SY0-401 Q&As

CompTIA Security+ Certification Exam

Pass CompTIA SY0-401 Exam with 100% Guarantee

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

https://www.pass4itsure.com/SY0-401.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

An employee reports work was being completed on a company-owned laptop using a public wireless hot-spot. A pop-up screen appeared, and the user closed the pop-up. Seconds later, the desktop background was changed to the image of a padlock with a message demanding immediate payment to recover the data. Which of the following types of malware MOST likely caused this issue?

A. Ransomware

B. Rootkit

C. Scareware

D. Spyware

Correct Answer: A

QUESTION 2

Having adequate lighting on the outside of a building is an example of which of the following security controls?

A. Deterrent

B. Compensating

C. Detective

D. Preventative

Correct Answer: A

QUESTION 3

A security administrator wishes to increase the security of the wireless network. Which of the following BEST addresses this concern?

A. Change the encryption from TKIP-based to CCMP-based.

B. Set all nearby access points to operate on the same channel.

C. Configure the access point to use WEP instead of WPA2.

D. Enable all access points to broadcast their SSIDs.

Correct Answer: A

CCMP makes use of 128-bit AES encryption with a 48-bit initialization vector. This initialization vector makes cracking a bit more difficult.

QUESTION 4

At an organization, unauthorized users have been accessing network resources via unused network wall jacks. Which of the following would be used to stop unauthorized access?

A. Configure an access list.

B. Configure spanning tree protocol.

C. Configure port security.

D. Configure loop protection.

Correct Answer: C

Port security in IT can mean several things. It can mean the physical control of all connection points, such as RJ-45 wall jacks or device ports, so that no unauthorized users or unauthorized devices can attempt to connect into an open port. This can be accomplished by locking down the wiring closet and server vaults and then disconnecting the workstation run from the patch panel (or punch-down block) that leads to a room\\'s wall jack. Any unneeded or unused wall jacks can (and should) be physically disabled in this manner. Another option is to use a smart patch panel that can monitor the MAC address of any device connected to each and every wall port across a building and detect not just when a new device is connected to an empty port, but also when a valid device is disconnected or replaced by an invalid device.

QUESTION 5

A security administrator has been asked to implement a VPN that will support remote access over IPSEC. Which of the following is an encryption algorithm that would meet this requirement?

A. MD5

B. AES

C. UDP

D. PKI

Correct Answer: B

QUESTION 6

A security administrator is segregating all web-facing server traffic from the internal network and restricting it to a single interface on a firewall. Which of the following BEST describes this new network?

A. VLAN

B. Subnet

C. VPN

D. DMZ

Correct Answer: D

A DMZ or demilitarized zone (sometimes referred to as a perimeter network) is a physical or logical subnetwork that contains and exposes an organization\\'s external-facing services to a larger and untrusted network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization\\'s local area network (LAN); an external network node only has direct access to equipment in the DMZ, rather than any other part of the network. The name is derived from the term "demilitarized zone", an area between nation states in which military operation is not permitted.

QUESTION 7

A system administrator is configuring shared secrets on servers and clients. Which of the following authentication services is being deployed by the administrator? (Select two.)

A. Kerberos

B. RADIUS

C. TACACS+

D. LDAP

E. Secure LDAP

Correct Answer: BD

QUESTION 8

When performing the daily review of the system vulnerability scans of the network Joe, the administrator, noticed several security related vulnerabilities with an assigned vulnerability identification number. Joe researches the assigned vulnerability identification number from the vendor website. Joe proceeds with applying the recommended solution for identified vulnerability.

Which of the following is the type of vulnerability described?

A. Network based

B. IDS

C. Signature based

D. Host based

Correct Answer: C

A signature-based monitoring or detection method relies on a database of signatures or patterns of known malicious or unwanted activity. The strength of a signature-based system is that it can quickly and accurately detect any event from its database of signatures.

QUESTION 9

An organization has three divisions: Accounting, Sales, and Human Resources. Users in the Accounting division require access to a server in the Sales division, but no users in the Human Resources division should have access to resources

in any other division, nor should any users in the Sales division have access to resources in the Accounting division. Which of the following network segmentation schemas would BEST meet this objective?

A. Create two VLANS, one for Accounting and Sales, and one for Human Resources.

B. Create one VLAN for the entire organization.

C. Create two VLANs, one for Sales and Human Resources, and one for Accounting.

D. Create three separate VLANS, one for each division.

Correct Answer: D

A virtual local area network (VLAN) is a hardware-imposed network segmentation created by switches. Communications between ports within the same VLAN occur without hindrance, but communications between VLANs require a routing function.

QUESTION 10

During a Linux security audit at a local college, it was noted that members of the dean\\'s group were able to modify employee records in addition to modifying student records, resulting in an audit exception. The college security policy states that the dean\\'s group should only have the ability to modify student records. Assuming that the correct user and group ownerships are in place, which of the following sets of permissions should have been assigned to the directories containing the employee records?

A. R-x---rwx

B. Rwxrwxrwx

C. Rwx----wx

D. Rwxrwxr-

Correct Answer: B

QUESTION 11

Configuring the mode, encryption methods, and security associations are part of which of the following?

A. IPSec

B. Full disk encryption

C. 802.1x

D. PKI

Correct Answer: A

IPSec can operate in tunnel mode or transport mode. It uses symmetric cryptography to provide encryption security. Furthermore, it makes use of Internet Security Association and Key Management Protocol (ISAKMP).

QUESTION 12

A security manager is preparing the training portion of an incident plan. Which of the following job roles should receive training on forensics, chain of custody, and the order of volatility?

A. System owners

B. Data custodians

C. First responders

D. Security guards

Correct Answer: C