SY0-701 Q&As

CompTIA Security+

Pass CompTIA SY0-701 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/sy0-701.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

QUESTION 1

An organization maintains intellectual property that it wants to protect. Which of the following concepts would be most beneficial to add to the company\\'s security awareness training program?

A. Insider threat detection

B. Simulated threats

C. Phishing awareness

D. Business continuity planning

Correct Answer: A

For an organization that wants to protect its intellectual property, adding insider threat detection to the security awareness training program would be most beneficial. Insider threats can be particularly dangerous because they come from trusted individuals within the organization who have legitimate access to sensitive information. Insider threat detection: Focuses on identifying and mitigating threats from within the organization, including employees, contractors, or business partners who might misuse their access. Simulated threats: Often used for testing security measures and training, but not specifically focused on protecting intellectual property. Phishing awareness: Important for overall security but more focused on preventing external attacks rather than internal threats. Business continuity planning: Ensures the organization can continue operations during and after a disruption but does not directly address protecting intellectual property from insider threats. Reference: CompTIA Security+ SY0-701 Exam Objectives, Domain 5.6 - Implement security awareness practices (Insider threat detection).

QUESTION 2

Which of the following is the most likely outcome if a large bank fails an internal PCI DSS compliance assessment?

A. Fines

B. Audit findings

C. Sanctions

D. Reputation damage

Correct Answer: B

QUESTION 3

A data administrator is configuring authentication for a SaaS application and would like to reduce the number of credentials employees need to maintain. The company prefers to use domain credentials to access new SaaS applications. Which of the following methods would allow this functionality?

A. SSO

B. LEAP

C. MFA

D. PEAP

Correct Answer: A

SSO stands for single sign-on, which is a method of authentication that allows users to access multiple applications or services with one set of credentials. SSO reduces the number of credentials employees need to maintain and simplifies the login process. SSO can also improve security by reducing the risk of password reuse, phishing, and credential theft. SSO can be implemented using various protocols, such as SAML, OAuth, OpenID Connect, and Kerberos, that enable the exchange of authentication information between different domains or systems. SSO is commonly used for accessing SaaS applications, such as Office 365, Google Workspace, Salesforce, and others, using domain credentials123. B. LEAP stands for Lightweight Extensible Authentication Protocol, which is a Cisco proprietary protocol that provides authentication for wireless networks. LEAP is not related to SaaS applications or domain credentials4. C. MFA stands for multi-factor authentication, which is a method of authentication that requires users to provide two or more pieces of evidence to prove their identity. MFA can enhance security by adding an extra layer of protection beyond passwords, such as tokens, biometrics, or codes. MFA is not related to SaaS applications or domain credentials, but it can be used in conjunction with SSO. D. PEAP stands for Protected Extensible Authentication Protocol, which is a protocol that provides secure authentication for wireless networks. PEAP uses TLS to create an encrypted tunnel between the client and the server, and then uses another authentication method, such as MS-CHAPv2 or EAP-GTC, to verify the user\\'s identity. PEAP is not related to SaaS applications or domain credentials.

References: 1: Security+ (SY0-701) Certification Study Guide | CompTIA IT Certifications 2: What is Single Sign-On (SSO)? - Definition from WhatIs.com 3: Single sign-on - Wikipedia 4: Lightweight Extensible Authentication Protocol -Wikipedia : What is Multi-Factor Authentication (MFA)? - Definition from WhatIs.com : Protected Extensible Authentication Protocol - Wikipedia

QUESTION 4

Which of the following is used to protect a computer from viruses, malware, and Trojans being installed and moving laterally across the network?

A. IDS

B. ACL

C. EDR

D. NAC

Correct Answer: C

Endpoint detection and response (EDR) is a technology that monitors and analyzes the activity and behavior of endpoints, such as computers, laptops, mobile devices, and servers. EDR can help to detect and prevent malicious software, such as viruses, malware, and Trojans, from infecting the endpoints and spreading across the network. EDR can also provide visibility and response capabilities to contain and remediate threats. EDR is different from IDS, which is a network-based technology that monitors and alerts on network traffic anomalies. EDR is also different from ACL, which is a list of rules that control the access to network resources. EDR is also different from NAC, which is a technology that enforces policies on the network access of devices based on their identity and compliance status.

References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 2561

QUESTION 5

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

Correct Answer: C

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.

QUESTION 6

A business needs a recovery site but does not require immediate failover. The business also wants to reduce the workload required to recover from an outage. Which of the following recovery sites is the best option?

A. Hot

B. Cold

C. Warm

D. Geographically dispersed

Correct Answer: C

A warm site is the best option for a business that does not require immediate failover but wants to reduce the workload required for recovery. A warm site has some pre-installed equipment and data, allowing for quicker recovery than a cold site, but it still requires some setup before becoming fully operational. Hot sites provide immediate failover but are more expensive and require constant maintenance. Cold sites require significant time and effort to get up and running after an outage. Geographically dispersed sites refer to a specific location strategy rather than the readiness of the recovery site.

QUESTION 7

The application development teams have been asked to answer the following questions:

1.

Does this application receive patches from an external source?

2.

Does this application contain open-source code?

3.

Is this application accessible by external users?

4.

Does this application meet the corporate password standard?

