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.lead4pass.com/SY0-401.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 classroom utilizes workstations running virtualization software for a maximum of one virtual machine per working station. The network settings on the virtual machines are set to bridged. Which of the following describes how the switch in the classroom should be configured to allow for the virtual machines and host workstation to connect to network resources?

A. The maximum-mac settings of the ports should be set to zero

B. The maximum-mac settings of the ports should be set to one

C. The maximum-mac settings of the ports should be set to two

D. The maximum mac settings of the ports should be set to three

Correct Answer: A

QUESTION 2

Which of the following protocols allows for the LARGEST address space?

A. IPX

B. IPv4

C. IPv6

D. Appletalk

Correct Answer: C

The main advantage of IPv6 over IPv4 is its larger address space. The length of an IPv6 address is 128 bits, compared with 32 bits in IPv4.

QUESTION 3

Which of the following would be MOST appropriate to secure an existing SCADA system by preventing connections from unauthorized networks?

A. Implement a HIDS to protect the SCADA system

B. Implement a Layer 2 switch to access the SCADA system

C. Implement a firewall to protect the SCADA system

D. Implement a NIDS to protect the SCADA system

Correct Answer: C

Firewalls manage traffic using filters, which is just a rule or set of rules. A recommended guideline for firewall rules is, "deny by default; allow by exception". This means that if a network connection is not specifically allowed, it will be

denied.

QUESTION 4

A company hires a penetration testing team to test its overall security posture. The organization has not disclosed any information to the penetration testing team and has allocated five days for testing. Which of the following types of testing will the penetration testing team have to conduct?

A. Static analysis

B. Gray Box

C. White box

D. Black box

Correct Answer: D

QUESTION 5

A security analyst needs to logon to the console to perform maintenance on a remote server. Which of the following protocols would provide secure access?

A. SCP

B. SSH

C. SFTP

D. HTTPS

Correct Answer: B

Secure Shell (SSH) is a tunneling protocol originally used on Unix systems. It\\'s now available for both Unix and Windows environments. SSH is primarily intended for interactive terminal sessions. SSH is used to establish a command-line, text-only interface connection with a server, router, switch, or similar device over any distance.

QUESTION 6

The programmer confirms that there is potential for a buffer overflow on one of the data input fields in a corporate application. The security analyst classifies this as a (N).

A. Threat

B. Risk

C. Attack

D. Vulnerability

Correct Answer: D

QUESTION 7

Ann is an employee in the accounting department and would like to work on files from her home computer. She recently heard about a new personal cloud storage service with an easy web interface. Before uploading her work related files into the cloud for access, which of the following is the MOST important security concern Ann should be aware of?

A. Size of the files

B. Availability of the files

C. Accessibility of the files from her mobile device

D. Sensitivity of the files

Correct Answer: D

Cloud computing has privacy concerns, regulation compliance difficulties, use of open- /closed-source solutions, and adoption of open standards. It is also unsure whether cloud- based data is actually secured (or even securable).

QUESTION 8

Users can authenticate to a company\\'s web applications using their credentials form a popular social media site. Which of the following poses the greatest risk with this integration?

A. Malicious users can exploit local corporate credentials with their social media credentials

B. Changes to passwords on the social media site can be delayed from replicating to the company

C. Data loss from the corporate servers can create legal liabilities with the social media site

D. Password breaches to the social media affect the company application as well

Correct Answer: D

QUESTION 9

Mike, a network administrator, has been asked to passively monitor network traffic to the company\\'s sales websites. Which of the following would be BEST suited for this task?

A. HIDS

B. Firewall

C. NIPS

D. Spam filter

Correct Answer: C

Network-based intrusion prevention system (NIPS) monitors the entire network for suspicious traffic by analyzing protocol activity.

QUESTION 10

Joe is exchanging encrypted email with another party. Joe encrypts the initial email with a key. When Joe receives a response, he is unable to decrypt the response with the same key he used initially. Which of the following would explain the situation?

A. An ephemeral key was used for one of the messages

B. A stream cipher was used for the initial email, a block cipher was used for the reply

C. Out-of-band key exchange has taken place

D. Asymmetric encryption is being used

Correct Answer: D

QUESTION 11

After making a bit-level copy of compromised server, the forensics analyst Joe wants to verify that he bid not accidentally make a change during his investigation. Which of the following should he perform?

A. Take a hash of the image and compare it to the one being investigated

B. Compare file sizes of all files prior to and after investigation

C. Make a third image and compare it to the second image being investigated

D. Compare the logs of the copy to the actual server

Correct Answer: A

QUESTION 12

Which of the following protocols operates at the HIGHEST level of the OSI model?

A. ICMP

B. IPSec

C. SCP

D. TCP

Correct Answer: C

SCP (Secure Copy) uses SSH (Secure Shell). SSH runs in the application layer (layer 7) of the OSI model.