

CompTIA

Exam Questions SY0-701

CompTIA Security+ Exam



NEW QUESTION 1

Which of the following is the best reason to complete an audit in a banking environment?

- A. Regulatory requirement
- B. Organizational change
- C. Self-assessment requirement
- D. Service-level requirement

Answer: A

Explanation:

A regulatory requirement is a mandate imposed by a government or an authority that must be followed by an organization or an individual. In a banking environment, audits are often required by regulators to ensure compliance with laws, standards, and policies related to security, privacy, and financial reporting. Audits help to identify and correct any gaps or weaknesses in the security posture and the internal controls of the organization. References:

? Official CompTIA Security+ Study Guide (SY0-701), page 507

? Security+ (Plus) Certification | CompTIA IT Certifications 2

NEW QUESTION 2

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 3

Which of the following methods to secure credit card data is best to use when a requirement is to see only the last four numbers on a credit card?

- A. Encryption
- B. Hashing
- C. Masking
- D. Tokenization

Answer: C

Explanation:

Masking is a method to secure credit card data that involves replacing some or all of the digits with symbols, such as asterisks, dashes, or Xs, while leaving some of the original digits visible. Masking is best to use when a requirement is to see only the last four numbers on a credit card, as it can prevent unauthorized access to the full card number, while still allowing identification and verification of the cardholder. Masking does not alter the original data, unlike encryption, hashing, or tokenization, which use algorithms to transform the data into different formats.

References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 2: Compliance and Operational Security, page 721. CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 2: Compliance and Operational Security, page 722.

NEW QUESTION 4

An engineer needs to find a solution that creates an added layer of security by preventing unauthorized access to internal company resources. Which of the following would be the best solution?

- A. RDP server
- B. Jump server
- C. Proxy server
- D. Hypervisor

Answer: B

Explanation:

= A jump server is a server that acts as an intermediary between a user and a target system. A jump server can provide an added layer of security by preventing unauthorized access to internal company resources. A user can connect to the jump server using a secure protocol, such as SSH, and then access the target system from the jump server. This way, the target system is isolated from the external network and only accessible through the jump server. A jump server can also enforce security policies, such as authentication, authorization, logging, and auditing, on the user's connection. A jump server is also known as a bastion host or a jump box. References = CompTIA Security+ Certification Exam Objectives, Domain 3.3: Given a scenario, implement secure network architecture concepts. CompTIA Security+ Study Guide (SY0-701), Chapter 3: Network Architecture and Design, page 101. Other Network Appliances – SY0-601 CompTIA Security+ : 3.3, Video 3:03. CompTIA Security+ Certification Exam SY0-701 Practice Test 1, Question 2.

NEW QUESTION 5

An administrator assists the legal and compliance team with ensuring information about customer transactions is archived for the proper time period. Which of the following data policies is the administrator carrying out?

- A. Compromise
- B. Retention
- C. Analysis
- D. Transfer
- E. Inventory

Answer: B

Explanation:

A data retention policy is a set of rules that defines how long data should be stored and when it should be deleted or archived. An administrator assists the legal and compliance team with ensuring information about customer transactions is archived for the proper time period by following the data retention policy of the organization. This policy helps the organization to comply with legal and regulatory requirements, optimize storage space, and protect data privacy and security. References

? CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 3, Section 3.4, page 1211

? CompTIA Security+ Practice Tests: Exam SY0-701, 3rd Edition, Chapter 3, Question 15, page 832

NEW QUESTION 6

An administrator is reviewing a single server's security logs and discovers the following:

Keywords	Date and Time	Source	Event ID	Task	Category
Audit	09/16/2022	Microsoft	4625	Logon	
Failure	11:13:05 AM	Windows security			
Audit	09/16/2022	Microsoft	4625	Logon	
Failure	11:13:07 AM	Windows security			
Audit	09/16/2022	Microsoft	4625	Logon	
Failure	11:13:09 AM	Windows security			
Audit	09/16/2022	Microsoft	4625	Logon	
Failure	11:13:11 AM	Windows security			
Audit	09/16/2022	Microsoft	4625	Logon	
Failure	11:13:13 AM	Windows security			
Audit	09/16/2022	Microsoft	4625	Logon	
Failure	11:13:15 AM	Windows security			
Audit	09/16/2022	Microsoft	4625	Logon	
Failure	11:13:17 AM	Windows security			
Audit	09/16/2022	Microsoft	4625	Logon	
Failure	11:13:19 AM	Windows security			
Audit	09/16/2022	Microsoft	4625	Logon	
Failure	11:13:21 AM	Windows security			
Audit	09/16/2022	Microsoft	4625	Logon	
Failure	11:13:23 AM	Windows security			
Audit	09/16/2022	Microsoft	4625	Logon	
Failure	11:13:25 AM	Windows security			
Audit	09/16/2022	Microsoft	4625	Logon	
Failure	11:13:27 AM	Windows security			

Which of the following best describes the action captured in this log file?

- A. Brute-force attack
- B. Privilege escalation
- C. Failed password audit
- D. Forgotten password by the user

Answer: A

Explanation:

A brute-force attack is a type of attack that involves systematically trying all possible combinations of passwords or keys until the correct one is found. The log file shows multiple failed login attempts in a short amount of time, which is a characteristic of a brute-force attack. The attacker is trying to guess the password of the Administrator account on the server. The log file also shows the event ID 4625, which indicates a failed logon attempt, and the status code 0xC000006A, which means the user name is correct but the password is wrong. These are indicators of compromise (IoC) that suggest a brute-force attack is taking place.

References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 215-216 and 223 1

NEW QUESTION 7

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 0.0.0.0/0 port 53

Answer: D

Explanation:

A firewall ACL (access control list) is a set of rules that determines which traffic is allowed or denied by the firewall. The rules are processed in order, from top to bottom, until a match is found. The syntax of a firewall ACL rule is:

Access list <direction> <action> <source address> <destination address> <protocol>
<port>

To limit outbound DNS traffic originating from the internal network, the firewall ACL should allow only the device with the IP address 10.50.10.25 to send DNS requests to any destination on port 53, and deny all other outbound traffic on port 53. The correct firewall ACL is:

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 0.0.0.0/0 port 53

The first rule permits outbound traffic from the source address 10.50.10.25/32 (a single host) to any destination address (0.0.0.0/0) on port 53 (DNS). The second rule denies all other outbound traffic on port 532.

