, page 251. CompTIA Security+ Certification Kit: Exam SY0- 701, 7th Edition, Chapter 1: General Security Concepts, page 252.
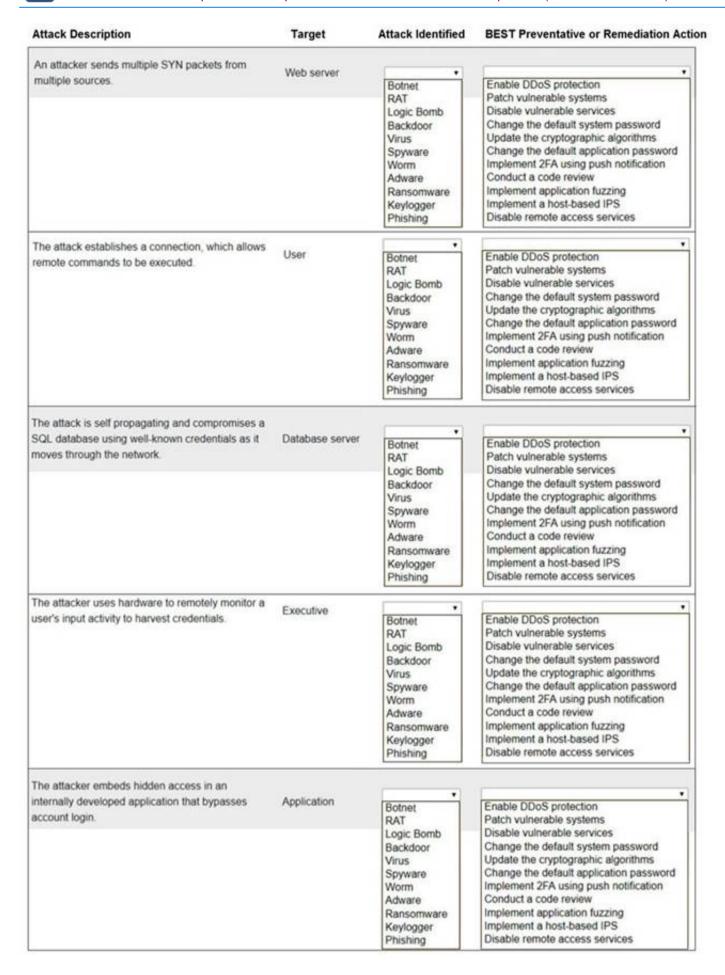
NEW QUESTION 15
HOTSPOT
Select the appropriate attack and remediation from each drop-down list to label the corresponding attack with its remediation.
INSTRUCTIONS
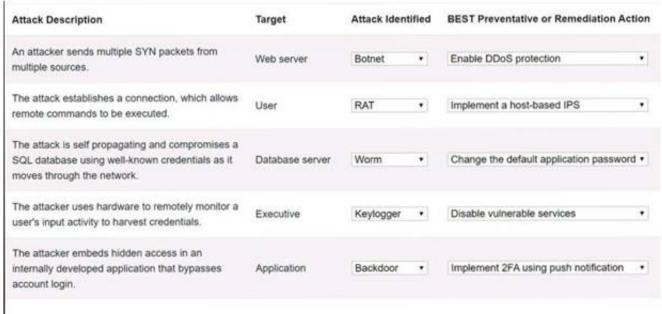Not all attacks and remediation actions will be used.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Attack Description	Target	Attack Identified	BEST Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources.	Web server	Botnet / RAT / Logic Bomb / Backdoor / Virus / Spyware / Worm / Adware / Ransomware / Keylogger / Phishing	Enable DDoS protection / Patch vulnerable systems / Disable vulnerable services / Change the default system password / Update the cryptographic algorithms / Change the default application password / Implement 2FA using push notification / Conduct a code review / Implement application fuzzing / Implement a host-based IPS / Disable remote access services
The attack establishes a connection, which allows remote commands to be executed.	User	Botnet / RAT / Logic Bomb / Backdoor / Virus / Spyware / Worm / Adware / Ransomware / Keylogger / Phishing	Enable DDoS protection / Patch vulnerable systems / Disable vulnerable services / Change the default system password / Update the cryptographic algorithms / Change the default application password / Implement 2FA using push notification / Conduct a code review / Implement application fuzzing / Implement a host-based IPS / Disable remote access services
The attack is self propagating and compromises a SQL database using well-known credentials as it moves through the network.	Database server	Botnet / RAT / Logic Bomb / Backdoor / Virus / Spyware / Worm / Adware / Ransomware / Keylogger / Phishing	Enable DDoS protection / Patch vulnerable systems / Disable vulnerable services / Change the default system password / Update the cryptographic algorithms / Change the default application password / Implement 2FA using push notification / Conduct a code review / Implement application fuzzing / Implement a host-based IPS / Disable remote access services
The attacker uses hardware to remotely monitor a user's input activity to harvest credentials.	Executive	Botnet / RAT / Logic Bomb / Backdoor / Virus / Spyware / Worm / Adware / Ransomware / Keylogger / Phishing	Enable DDoS protection / Patch vulnerable systems / Disable vulnerable services / Change the default system password / Update the cryptographic algorithms / Change the default application password / Implement 2FA using push notification / Conduct a code review / Implement application fuzzing / Implement a host-based IPS / Disable remote access services
The attacker embeds hidden access in an internally developed application that bypasses account login.	Application	Botnet / RAT / Logic Bomb / Backdoor / Virus / Spyware / Worm / Adware / Ransomware / Keylogger / Phishing	Enable DDoS protection / Patch vulnerable systems / Disable vulnerable services / Change the default system password / Update the cryptographic algorithms / Change the default application password / Implement 2FA using push notification / Conduct a code review / Implement application fuzzing / Implement a host-based IPS / Disable remote access services

Solution:

Web serverBotnet Enable DDoS protectionUser RAT Implement a host-based IPS Database server Worm Change the default application passwordExecutive KeyloggerDisable vulnerable servicesApplication Backdoor Implement 2FA using push notification

Attack Description	Target	Attack Identified	BEST Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources.	Web server	Botnet	Enable DDoS protection
The attack establishes a connection, which allows remote commands to be executed.	User	RAT	Implement a host-based IPS
The attack is self propagating and compromises a SQL database using well-known credentials as it moves through the network.	Database server	Worm	Change the default application password
The attacker uses hardware to remotely monitor a user's input activity to harvest credentials.	Executive	Keylogger	Disable vulnerable services
The attacker embeds hidden access in an internally developed application that bypasses account login.	Application	Backdoor	Implement 2FA using push notification

A screenshot of a computer program
Description automatically generated with low confidence

Does this meet the goal?

A. Yes
B. No

Answer: A

NEW QUESTION 16
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 17
......

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

SY0-701 Practice Exam Features:

* SY0-701 Questions and Answers Updated Frequently

* SY0-701 Practice Questions Verified by Expert Senior Certified Staff

* SY0-701 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* SY0-701 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
Order The SY0-701 Practice Test Here