PASS QUESTION

PRACTICE QUESTIONS

EXAM PREPARATION GUIDE

Learn Smarter

Practice Effectively

Achieve Your Goals

https://www.passquestion.com

One Year of Content Updates Included

Exam : **SY0-701**

Title : CompTIA Security+

Version : DEMO

1.A security analyst is creating base for the server team to follow when hardening new devices for deployment.
Which of the following beet describes what the analyst is creating?
A. Change management procedure
B. Information security policy
C. Cybersecurity framework
D. Secure configuration guide
Answer: D
Explanation:
The security analyst is creating a "secure configuration guide," which is a set of instructions or guidelines used to configure devices securely before deployment. This guide ensures that the devices are set up according to best practices to minimize vulnerabilities and protect against potential security threats.
References = CompTIA Security+ SY0-701 Course Content: Domain 03 Security Architecture. CompTIA Security+ SY0-601 Study Guide: Chapter on System Hardening and Secure Configuration.

2.A company's accounting department receives an urgent payment message from the company's bank domain with instructions to wire transfer funds. The sender requests that the transfer be completed as soon as possible.
Which of the following attacks is described?
A. Business email compromise
B. Vishing
C. Spear phishing
D. Impersonation
Answer: A
Explanation:
This is a classic example of Business Email Compromise (BEC), where attackers spoof or compromise trusted email accounts to trick employees into performing unauthorized financial transactions.
Vishing (B) is voice phishing, spear phishing (C) targets individuals with customized messages, and impersonation (D) is a general term for identity deception but BEC specifically describes financial fraud via email.
BEC is a major threat covered in the Threats domain of SY0-7016: Chapter 2†CompTIA Security+ Study Guide

3.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

4.A security engineer at a large company needs to enhance IAM to ensure that employees can only access corporate systems during their shifts.
Which of the following access controls should the security engineer implement?
A. Role-based
B. Time-of-day restrictions
C. Least privilege
D. Biometric authentication
Answer: B
Explanation:
Detailed Explanation
Time-of-day restrictions limit access to corporate systems based on predefined schedules.
This ensures employees can only access resources during their assigned work hours.
Reference: CompTIA Security+ SY0-701 Study Guide, Domain 3: Security Architecture, Section: "Access Control Models".

5.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
Answer: A
Explanation:
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.