References: CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 4, page 175.

NEW QUESTION 8

Which of the following enables the use of an input field to run commands that can view or manipulate data?

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

Answer: D

Explanation:

= SQL injection is a type of attack that enables the use of an input field to run commands that can view or manipulate data in a database. SQL stands for Structured Query Language, which is a language used to communicate with databases. By injecting malicious SQL statements into an input field, an attacker can bypass authentication, access sensitive information, modify or delete data, or execute commands on the server.

SQL injection is one of the most common and dangerous web application

vulnerabilities. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 5, page 195. CompTIA Security+ SY0-701 Exam Objectives, Domain 1.1, page 8.

NEW QUESTION 9

A company prevented direct access from the database administrators' workstations to the network segment that contains database servers. Which of the following should a database administrator use to access the database servers?

- A. Jump server
- B. RADIUS
- C. HSM
- D. Load balancer

Answer: A

Explanation:

A jump server is a device or virtual machine that acts as an intermediary between a user's workstation and a remote network segment. A jump server can be used to securely access servers or devices that are not directly reachable from the user's workstation, such as database servers. A jump server can also provide audit logs and access control for the remote connections. A jump server is also known as a jump box or a jump host12.

RADIUS is a protocol for authentication, authorization, and accounting of network access. RADIUS is not a device or a method to access remote servers, but rather a way to verify the identity and permissions of users or devices that request network access34. HSM is an acronym for Hardware Security Module, which is a physical device that provides secure storage and generation of cryptographic keys. HSMs are used to protect sensitive data and applications, such as digital signatures, encryption, and authentication. HSMs are not used to access remote servers, but rather to enhance the security of the data and applications that reside on them5 .

A load balancer is a device or software that distributes network traffic across multiple servers or devices, based on criteria such as availability, performance, or capacity. A load balancer can improve the scalability, reliability, and efficiency of network services, such as web servers, application servers, or database servers.

A load balancer is not used to access remote servers, but rather to optimize the delivery of the services that run on them. References =

? How to access a remote server using a jump host

? Jump server

? RADIUS

? Remote Authentication Dial-In User Service (RADIUS)

? Hardware Security Module (HSM)

? [What is an HSM?]

? [Load balancing (computing)]

? [What is Load Balancing?]

NEW QUESTION 10

A business received a small grant to migrate its infrastructure to an off-premises solution. Which of the following should be considered first?

- A. Security of cloud providers
- B. Cost of implementation
- C. Ability of engineers
- D. Security of architecture

Answer: D

Explanation:

Security of architecture is the process of designing and implementing a secure infrastructure that meets the business objectives and requirements. Security of architecture should be considered first when migrating to an off-premises solution, such as cloud computing, because it can help to identify and mitigate the potential risks and challenges associated with the migration, such as data security, compliance, availability, scalability, and performance. Security of architecture is different from security of cloud providers, which is the process of evaluating and selecting a trustworthy and reliable cloud service provider that can meet the security and operational needs of the business. Security of architecture is also different from cost of implementation, which is the amount of money required to migrate and maintain the infrastructure in the cloud. Security of architecture is also different from ability of engineers, which is the level of skill and knowledge of the IT staff who are responsible for the migration and management of the cloud infrastructure. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 3491

NEW QUESTION 10

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: D

Explanation:

The data plane, also known as the forwarding plane, is the part of the network that carries user traffic and data. It is responsible for moving packets from one device to another based on the routing and switching decisions made by the control plane. The data plane is a critical component of the Zero Trust architecture, as it is where most of the attacks and breaches occur. Therefore, implementing Zero Trust principles within the data plane can help to improve the security and resilience of the network.

One of the key principles of Zero Trust is to assume breach and minimize the blast radius and segment access. This means that the network should be divided into smaller and isolated segments or zones, each with its own security policies and controls. This way, if one segment is compromised, the attacker cannot easily move laterally to other segments and access more resources or data. This principle is also known as threat scope reduction, as it reduces the scope and impact of a potential threat.

The other options are not as relevant for the data plane as threat scope reduction. Secured zones are a concept related to the control plane, which is the part of the network that makes routing and switching decisions. Subject role is a concept related to the identity plane, which is the part of the network that authenticates and authorizes users and devices. Adaptive identity is a concept related to the policy plane, which is the part of the network that defines and enforces the security policies and rules.

References = <https://bing.com/search?q=Zero+Trust+data+plane> <https://learn.microsoft.com/en-us/security/zero-trust/deploy/data>

NEW QUESTION 15

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 (C) 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 20

A hacker gained access to a system via a phishing attempt that was a direct result of a user clicking a suspicious link. The link laterally deployed ransomware, which laid dormant for multiple weeks, across the network. Which of the following would have mitigated the spread?

- A. IPS
- B. IDS
- C. WAF
- D. UAT

Answer: A

Explanation:

IPS stands for intrusion prevention system, which is a network security device that monitors and blocks malicious traffic in real time. IPS is different from IDS, which only detects and alerts on malicious traffic, but does not block it. IPS would have mitigated the spread of ransomware by preventing the hacker from accessing the system via the phishing link, or by stopping the ransomware from communicating with its command and control server or encrypting the files.

NEW QUESTION 24

Which of the following exercises should an organization use to improve its incident response process?

- A. Tabletop
- B. Replication
- C. Failover
- D. Recovery

Answer: A

Explanation:

A tabletop exercise is a simulated scenario that tests the organization's incident response plan and procedures. It involves key stakeholders and decision-makers who discuss their roles and actions in response to a hypothetical incident. It can help identify gaps, weaknesses, and improvement areas in the incident response process. It can also enhance communication, coordination, and collaboration among the participants. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 525 1

NEW QUESTION 29

A security consultant needs secure, remote access to a client environment. Which of the following should the security consultant most likely use to gain access?