Which of the following are these questions part of?

A. Risk control self-assessment

B. Risk management strategy

C. Risk acceptance

D. Risk matrix

Correct Answer: A

The questions listed are part of a Risk Control Self-Assessment (RCSA), which is a process where teams evaluate the risks associated with their operations and assess the effectiveness of existing controls. The questions focus on aspects

such as patch management, the use of open-source code, external access, and compliance with corporate standards, all of which are critical for identifying and mitigating risks.

References:

CompTIA Security+ SY0-701 Course Content: The course discusses various risk management processes, including self-assessments that help in identifying and managing risks within the organization.

QUESTION 8

A security engineer is working to address the growing risks that shadow IT services are introducing to the organization. The organization has taken a cloud-first approach end does not have an on-premises IT infrastructure. Which of the following would best secure the organization?

A. Upgrading to a next-generation firewall

B. Deploying an appropriate in-line CASB solution

C. Conducting user training on software policies

D. Configuring double key encryption in SaaS platforms

Correct Answer: B

A Cloud Access Security Broker (CASB) solution is the most suitable option for securing an organization that has adopted a cloud-first strategy and does not have an on-premises IT infrastructure. CASBs provide visibility and control over

shadow IT services, enforce security policies, and protect data across cloud services.

References: CompTIA Security+ SY0-701 study materials, particularly in the domain of cloud security and managing risks associated with shadow IT.

QUESTION 9

Two organizations plan to collaborate on the evaluation of new SIEM solutions for their respective companies. A combined effort from both organizations\\' SOC teams would speed up the effort. Which of the following can be written to document this agreement?

A. MOU

B. ISA

C. SLA

D. NDA

Correct Answer: A

A document that regulates security-relevant aspects of an intended connection between an agency and an external system. It regulates the security interface between any two systems operating under two different distinct authorities. It includes a variety of descriptive, technical, procedural, and planning information. It is usually preceded by a formal MOA/MOU that defines high- level roles and responsibilities in management of a cross-domain connection.

QUESTION 10

An employee fell for a phishing scam, which allowed an attacker to gain access to a company PC. The attacker scraped the PC\\'s memory to find other credentials. Without cracking these credentials, the attacker used them to move laterally through the corporate network. Which of the following describes this type of attack?

A. Privilege escalation

B. Buffer overflow

C. SQL injection

D. Pass-the-hash

Correct Answer: D

The scenario describes an attacker who obtained credentials from a compromised system\\'s memory and used them without cracking to move laterally within the network. This technique is known as a "pass-the-hash" attack, where the

attacker captures hashed credentials (e.g., NTLM hashes) and uses them to authenticate and gain access to other systems without needing to know the plaintext password. This is a common attack method in environments where weak

security practices or outdated protocols are in use.

References:

CompTIA Security+ SY0-701 Course Content: The course discusses credential- based attacks like pass-the-hash, emphasizing their impact and the importance of protecting credential stores.

QUESTION 11

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

Correct Answer: B

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, Question2.

QUESTION 12

Which of the following is a common source of unintentional corporate credential leakage in cloud environments?

A. Code repositories

B. Dark web

C. Threat feeds

D. State actors

E. Vulnerability databases

Correct Answer: A

Code repositories are a common source of unintentional corporate credential leakage, especially in cloud environments. Developers may accidentally commit and push sensitive information, such as API keys, passwords, and other

credentials, to public or poorly secured repositories. These credentials can then be accessed by unauthorized users, leading to security breaches. Ensuring that repositories are properly secured and that sensitive data is never committed is

critical for protecting against this type of leakage.

References:

CompTIA Security+ SY0-701 Course Content: Domain 03 Security Architecture. CompTIA Security+ SY0-601 Study Guide: Chapter on Threats and Vulnerability Management.

QUESTION 13

An organization plans to take online orders via a new website. Three web servers are available for this website. However, the organization does not want to reveal the network addresses or quantity of the individual servers to the general public. Which of the following would best fulfill these requirements?

A. IPSec

B. Explicit proxy

C. Port security

D. Virtual IP

Correct Answer: D

QUESTION 14

Which of the following risks can be mitigated by HTTP headers?

A. SQLi

B. XSS

C. DoS

D. SSL

Correct Answer: B

HTTP headers can be used to mitigate risks associated with Cross-Site Scripting (XSS). Security-related HTTP headers such as Content Security Policy (CSP) and X-XSS-Protection can be configured to prevent the execution of malicious

scripts in the context of a web page.

XSS (Cross-Site Scripting): A vulnerability that allows attackers to inject malicious scripts into web pages viewed by other users. HTTP headers like CSP help prevent XSS attacks by specifying which dynamic resources are allowed to load.

SQLi (SQL Injection): Typically mitigated by using parameterized queries and input validation, not HTTP headers.

DoS (Denial of Service): Mitigated by network and application-level defenses rather than HTTP headers.

SSL (Secure Sockets Layer): Refers to securing communications and is not directly mitigated by HTTP headers; rather, it\\'s implemented using SSL/TLS protocols.

Reference: CompTIA Security+ SY0-701 Exam Objectives, Domain 3.3 - Protect data (HTTP headers for securing web applications).

QUESTION 15

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

Correct Answer: C

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