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.geekcert.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

While considering the organization\\'s cloud-adoption strategy, the Chief Information Security Officer sets a goal to outsource patching of firmware, operating systems, and applications to the chosen cloud vendor. Which of the following best meets this goal?

A. Community cloud

B. PaaS

C. Containerization

D. Private cloud

E. SaaS

F. IaaS

Correct Answer: E

Software as a Service (SaaS) is the cloud model that best meets the goal of outsourcing the management, including patching, of firmware, operating systems, and applications to the cloud vendor. In a SaaS environment, the cloud provider is responsible for maintaining and updating the entire software stack, allowing the organization to focus on using the software rather than managing its infrastructure. References: CompTIA Security+ SY0-701 study materials, particularly the domains related to cloud security models.

QUESTION 2

Which of the following is a reason why a forensic specialist would create a plan to preserve data after an modem and prioritize the sequence for performing forensic analysis?

A. Order of volatility

B. Preservation of event logs

C. Chain of custody

D. Compliance with legal hold

Correct Answer: A

When conducting a forensic analysis after an incident, it\\'s essential to prioritize the data collection process based on the "order of volatility." This principle dictates that more volatile data (e.g., data in memory, network connections) should be

captured before less volatile data (e.g., disk drives, logs). The idea is to preserve the most transient and potentially valuable evidence first, as it is more likely to be lost or altered quickly.

References:

CompTIA Security+ SY0-701 Course Content: Domain 04 Security Operations. CompTIA Security+ SY0-601 Study Guide: Chapter on Digital Forensics.

QUESTION 3

Which of the following best describes why the SMS OTP authentication method is more risky to implement than the TOTP method?

A. The SMS OTP method requires an end user to have an active mobile telephone service and SIM card.

B. Generally. SMS OTP codes are valid for up to 15 minutes while the TOTP time frame is 30 to 60 seconds

C. The SMS OTP is more likely to be intercepted and lead to unauthorized disclosure of the code than the TOTP method.

D. The algorithm used to generate on SMS OTP code is weaker than the one used to generate a TOTP code

Correct Answer: C

The SMS OTP (One-Time Password) method is more vulnerable to interception compared to TOTP (Time-based One-Time Password) because SMS messages can be intercepted through various attack vectors like SIM swapping or SMS

phishing. TOTP, on the other hand, generates codes directly on the device and does not rely on a communication channel like SMS, making it less susceptible to interception.

References: CompTIA Security+ SY0-701 study materials, particularly in the domain of identity and access management.

QUESTION 4

A user would like to install software and features that are not available with a smartphone\\'s default software. Which of the following would allow the user to install unauthorized software and enable new features?

A. SOU

B. Cross-site scripting

C. Jailbreaking

D. Side loading

Correct Answer: C

Jailbreaking is the process of removing restrictions imposed by the manufacturer on a smartphone, allowing the user to install unauthorized software and features not available through official app stores. This action typically voids the warranty and can introduce security risks by bypassing built-in protections. SOU (Statement of Understanding) is not related to modifying devices. Cross-site scripting is a web-based attack technique, unrelated to smartphone software. Side loading refers to installing apps from unofficial sources but without necessarily removing built-in restrictions like jailbreaking does.

QUESTION 5

An employee receives a text message from an unknown number claiming to be the company\\'s Chief Executive Officer and asking the employee to purchase several gift cards. Which of the following types of attacks does this describe?

A. Vishing

B. Smishing

C. Pretexting

D. Phishing

Correct Answer: B

Smishing is a type of phishing attack that uses text messages or common messaging apps to trick victims into clicking on malicious links or providing personal information. The scenario in the question describes a smishing attack that uses pretexting, which is a form of social engineering that involves impersonating someone else to gain trust or access. The unknown number claims to be the company\\'s CEO and asks the employee to purchase gift cards, which is a common scam tactic. Vishing is a similar type of attack that uses phone calls or voicemails, while phishing is a broader term that covers any email- based attack. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 771; Smishing vs. Phishing: Understanding the Differences2