- A. EAP
- B. DHCP
- C. IPSec
- D. NAT

Answer: C

Explanation:

IPSec is a protocol suite that provides secure communication over IP networks. IPSec can be used to create virtual private networks (VPNs) that encrypt and authenticate the data exchanged between two or more parties. IPSec can also provide data integrity, confidentiality, replay protection, and access control. A security consultant can use IPSec to gain secure, remote access to a client environment by establishing a VPN tunnel with the client's network. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 8: Secure Protocols and Services, page 385 1

NEW QUESTION 30

Which of the following actions could a security engineer take to ensure workstations and servers are properly monitored for unauthorized changes and software?

- A. Configure all systems to log scheduled tasks.
- B. Collect and monitor all traffic exiting the network.
- C. Block traffic based on known malicious signatures.
- D. Install endpoint management software on all systems.

Answer: D

Explanation:

Endpoint management software is a tool that allows security engineers to monitor and control the configuration, security, and performance of workstations and servers from a central console. Endpoint management software can help detect and prevent unauthorized changes and software installations, enforce policies and compliance, and provide reports and alerts on the status of the endpoints. The other options are not as effective or comprehensive as endpoint management software for this purpose. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 137 1

NEW QUESTION 31

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 36

A security analyst is reviewing the following logs:

```
[10:00:00 AM] Login rejected - username administrator - password Spring2023
[10:00:01 AM] Login rejected - username jsmith - password Spring2023
[10:00:01 AM] Login rejected - username guest - password Spring2023
[10:00:02 AM] Login rejected - username cpolk - password Spring2023
[10:00:03 AM] Login rejected - username fmartin - password Spring2023
```

Which of the following attacks is most likely occurring?

- A. Password spraying
- B. Account forgery
- C. Pass-the-hash
- D. Brute-force

Answer: A

Explanation:

Password spraying is a type of brute force attack that tries common passwords across several accounts to find a match. It is a mass trial-and-error approach that can bypass account lockout protocols. It can give hackers access to personal or business accounts and information. It is not a targeted attack, but a high-volume attack tactic that uses a dictionary or a list of popular or weak passwords¹².

The logs show that the attacker is using the same password ("password123") to attempt to log in to different accounts ("admin", "user1", "user2", etc.) on the same web server. This is a typical pattern of password spraying, as the attacker is hoping that at least one of the accounts has a weak password that matches the one they are trying. The attacker is also using a tool called Hydra, which is one of the most popular brute force tools, often used in cracking passwords for network authentication³.

Account forgery is not the correct answer, because it involves creating fake accounts or credentials to impersonate legitimate users or entities. There is no evidence of account forgery in the logs, as the attacker is not creating any new accounts or using forged credentials.

Pass-the-hash is not the correct answer, because it involves stealing a hashed user credential and using it to create a new authenticated session on the same network. Pass-the-hash does not require the attacker to know or crack the password, as they use the stored version of the password to initiate a new session⁴. The logs show that the attacker is using plain text passwords, not hashes, to try to log in to the web server.

Brute-force is not the correct answer, because it is a broader term that encompasses different types of attacks that involve trying different variations of symbols or words until the correct password is found. Password spraying is a specific type of brute force attack that uses a single common password against multiple accounts⁵. The logs show that the attacker is using password spraying, not brute force in general, to try to gain access to the web server. References = 1:

Password spraying: An overview of password spraying attacks ... - Norton, 2: Security: Credential Stuffing vs. Password Spraying -

Baeldung, 3: Brute Force Attack: A definition + 6 types to know | Norton, 4: What is a Pass-the-Hash Attack? - CrowdStrike, 5: What is a Brute Force Attack? | Definition, Types &

How It Works - Fortinet

NEW QUESTION 38

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 jsmith's workstation
- C. An attacker is attempting to brute force jsmith'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 jsmith 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 jsmith, 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 jsmith's password, and notify jsmith 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 40

An administrator was notified that a user logged in remotely after hours and copied large amounts of data to a personal device.

Which of the following best describes the user's activity?

- A. Penetration testing
- B. Phishing campaign
- C. External audit
- D. Insider threat

Answer: D

Explanation:

An insider threat is a security risk that originates from within the organization, such as an employee, contractor, or business partner, who has authorized access to the organization's data and systems. An insider threat can be malicious, such as stealing, leaking, or sabotaging sensitive data, or unintentional, such as falling victim to phishing or social engineering. An insider threat can cause significant damage to the organization's reputation, finances, operations, and legal compliance. The user's activity of logging in remotely after hours and copying large amounts of data to a personal device is an example of a malicious insider threat, as it violates the organization's security policies and compromises the confidentiality and integrity of the data. References = Insider Threats – CompTIA Security+ SY0-701: 3.2, video at 0:00; CompTIA Security+ SY0-701 Certification Study Guide, page 133.

NEW QUESTION 45

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 50

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 55

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 58

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 59

Which of the following factors are the most important to address when formulating a training curriculum plan for a security awareness program? (Select two).

- A. Channels by which the organization communicates with customers
- B. The reporting mechanisms for ethics violations
- C. Threat vectors based on the industry in which the organization operates
- D. Secure software development training for all personnel
- E. Cadence and duration of training events
- F. Retraining requirements for individuals who fail phishing simulations

Answer: CE

Explanation:

A training curriculum plan for a security awareness program should address the following factors:

? The threat vectors based on the industry in which the organization operates. This will help the employees to understand the specific risks and challenges that their organization faces, and how to protect themselves and the organization from cyberattacks. For example, a healthcare organization may face different threat vectors than a financial organization, such as ransomware, data breaches, or medical device hacking¹.

? The cadence and duration of training events. This will help the employees to retain the information and skills they learn, and to keep up with the changing security landscape. The training events should be frequent enough to reinforce the key concepts and behaviors, but not too long or too short to lose the attention or interest of the employees. For example, a security awareness program may include monthly newsletters, quarterly webinars, annual workshops, or periodic quizzes².

References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 2, page 34; CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 2, page 55.

