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.leads4pass.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

A user forwarded a suspicious email to the security team, Upon investigation, a malicious URL was discovered. Which of the following should be done FIRST to prevent other users from accessing the malicious URL?

A. Configure the web content filter for the web address.

B. Report the website to threat intelligence partners

C. Set me SIEM to alert for any activity to the web address.

D. Send out a corporate communication to warn all users Of the malicious email.

Correct Answer: A

Web content filtering is the practice of blocking access to web content that may be deemed offensive, inappropriate, or even dangerous. Better to just block out the URL since we already know its malicious now and notify later since you don\\'t know how many other people received the email.

QUESTION 2

A security architect is designing a remote access solution for a business partner. The business partner needs to access one Linux server at the company. The business partner wants to avoid managing a password for authentication and additional software installation. Which of the following should the architect recommend?

A. Soft token

B. Smart card

C. CSR

D. SSH key

Correct Answer: D

QUESTION 3

A company is adding a clause to its AUP that states employees are not allowed to modify the operating system on mobile devices. Which of the following vulnerabilities is the organization addressing?

A. Cross-site scripting

B. Buffer overflow

C. Jailbreaking

D. Side loading

Correct Answer: C

Jailbreaking is a process in which an individual gains unauthorized access to the operating system of a mobile device,

typically to remove software restrictions imposed by the manufacturer or carrier. This allows users to install unauthorized apps and make modifications to the device\\'s operating system, which can create security risks and expose the device to potential threats and vulnerabilities.

By adding a clause to the Acceptable Use Policy (AUP) that prohibits employees from modifying the operating system on mobile devices, the company aims to prevent the practice of jailbreaking, which helps mitigate potential security risks associated with unauthorized software modifications.

QUESTION 4

Which of the following policies establishes rules to measure third-party work tasks and ensure deliverables are provided within a specific time line?

A. SLA

B. MOU

C. AUP

D. NDA

Correct Answer: A

QUESTION 5

A security administrator needs to provide secure access to internal networks for external partners The administrator has given the PSK and other parameters to the third-party security administrator. Which of the following is being used to establish this connection?

A. Kerberos

B. SSL/TLS

C. IPSec

D. SSH

Correct Answer: C

IPSec is a protocol suite that provides secure communication over IP networks. It uses encryption, authentication, and integrity mechanisms to protect data from unauthorized access or modification. IPSec can operate in two modes: transport mode and tunnel mode. In tunnel mode, IPSec can create a virtual private network (VPN) between two endpoints, such as external partners and internal networks. To establish a VPN connection, IPSec requires a pre-shared key (PSK) or other parameters to negotiate the security association.

References: https://www.comptia.org/content/guides/what-is-vpn