SY0-601 Q&As

CompTIA Security+

Pass CompTIA SY0-601 Exam with 100% Guarantee

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

https://www.passapply.com/sy0-601.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

The Chief Compliance Officer from a bank has approved a background check policy for all new hires Which of the following is the policy MOST likely protecting against?

A. Preventing any current employees\\' siblings from working at the bank to prevent nepotism

B. Hiring an employee who has been convicted of theft to adhere to industry compliance

C. Filtenng applicants who have added false information to resumes so they appear better qualified

D. Ensuring no new hires have worked at other banks that may be trying to steal customer information

Correct Answer: B

Source: https://www.pcicomplianceguide.org/what-does-the-pci-dss-say-about-employee-background-checks/

PCI DSS requires background checks for employees handling credit card holder data.

QUESTION 2

An auditor is performing an assessment of a security appliance with an embedded OS that was vulnerable during the last two assessments. Which of the following BEST explains the appliance\\'s vulnerable state?

A. The system was configured with weak default security settings.

B. The device uses weak encryption ciphers.

C. The vendor has not supplied a patch for the appliance.

D. The appliance requires administrative credentials for the assessment

Correct Answer: C

QUESTION 3

Which of the following authentication methods is considered to be the LEAST secure?

A. TOTP

B. SMS

C. HOTP

D. Token key

Correct Answer: B

SMS (Short Message Service) authentication involves sending a one-time passcode (OTP) to the user\\'s mobile phone via text message, which the user then enters to complete the authentication process. While it is more convenient than

some other methods, it is also less secure compared to the other options listed.

SMS authentication has several security weaknesses:

Phishing: Attackers can use social engineering to trick users into revealing their SMS OTP, compromising the authentication.

SIM swapping: Attackers can contact the user\\'s mobile service provider and convince them to transfer the phone number to a new SIM card, gaining access to the SMS OTP.

Intercepting SMS: In some cases, attackers with advanced capabilities can intercept SMS messages, allowing them to capture the OTP.

Due to these vulnerabilities, SMS authentication is considered less secure compared to other authentication methods like TOTP (Time-based One-Time Password) and HOTP (HMAC-based One-Time Password), which rely on algorithms

and do not involve transmitting the OTP via SMS.

QUESTION 4

Which of the following describes a maintenance metric that measures the average time required to troubleshoot and restore failed equipment?

A. RTO

B. MTBF

C. MTTR

D. RPO

Correct Answer: C

Mean time to repair (MTTR) is a measure of the maintainability of a repairable item, which tells the average time required to repair a specific item or component and return it to working status. It is a basic measure of the maintainability of equipment and parts. This includes the notification time, diagnosis and the time spent on actual repair as well as other activities required before the equipment can be used again. Mean time to repair is also known as mean repair time.

https://www.techopedia.com/definition/2719/mean-time-to-repair-mttr

QUESTION 5

A company recently experienced a major breach. An investigation concludes that customer credit card data was stolen and exfiltrated through a dedicated business partner connection to a vendor, who is not held to the same security contral standards.

Which of the following is the MOST likely source of the breach?

A. Side channel

B. Supply chain

C. Cryptographic downgrade

D. Malware

Correct Answer: B

Based on the information provided, the most likely source of the breach is the supply chain. The breach occurred when customer credit card data was stolen and exfiltrated through a dedicated business partner connection to a vendor. This indicates that the vendor, who is part of the supply chain, may not have the same level of security control standards as the company itself, making it a potential weak link in the overall security posture. Supply chain attacks involve targeting third-party vendors, suppliers, or business partners as a means to gain unauthorized access to the main target organization\\'s systems or data.