NEW QUESTION 62

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 63

An employee receives a text message that appears to have been sent by the payroll department and is asking for credential verification. Which of the following social engineering techniques are being attempted? (Choose two.)

- A. Typosquatting
- B. Phishing
- C. Impersonation
- D. Vishing
- E. Smishing
- F. Misinformation

Answer: BE

Explanation:

Smishing is a type of social engineering technique that uses text messages (SMS) to trick victims into revealing sensitive information, clicking malicious links, or downloading malware. Smishing messages often appear to come from legitimate sources, such as banks, government agencies, or service providers, and use urgent or threatening language to persuade the recipients to take action¹². In this scenario, the text message that claims to be from the payroll department is an example of smishing.

Impersonation is a type of social engineering technique that involves pretending to be someone else, such as an authority figure, a trusted person, or a colleague, to gain the trust or cooperation of the target. Impersonation can be done through various channels, such as phone calls, emails, text messages, or in-person visits, and can be used to obtain information, access, or money from the victim³⁴. In this scenario, the text message that pretends to be from the payroll department is an example of impersonation.

* A. Typosquatting is a type of cyberattack that involves registering domain names that are similar to popular or well-known websites, but with intentional spelling errors or different extensions. Typosquatting aims to exploit the common mistakes that users make when typing web addresses, and redirect them to malicious or fraudulent sites that may steal their information, install malware, or display ads⁵⁶. Typosquatting is not related to text messages or credential verification.

* B. Phishing is a type of social engineering technique that uses fraudulent emails to trick recipients into revealing sensitive information, clicking malicious links, or downloading malware. Phishing emails often mimic the appearance and tone of legitimate organizations, such as banks, retailers, or service providers, and use deceptive or urgent language to persuade the recipients to take action⁷⁸. Phishing is not related to text messages or credential verification.

* D. Vishing is a type of social engineering technique that uses voice calls to trick victims into revealing sensitive information, such as passwords, credit card numbers, or bank account details. Vishing calls often appear to come from legitimate sources, such as law enforcement, government agencies, or technical support, and use scare tactics or false promises to persuade the recipients to comply⁹. Vishing is not related to text messages or credential verification.

* F. Misinformation is a type of social engineering technique that involves spreading false or misleading information to influence the beliefs, opinions, or actions of the target. Misinformation can be used to manipulate public perception, create confusion, damage reputation, or promote an agenda. Misinformation is not related to text messages or credential verification.

References = 1: What is Smishing? | Definition and Examples | Kaspersky 2: Smishing - Wikipedia 3: Impersonation Attacks: What Are They and How Do You Protect Against Them? 4: Impersonation - Wikipedia 5: What is Typosquatting? | Definition and Examples | Kaspersky 6: Typosquatting - Wikipedia 7: What is Phishing? | Definition and Examples | Kaspersky 8: Phishing - Wikipedia 9: What is Vishing? | Definition and Examples | Kaspersky : Vishing - Wikipedia : What is Misinformation? | Definition and Examples | Britannica : Misinformation - Wikipedia

NEW QUESTION 68

A technician wants to improve the situational and environmental awareness of existing users as they transition from remote to in-office work. Which of the following is the best option?

- A. Send out periodic security reminders.
- B. Update the content of new hire documentation.
- C. Modify the content of recurring training.
- D. Implement a phishing campaign.

Answer: C

Explanation:

Recurring training is a type of security awareness training that is conducted periodically to refresh and update the knowledge and skills of the users. Recurring training can help improve the situational and environmental awareness of existing users as they transition from remote to in-office work, as it can cover the latest threats, best practices, and policies that are relevant to their work environment. Modifying the content of recurring training can ensure that the users are aware of the current security landscape and the expectations of their roles. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 5, page 232. CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 5.1, page 18.

NEW QUESTION 73

A company requires hard drives to be securely wiped before sending decommissioned systems to recycling. Which of the following best describes this policy?

- A. Enumeration
- B. Sanitization
- C. Destruction
- D. Inventory

Answer: B

Explanation:

Sanitization is the process of removing sensitive data from a storage device or a system before it is disposed of or reused. Sanitization can be done by using software tools or hardware devices that overwrite the data with random patterns or zeros, making it unrecoverable. Sanitization is different from destruction, which is the physical damage of the storage device to render it unusable. Sanitization is also different from enumeration, which is the identification of network resources or devices, and inventory, which is the tracking of assets and their locations. The policy of securely wiping hard drives before sending decommissioned systems to recycling is an example of sanitization, as it ensures that no confidential data can be retrieved from the recycled devices. References = Secure Data Destruction – SY0-601 CompTIA Security+ : 2.7, video at 1:00; CompTIA Security+ SY0-701 Certification Study Guide, page 387.

NEW QUESTION 75

After a company was compromised, customers initiated a lawsuit. The company's attorneys have requested that the security team initiate a legal hold in response to the lawsuit. Which of the following describes the action the security team will most likely be required to take?

- A. Retain the emails between the security team and affected customers for 30 days.
- B. Retain any communications related to the security breach until further notice.
- C. Retain any communications between security members during the breach response.
- D. Retain all emails from the company to affected customers for an indefinite period of time.

Answer: B

Explanation:

A legal hold (also known as a litigation hold) is a notification sent from an organization's legal team to employees instructing them not to delete electronically stored information (ESI) or discard paper documents that may be relevant to a new or imminent legal case. A legal hold is intended to preserve evidence and prevent spoliation, which is the intentional or negligent destruction of evidence that could harm a party's case. A legal hold can be triggered by various events, such as a lawsuit, a regulatory investigation, or a subpoena¹². In this scenario, the company's attorneys have requested that the security team initiate a legal hold in response to the lawsuit filed by the customers after the company was compromised. This means that the security team will most likely be required to retain any communications related to the security breach until further notice. This could include emails, instant messages, reports, logs, memos, or any other documents that could be relevant to the lawsuit. The security team should also inform the relevant custodians (the employees who have access to or control over the ESI) of their preservation obligations and monitor their compliance. The security team should also document the legal hold process and its scope, as well as take steps to protect the ESI from alteration, deletion, or loss³⁴.

