SY0-701 Q&As

CompTIA Security+ 2024

Pass CompTIA SY0-701 Exam with 100% Guarantee

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

https://www.pass4itsure.com/sy0-701.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Several users have opened tickets with the help desk. The help desk has reassigned the tickets to a securty analyst for further review The security analyst reviews the following metrics:

Hostname	Normal CPU utilization %	Current CPU utilization %	Normal network connections	Current network connections
Accounting-PC	22%	48%	12	66
HR-PC	35%	55%	15	57
IT-PC	78%	98%	25	92
Sales-PC	28%	50%	20	56
Manager-PC	21%	44%	18	49

Which of the following is MOST likely the result of the security analyst\\'s review?

A. The ISP is dropping outbound connections

B. The user of the Sales-PC fell for a phishing attack

C. Corporate PCs have been turned into a botnet

D. An on-path attack is taking place between PCs and the router

Correct Answer: C

The metrics show a significant increase in both CPU utilization and network connections for all the listed PCs compared to their normal values. This could indicate that the machines are being used for unauthorized activities. The current CPU utilization of all the PCs is significantly higher than the normal CPU utilization. This indicates that the PCs are running a lot of processes, which is a common symptom of a botnet infection. The number of current network connections for all the PCs is also significantly higher than the normal number of network connections. This is another common symptom of a botnet infection. A botnet is a network of computers that have been infected with malware and controlled by a remote attacker. The attacker can use the botnet to carry out a variety of malicious activities, such as sending spam, launching DDoS attacks, or stealing data.

QUESTION 2

An administrator needs to protect user passwords and has been advised to hash the passwords. Which of the following BEST describes what the administrator is being advised to do?

A. Perform a mathematical operation on the passwords that will convert them into umgue stnngs

B. Add extra data to the passwords so their length is increased, making them harder to brute force

C. Store all passwords in the system in a rainbow table that has a centralized location

D. Enforce the use of one-time passwords that are changed for every login session.

Correct Answer: A

Admin is being advised to hash. A is the definition of hashing

QUESTION 3

Which of the following roles, according to the shared responsibility model, is responsible for securing the company\\'s database in an IaaS model for a cloud environment?

A. Client

B. Third-party vendor

C. Cloud provider

D. DBA

Correct Answer: A

According to the shared responsibility model, the client and the cloud provider have different roles and responsibilities for securing the cloud environment, depending on the service model. In an IaaS (Infrastructure as a Service) model, the cloud provider is responsible for securing the physical infrastructure, such as the servers, storage, and network devices, while the client is responsible for securing the operating systems, applications, and data that run on the cloud infrastructure. Therefore, the client is responsible for securing the company\\'s database in an IaaS model for a cloud environment, as the database is an application that stores data. The client can use various security controls, such as encryption, access control, backup, and auditing, to protect the database from unauthorized access, modification, or loss. The third-party vendor and the DBA (Database Administrator) are not roles defined by the shared responsibility model, but they may be involved in the implementation or management of the database security.

References: CompTIA Security+ SY0-701 Certification Study Guide, page 263- 264; Professor Messer\\'s CompTIA SY0-701 Security+ Training Course, video 3.1 - Cloud and Virtualization, 5:00 - 7:40.

QUESTION 4

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 5

Which of the following is used to add extra complexity before using a one-way data transformation algorithm?

A. Key stretching

B. Data masking

C. Steganography

D. Salting

Correct Answer: D

Salting is the process of adding extra random data to a password or other data before applying a one-way data transformation algorithm, such as a hash function. Salting increases the complexity and randomness of the input data, making it

harder for attackers to guess or crack the original data using precomputed tables or brute force methods. Salting also helps prevent identical passwords from producing identical hash values, which could reveal the passwords to attackers who

have access to the hashed data. Salting is commonly used to protect passwords stored in databases or transmitted over networks.

References:

Passwords technical overview

Encryption, hashing, salting ?what\\'s the difference? Salt (cryptography)