SY0-501 Q&As

CompTIA Security+ Certification Exam

Pass CompTIA SY0-501 Exam with 100% Guarantee

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

https://www.leads4pass.com/sy0-501.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

Which of the following BEST describes the concept of perfect forward secrecy?

A. Using quantum random number generation to make decryption effectively impossible

B. Preventing cryptographic reuse so a compromise of one operation does not affect other operations

C. Implementing elliptic curve cryptographic algorithms with true random numbers

D. The use of NDAs and policy controls to prevent disclosure of company secrets

Correct Answer: B

QUESTION 2

A company has noticed multiple instances of proprietary information on public websites. It has also observed an increase in the number of email messages sent to random employees containing malicious links and PDFs. Which of the following changes should the company make to reduce the risks associated with phishing attacks? (Select TWO)

A. Install an additional firewall

B. Implement a redundant email server

C. Block access to personal email on corporate systems

D. Update the X.509 certificates on the corporate email server

E. Update corporate policy to prohibit access to social media websites

F. Review access violation on the file server

Correct Answer: CE

QUESTION 3

A web server, which is configured to use TLS with AES-GCM-256, SHA-384, and ECDSA, recently suffered an information loss breach. Which of the following is MOST likely the cause?

A. Insufficient key bit length

B. Weak cipher suite

C. Unauthenticated encryption method

D. Poor implementation

Correct Answer: D

QUESTION 4

An organization plans to transition the intrusion detection and prevention techniques on a critical subnet to an anomaly-based system. Which of the following does the organization need to determine for this to be successful?

A. The baseline

B. The endpoint configurations

C. The adversary behavior profiles

D. The IPS signatures

Correct Answer: D

QUESTION 5

Which of the following are considered to be "something you do"? (Select TWO).

A. Iris scan

B. Handwriting

C. Common Access Card

D. Gait

E. PIN

F. Fingerprint

Correct Answer: BD

QUESTION 6

Which of the following BEST explains the difference between a credentialed scan and a non- credentialed scan?

A. A credentialed scan sees devices in the network, including those behind NAT, while a non- credentialed scan sees outward-facing applications.

B. A credentialed scan will not show up in system logs because the scan is running with the necessary authorization, while non-credentialed scan activity will appear in the logs.

C. A credentialed scan generates significantly more false positives, while a non-credentialed scan generates fewer false positives.

D. A credentialed scan sees the system the way an authorized user sees the system, while a non- credentialed scan sees the system as a guest.

Correct Answer: D

QUESTION 7

A technician must configure a firewall to block external DNS traffic from entering a network. Which of the following ports should they block on the firewall?

A. 53

B. 110

C. 143

D. 443

Correct Answer: A

QUESTION 8

Which of the following locations contain the MOST volatile data?

A. SSD

B. Paging file

C. RAM

D. Cache memory

Correct Answer: D

QUESTION 9

Ann, a user, reported to the service desk that many files on her computer will not open or the contents are not readable. The service desk technician asked Ann if she encountered any strange messages on boot-up or login, and Ann indicated she did not. Which of the following has MOST likely occurred on Ann\\'s computer?

A. The hard drive is falling, and the files are being corrupted.

B. The computer has been infected with crypto-malware.

C. A replay attack has occurred.

D. A keylogger has been installed.

Correct Answer: B

QUESTION 10

An organization discovers that unauthorized applications have been installed on company- provided mobile phones. The organization issues these devices, but some users have managed to bypass the security controls. Which of the

following Is the MOST likely issue, and how can the organization BEST prevent this from happening?

A. The mobile phones are being infected Willi malware that covertly installs the applications. Implement full disk encryption and integrity-checking software.

B. Some advanced users are jailbreaking the OS and bypassing the controls. Implement an MDM solution to control access to company resources.

C. The mobile phones have been compromised by an APT and can no longer be trusted. Scan the devices for the unauthorized software, recall any compromised devices, and issue completely new ones.

D. Some advanced users are upgrading the devices\\' OS and installing the applications. The organization should create an AUP that prohibits this activity.

Correct Answer: B

QUESTION 11

A security administrator needs to implement a system that detects possible intrusions based upon a vendor provided list. Which of the following BEST describes this type of IDS?

A. Signature based

B. Heuristic

C. Anomaly-based

D. Behavior-based

Correct Answer: A

QUESTION 12

Management wishes to add another authentication factor in addition to fingerprints and passwords in order to have three-factor authentication. Which of the following would BEST satisfy this request?

A. Retinal scan

B. Passphrase

C. Token fob

D. Security question

Correct Answer: C

QUESTION 13

A recent internal audit is forcing a company to review each internal business unit\\'s VMs because the cluster they are

installed on is in danger of running out of computer resources. Which of the following vulnerabilities exist?

A. Buffer overflow

B. End-of-life systems

C. System sprawl

D. Weak configuration

Correct Answer: C

QUESTION 14

Which of the following is an algorithm family that was developed for use cases in which power consumption and lower computing power are constraints?

A. Elliptic curve

B. RSA

C. Diffie-Hellman

D. SHA

Correct Answer: A

QUESTION 15

A network technician is setting up a segmented network that will utilize a separate ISP to provide wireless access to the public area for a company. Which of the following wireless security methods should the technician implement to provide basic accountability for access to the public network?

A. Pre-shared key

B. Enterprise

C. Wi-Fi Protected setup

D. Captive portal

Correct Answer: D