References:

1: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 6: Risk Management, page 303 2: CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 6: Risk Management, page 305 3: Legal Hold (Litigation Hold) - The Basics of E-Discovery - Exterro 5 4: The Legal Implications and Consequences of a Data Breach 6

NEW QUESTION 79

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 82

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 85

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

- A. SCAP
- B. Net Flow
- C. Antivirus
- D. DLP

Answer: D

Explanation:

DLP stands for Data Loss Prevention, which is a tool that can assist with detecting and preventing the unauthorized transmission or leakage of sensitive data, such as a customer's PII (Personally Identifiable Information). DLP can monitor, filter, and block data in motion (such as emails), data at rest (such as files), and data in use (such as applications). DLP can also alert the sender, the recipient, or the administrator of the data breach, and apply remediation actions, such as encryption, quarantine, or deletion. DLP can help an organization comply with data protection regulations, such as GDPR, HIPAA, or PCI DSS, and protect its reputation and assets. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 2, page 78. CompTIA Security+ SY0-701 Exam Objectives, Domain 2.5, page 11.

NEW QUESTION 86

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 87

A systems administrator is looking for a low-cost application-hosting solution that is cloud- based. Which of the following meets these requirements?

- A. Serverless framework
- B. Type 1 hypervisor
- C. SD-WAN

D. SDN

Answer: A

Explanation:

A serverless framework is a cloud-based application-hosting solution that meets the requirements of low-cost and cloud-based. A serverless framework is a type of cloud computing service that allows developers to run applications without managing or provisioning any servers. The cloud provider handles the server-side infrastructure, such as scaling, load balancing, security, and maintenance, and charges the developer only for the resources consumed by the application. A serverless framework enables developers to focus on the application logic and functionality, and reduces the operational costs and complexity of hosting applications. Some examples of serverless frameworks are AWS Lambda, Azure Functions, and Google Cloud Functions.

A type 1 hypervisor, SD-WAN, and SDN are not cloud-based application-hosting solutions that meet the requirements of low-cost and cloud-based. A type 1 hypervisor is a software layer that runs directly on the hardware and creates multiple virtual machines that can run different operating systems and applications. A type 1 hypervisor is not a cloud-based service, but a virtualization technology that can be used to create private or hybrid clouds. A type 1 hypervisor also requires the developer to manage and provision the servers and the virtual machines, which can increase the operational costs and complexity of hosting applications. Some examples of type 1 hypervisors are VMware ESXi, Microsoft Hyper-V, and Citrix XenServer.

SD-WAN (Software-Defined Wide Area Network) is a network architecture that uses software to dynamically route traffic across multiple WAN connections, such as broadband, LTE, or MPLS. SD-WAN is not a cloud-based service, but a network optimization technology that can improve the performance, reliability, and security of WAN connections. SD-WAN can be used to connect remote sites or users to cloud-based applications, but it does not host the applications itself. Some examples of SD-WAN vendors are Cisco, VMware, and Fortinet.

SDN (Software-Defined Networking) is a network architecture that decouples the control plane from the data plane, and uses a centralized controller to programmatically manage and configure the network devices and traffic flows. SDN is not a cloud-based service, but a network automation technology that can enhance the scalability, flexibility, and efficiency of the network. SDN can be used to create virtual networks or network functions that can support cloud-based applications, but it does not host the applications itself. Some examples of SDN vendors are OpenFlow, OpenDaylight, and OpenStack.

References = CompTIA Security+ SY0-701 Certification Study Guide, page 264-265; Professor Messer's CompTIA SY0-701 Security+ Training Course, video 3.1 - Cloud and Virtualization, 7:40 - 10:00; [Serverless Framework]; [Type 1 Hypervisor]; [SD-WAN]; [SDN].

NEW QUESTION 92

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 94

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 99

Which of the following is used to validate a certificate when it is presented to a user?

- A. OCSP
- B. CSR
- C. CA
- D. CRC

Answer: A

Explanation:

OCSP stands for Online Certificate Status Protocol. It is a protocol that allows applications to check the revocation status of a certificate in real-time. It works by sending a query to an OCSP responder, which is a server that maintains a database of revoked certificates. The OCSP responder returns a response that indicates whether the certificate is valid, revoked, or unknown. OCSP is faster and more efficient than downloading and parsing Certificate Revocation Lists (CRLs), which are large files that contain the serial numbers of all revoked certificates issued by a Certificate Authority (CA). References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 337 1

NEW QUESTION 102

A security practitioner completes a vulnerability assessment on a company's network and finds several vulnerabilities, which the operations team remediates. Which of the following should be done next?

- A. Conduct an audit.
- B. Initiate a penetration test.
- C. Rescan the network.
- D. Submit a report.

Answer: C

Explanation:

After completing a vulnerability assessment and remediating the identified vulnerabilities, the next step is to rescan the network to verify that the vulnerabilities have been successfully fixed and no new vulnerabilities have been introduced. A vulnerability assessment is a process of identifying and evaluating the weaknesses and exposures in a network, system, or application that could be exploited by attackers. A vulnerability assessment typically involves using automated tools, such as scanners, to scan the network and generate a report of the findings. The report may include information such as the severity, impact, and remediation of the vulnerabilities. The operations team is responsible for applying the appropriate patches, updates, or configurations to address the vulnerabilities and reduce the risk to the network. A rescan is necessary to confirm that the remediation actions have been effective and that the network is secure.

Conducting an audit, initiating a penetration test, or submitting a report are not the next steps after completing a vulnerability assessment and remediating the vulnerabilities. An audit is a process of reviewing and verifying the compliance of the network with the established policies, standards, and regulations. An audit may be performed by internal or external auditors, and it may use the results of the vulnerability assessment as part of the evidence. However, an audit is not a mandatory step after a vulnerability assessment, and it does not validate the effectiveness of the remediation actions.

