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.geekcert.com/sy0-601.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

A systems administrator needs to install the same X.509 certificate on multiple servers. Which of the following should the administrator use?

A. Key escrow

B. A self-signed certificate

C. Certificate chaining

D. An extended validation certificate

Correct Answer: B

Internal certificates don\\'t need to be signed by a public CA ? Your company is the only one going to use it

1.

No need to purchase trust for devices that already trust you

2.

Build your own CA ?Issue your own certificates signed by your own CA

3.

Install the CA certificate/trusted chain on all devices

4.

They\\'ll now trust any certificates signed by your internal CA

5.

Works exactly like a certificate you purchased

QUESTION 2

An attacker was eavesdropping on a user who was shopping online. The attacker was able to spoof the IP address associated with the shopping site. Later, the user received an email regarding the credit card statement with unusual purchases. Which of the following attacks took place?

A. On-path attack

B. Protocol poisoning

C. Domain hijacking

D. Bluejacking

Correct Answer: A

On path attack is often known as man in the middle.

QUESTION 3

A user wanted to catch up on some work over the weekend but had issues logging in to the corporate network using a VPN. On Monday, the user opened a ticket for this issue but was able to log in successfully.

Which of the following BEST describes the policy that is being implemented?

A. Time-based logins

B. Geofencing

C. Network location

D. Password history

Correct Answer: A

Time based logins should be the answer because Geofencing is accepting or rejecting access requests based on location.

QUESTION 4

Against the recommendation of the IT security analyst, a company set all user passwords on a server as "P@)55wOrD". Upon review of the /etc/pesswa file, an attacker found the following:

alice:a8df3b6c4fd75f0617431fd248f35191df8d237f bob:2d250c5b2976b03d757f324ebd59340df96aa05e chris:ea981ec3285421d014108089f3f3f997ce0f4150

Which of the following BEST explains why the encrypted passwords do not match?

A. Perfect forward secrecy

B. Key stretching

C. Salting

D. Hashing

Correct Answer: C

QUESTION 5

An engineer needs to deploy a security measure to identify and prevent data tampering within the enterprise. Which of the following will accomplish this goal?

A. Antivirus

B. IPS.

C. FTP

D. FIM

Correct Answer: D

File Integrity Monitoring (FIM) is a security measure that helps identify and prevent data tampering within the enterprise. FIM systems monitor files and directories for any unauthorized changes, modifications, or tampering. When changes are detected, alerts or notifications are generated, allowing security teams to investigate and respond to potential security incidents.

FIM is particularly useful for detecting unauthorized changes to critical system files, configurations, and sensitive data. It helps maintain the integrity of important files and ensures that they remain in their original state, protecting against unauthorized access or manipulation.

Reference: https://www.cypressdatadefense.com/blog/data-tampering-prevention/