A penetration test is a process of simulating a real-world attack on the network to test the security defenses and identify any gaps or weaknesses. A penetration test may use the results of the vulnerability assessment as a starting point, but it goes beyond scanning and involves exploiting the vulnerabilities to gain access or cause damage. A penetration test may be performed after a vulnerability assessment, but only with the proper authorization, scope, and rules of engagement. A penetration test is not a substitute for a rescan, as it does not verify that the vulnerabilities have been fixed.

Submitting a report is a step that is done after the vulnerability assessment, but before the remediation. The report is a document that summarizes the findings and recommendations of the vulnerability assessment, and it is used to communicate the results to the stakeholders and the operations team. The report may also include a follow-up plan and a timeline for the remediation actions. However, submitting a report is not the final step after the remediation, as it does not confirm that the network is secure.

References = CompTIA Security+ SY0-701 Certification Study Guide, page 372- 375; Professor Messer's CompTIA SY0-701 Security+ Training Course, video 4.1 - Vulnerability Scanning, 0:00 - 8:00.

NEW QUESTION 103

A company's marketing department collects, modifies, and stores sensitive customer data. The infrastructure team is responsible for securing the data while in transit and at rest. Which of the following data roles describes the customer?

- A. Processor
- B. Custodian
- C. Subject
- D. Owner

Answer: C

Explanation:

According to the CompTIA Security+ SY0-701 Certification Study Guide, data subjects are the individuals whose personal data is collected, processed, or stored by an organization. Data subjects have certain rights and expectations regarding how their data is handled, such as the right to access, correct, delete, or restrict their data. Data subjects are different from data owners, who are the individuals or entities that have the authority and responsibility to determine how data is classified, protected, and used. Data subjects are also different from data processors, who are the individuals or entities that perform operations on data on behalf of the data owner, such as collecting, modifying, storing, or transmitting data. Data subjects are also different from data custodians, who are the individuals or entities that implement the security controls and procedures specified by the data owner to protect data while in transit and at rest.

ReferencesCompTIA Security+ SY0-701 Certification Study Guide, Chapter 2: Data Security, page 511

NEW QUESTION 107

An organization's internet-facing website was compromised when an attacker exploited a buffer overflow. Which of the following should the organization deploy to best protect against similar attacks in the future?

- A. NGFW
- B. WAF
- C. TLS
- D. SD-WAN

Answer: B

Explanation:

A buffer overflow is a type of software vulnerability that occurs when an application writes more data to a memory buffer than it can hold, causing the excess data to overwrite adjacent memory locations. This can lead to unexpected behavior, such as crashes, errors, or code execution. A buffer overflow can be exploited by an attacker to inject malicious code or commands into the application, which can compromise the security and functionality of the system. An organization's internet-facing website was compromised when an attacker exploited a buffer overflow. To best protect against similar attacks in the future, the organization should deploy a web application firewall (WAF). A WAF is a type of firewall that monitors and filters the traffic between a web application and the internet. A WAF can detect and block common web attacks, such as buffer overflows, SQL injections, cross-site scripting (XSS), and more. A WAF can also enforce security policies and rules, such as input validation, output encoding, and encryption. A WAF can provide a layer of protection for the web application, preventing attackers from exploiting its vulnerabilities and compromising its data. References = Buffer Overflows – CompTIA Security+ SY0-701

– 2.3, Web Application Firewalls – CompTIA Security+ SY0-701 – 2.4, [CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition]

NEW QUESTION 112

During the onboarding process, an employee needs to create a password for an intranet account. The password must include ten characters, numbers, and letters, and two special characters. Once the password is created, the company will grant the employee access to other company-owned websites based on the intranet profile. Which of the following access management concepts is the company most likely using to safeguard intranet accounts and grant access to multiple sites based on a user's intranet account? (Select two).

- A. Federation
- B. Identity proofing
- C. Password complexity
- D. Default password changes
- E. Password manager
- F. Open authentication

Answer: AC

Explanation:

Federation is an access management concept that allows users to authenticate once and access multiple resources or services across different domains or organizations. Federation relies on a trusted third party that stores the user's credentials and provides them to the requested resources or services without exposing them. Password complexity is a security measure that requires users to create passwords that meet certain criteria, such as length, character types, and uniqueness. Password complexity can help prevent brute-force attacks, password guessing, and credential stuffing by making passwords harder to crack or guess. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 308-309 and 312-313 1

NEW QUESTION 117

Which of the following is the most likely to be included as an element of communication in a security awareness program?

- A. Reporting phishing attempts or other suspicious activities
- B. Detecting insider threats using anomalous behavior recognition
- C. Verifying information when modifying wire transfer data
- D. Performing social engineering as part of third-party penetration testing

Answer: A

Explanation:

A security awareness program is a set of activities and initiatives that aim to educate and inform the users and employees of an organization about the security policies, procedures, and best practices. A security awareness program can help to reduce the human factor in security risks, such as social engineering, phishing, malware, data breaches, and insider threats. A security awareness program should include various elements of communication, such as newsletters, posters, videos, webinars, quizzes, games, simulations, and feedback mechanisms, to deliver the security messages and reinforce the security culture. One of the most likely elements of communication to be included in a security awareness program is reporting phishing attempts or other suspicious activities, as this can help to raise the awareness of the users and employees about the common types of cyberattacks and how to respond to them. Reporting phishing attempts or other suspicious activities can also help to alert the security team and enable them to take appropriate actions to prevent or mitigate the impact of the attacks. Therefore, this is the best answer among the given options.

The other options are not as likely to be included as elements of communication in a security awareness program, because they are either technical or operational tasks that are not directly related to the security awareness of the users and employees. Detecting insider threats using anomalous behavior recognition is a technical task that involves using security tools or systems to monitor and analyze the activities and behaviors of the users and employees and identify any deviations or anomalies that may indicate malicious or unauthorized actions. This task is usually performed by the security team or the security operations center, and it does not require the communication or participation of the users and employees. Verifying information when modifying wire transfer data is an operational task that involves using verification methods, such as phone calls, emails, or digital signatures, to confirm the authenticity and accuracy of the information related to wire transfers, such as the account number, the amount, or the recipient. This task is usually performed by the financial or accounting department, and it does not involve the security awareness of the users and employees. Performing social engineering as part of third-party penetration testing is a technical task that involves using deception or manipulation techniques, such as phishing, vishing, or impersonation, to test the security posture and the vulnerability of the users and employees to social engineering attacks. This task is usually performed by external security professionals or consultants, and it does not require the communication or consent of the users and employees. Therefore, these options are not the best answer for this question. References = Security Awareness and Training –

CompTIA Security+ SY0-701: 5.2, video at 0:00; CompTIA Security+ SY0-701 Certification Study Guide, page 263.

NEW QUESTION 121

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 125

Which of the following is the best way to consistently determine on a daily basis whether security settings on servers have been modified?

- A. Automation
- B. Compliance checklist
- C. Attestation
- D. Manual audit

Answer: A

Explanation:

Automation is the best way to consistently determine on a daily basis whether security settings on servers have been modified. Automation is the process of using software, hardware, or other tools to perform tasks that would otherwise require human intervention or manual effort. Automation can help to improve the

efficiency, accuracy, and consistency of security operations, as well as reduce human errors and costs. Automation can be used to monitor, audit, and enforce security settings on servers, such as firewall rules, encryption keys, access controls, patch levels, and configuration files. Automation can also alert security personnel of any changes or anomalies that may indicate a security breach or compromise¹².

The other options are not the best ways to consistently determine on a daily basis whether security settings on servers have been modified:

? Compliance checklist: This is a document that lists the security requirements, standards, or best practices that an organization must follow or adhere to. A compliance checklist can help to ensure that the security settings on servers are aligned with the organizational policies and regulations, but it does not automatically detect or report any changes or modifications that may occur on a daily basis³.

? Attestation: This is a process of verifying or confirming the validity or accuracy of a statement, claim, or fact. Attestation can be used to provide assurance or evidence that the security settings on servers are correct and authorized, but it does not continuously monitor or audit any changes or modifications that may occur on a daily basis⁴.

? Manual audit: This is a process of examining or reviewing the security settings on servers by human inspectors or auditors. A manual audit can help to identify and correct any security issues or discrepancies on servers, but it is time-consuming, labor-intensive, and prone to human errors. A manual audit may not be feasible or practical to perform on a daily basis.

References = 1: CompTIA Security+ SY0-701 Certification Study Guide, page 1022: Automation and Scripting – CompTIA Security+ SY0-701 – 5.1, video by Professor Messer³: CompTIA Security+ SY0-701 Certification Study Guide, page 974: CompTIA Security+ SY0-701 Certification Study Guide, page 98. : CompTIA Security+ SY0-701 Certification Study Guide, page 99.

NEW QUESTION 126

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 131

A company hired a consultant to perform an offensive security assessment covering penetration testing and social engineering. Which of the following teams will conduct this assessment activity?

- A. White
- B. Purple
- C. Blue
- D. Red

Answer: D

Explanation:

A red team is a group of security professionals who perform offensive security assessments covering penetration testing and social engineering. A red team simulates real-world attacks and exploits the vulnerabilities of a target organization, system, or network. A red team aims to test the effectiveness of the security controls, policies, and procedures of the target, as well as the awareness and response of the staff and the blue team. A red team can be hired as an external consultant or formed internally within the organization. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 1, page 18. CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 1.8, page 4. Security Teams – SY0-601 CompTIA Security+ : 1.8

NEW QUESTION 135

Which of the following is the most common data loss path for an air-gapped network?

- A. Bastion host
- B. Unsecured Bluetooth
- C. Unpatched OS
- D. Removable devices

Answer: D

Explanation:

An air-gapped network is a network that is physically isolated from other networks, such as the internet, to prevent unauthorized access and data leakage. However, an air-gapped network can still be compromised by removable devices, such as USB drives, CDs, DVDs, or external hard drives, that are used to transfer data between the air-gapped network and other networks. Removable devices can carry malware, spyware, or other malicious code that can infect the air-gapped network or exfiltrate data from it. Therefore, removable devices are the most common data loss path for an air-gapped network. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 9: Network Security, page 449 1

NEW QUESTION 139

An IT manager informs the entire help desk staff that only the IT manager and the help desk lead will have access to the administrator console of the help desk software. Which of the following security techniques is the IT manager setting up?

- A. Hardening
- B. Employee monitoring
- C. Configuration enforcement
- D. Least privilege

Answer: D

Explanation:

The principle of least privilege is a security concept that limits access to resources to the minimum level needed for a user, a program, or a device to perform a legitimate function. It is a cybersecurity best practice that protects high-value data and assets from compromise or insider threat. Least privilege can be applied to different abstraction layers of a computing environment, such as processes, systems, or connected devices. However, it is rarely implemented in practice. In this scenario, the IT manager is setting up the principle of least privilege by restricting access to the administrator console of the help desk software to only two authorized users: the IT manager and the help desk lead. This way, the IT manager can prevent unauthorized or accidental changes to the software configuration, data, or functionality by other help desk staff. The other help desk staff will only have access to the normal user interface of the software, which is sufficient for them to perform their job functions.

The other options are not correct. Hardening is the process of securing a system by reducing its surface of vulnerability, such as by removing unnecessary software, changing default passwords, or disabling unnecessary services. Employee monitoring is the surveillance of workers' activity, such as by tracking web browsing, application use, keystrokes, or screenshots. Configuration enforcement is the process of ensuring that a system adheres to a predefined set of security settings, such as by applying a patch, a policy, or a template.

References = https://en.wikipedia.org/wiki/Principle_of_least_privilege https://en.wikipedia.org/wiki/Principle_of_least_privilege

NEW QUESTION 144

Several employees received a fraudulent text message from someone claiming to be the Chief Executive Officer (CEO). The message stated:

"I'm in an airport right now with no access to email. I need you to buy gift cards for employee recognition awards. Please send the gift cards to following email address."

Which of the following are the best responses to this situation? (Choose two).

- A. Cancel current employee recognition gift cards.
- B. Add a smishing exercise to the annual company training.
- C. Issue a general email warning to the company.
- D. Have the CEO change phone numbers.
- E. Conduct a forensic investigation on the CEO's phone.
- F. Implement mobile device management.

Answer: BC

Explanation:

This situation is an example of smishing, which is a type of phishing that uses text messages (SMS) to entice individuals into providing personal or sensitive information to cybercriminals. The best responses to this situation are to add a smishing exercise to the annual company training and to issue a general email warning to the company. A smishing exercise can help raise awareness and educate employees on how to recognize and avoid smishing attacks. An email warning can alert employees to the fraudulent text message and remind them to verify the identity and legitimacy of any requests for information or money.

References = What Is Phishing | Cybersecurity | CompTIA, Phishing – SY0-601 CompTIA Security+ : 1.1 - Professor Messer IT Certification Training Courses

NEW QUESTION 149

Which of the following threat actors is the most likely to use large financial resources to attack critical systems located in other countries?

- A. Insider
- B. Unskilled attacker
- C. Nation-state
- D. Hacktivist

Answer: C

Explanation:

A nation-state is a threat actor that is sponsored by a government or a political entity to conduct cyberattacks against other countries or organizations. Nation-states have large financial resources, advanced technical skills, and strategic objectives that may target critical systems such as military, energy, or infrastructure. Nation-states are often motivated by espionage, sabotage, or warfare¹². References = 1: CompTIA Security+ SY0-701 Certification Study Guide, page 542:

Threat Actors – CompTIA

Security+ SY0-701 – 2.1, video by Professor Messer.

NEW QUESTION 150

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 154

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 I 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 159

An administrator finds that all user workstations and servers are displaying a message that is associated with files containing an extension of .ryk. Which of the following types of infections is present on the systems?

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

Answer: D

Explanation:

Ransomware is a type of malware that encrypts the victim's files and demands a ransom for the decryption key. The ransomware usually displays a message on the infected system with instructions on how to pay the ransom and recover the files. The .ryk extension is associated with a ransomware variant called Ryuk, which targets large organizations and demands high ransoms¹.

References: CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 1, page 17.

NEW QUESTION 163

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 164

A user is attempting to patch a critical system, but the patch fails to transfer. Which of the following access controls is most likely inhibiting the transfer?

- A. Attribute-based
- B. Time of day
- C. Role-based
- D. Least privilege

Answer: D

Explanation:

The least privilege principle states that users and processes should only have the minimum level of access required to perform their tasks. This helps to prevent unauthorized or unnecessary actions that could compromise security. In this case, the patch transfer might be failing because the user or process does not have the appropriate permissions to access the critical system or the network resources needed for the transfer. Applying the least privilege principle can help to avoid this issue by granting the user or process the necessary access rights for the patching activity. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 931

NEW QUESTION 169

After a recent ransomware attack on a company's system, an administrator reviewed the log files. Which of the following control types did the administrator use?

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

Answer: B

Explanation:

Detective controls are security measures that are designed to identify and monitor any malicious activity or anomalies on a system or network. They can help to discover the source, scope, and impact of an attack, and provide evidence for further analysis or investigation. Detective controls include log files, security audits, intrusion detection systems, network monitoring tools, and antivirus software. In this case, the administrator used log files as a detective control to review the ransomware attack on the company's system. Log files are records of events and activities that occur on a system or network, such as user actions, system errors, network traffic, and security alerts. They can provide valuable information for troubleshooting, auditing, and forensics.

References:

? Security+ (Plus) Certification | CompTIA IT Certifications, under "About the exam", bullet point 3: "Operate with an awareness of applicable regulations and policies, including principles of governance, risk, and compliance."

? CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 1, page 14: "Detective controls are designed to identify and monitor any malicious activity or anomalies on a system or network."

? Control Types – CompTIA Security+ SY0-401: 2.1 - Professor Messer IT ..., under "Detective Controls": "Detective controls are security measures that are designed to identify and monitor any malicious activity or anomalies on a system or network."

NEW QUESTION 171

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 175

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 178

A company is developing a critical system for the government and storing project information on a fileshare. Which of the following describes how this data will most likely be classified? (Select two).

- A. Private
- B. Confidential
- C. Public
- D. Operational
- E. Urgent
- F. Restricted

Answer: BF

Explanation:

Data classification is the process of assigning labels to data based on its sensitivity and business impact. Different organizations and sectors may have different data classification schemes, but a common one is the following¹:

? Public: Data that can be freely disclosed to anyone without any harm or risk.

? Private: Data that is intended for internal use only and may cause some harm or risk if disclosed.

? Confidential: Data that is intended for authorized use only and may cause significant harm or risk if disclosed.

? Restricted: Data that is intended for very limited use only and may cause severe harm or risk if disclosed.

In this scenario, the company is developing a critical system for the government and storing project information on a fileshare. This data is likely to be classified as confidential and restricted, because it is not meant for public or private use, and it may cause serious damage to national security or public safety if disclosed. The government may also have specific requirements or regulations for handling such data, such as encryption, access control, and auditing2. References: 1: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 16-17 2: Data Classification Practices: Final Project Description Released

NEW QUESTION 183

A systems administrator set up a perimeter firewall but continues to notice suspicious connections between internal endpoints. Which of the following should be set up in order to mitigate the threat posed by the suspicious activity?

- A. Host-based firewall
- B. Web application firewall
- C. Access control list
- D. Application allow list

Answer: A

Explanation:

A host-based firewall is a software application that runs on an individual endpoint and filters the incoming and outgoing network traffic based on a set of rules. A host-based firewall can help to mitigate the threat posed by suspicious connections between internal endpoints by blocking or allowing the traffic based on the source, destination, port, protocol, or application. A host-based firewall is different from a web application firewall, which is a type of firewall that protects web applications from common web-based attacks, such as SQL injection, cross-site scripting, and session hijacking. A host-based firewall is also different from an access control list, which is a list of rules that control the access to network resources, such as files, folders, printers, or routers. A host-based firewall is also different from an application allow list, which is a list of applications that are authorized to run on an endpoint, preventing unauthorized or malicious applications from executing. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 254

NEW QUESTION 188

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

SY0-701 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](#)