JK0-022 Q&As

CompTIA Security+ Certification

Pass CompTIA JK0-022 Exam with 100% Guarantee

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

https://www.leads4pass.com/jk0-022.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Which of the following security devices can be replicated on a Linux based computer using IP tables to inspect and properly handle network based traffic?

A. Sniffer

B. Router

C. Firewall

D. Switch

Correct Answer: C

Ip tables are a user-space application program that allows a system administrator to configure the tables provided by the Linux kernel firewall and the chains and rules it stores.

Incorrect Answers:

A: A sniffer is a tool used in the process of monitoring the data that is transmitted across a network. B, D: A router is connected to two or more data lines from different networks, whereas a network switch is connected to data lines from one single network. These may include a firewall, but not by default.

References:

http://en.wikipedia.org/wiki/Iptables

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 342.

http://en.wikipedia.org/wiki/Router_(computing)

QUESTION 2

A way to assure data at-rest is secure even in the event of loss or theft is to use:

A. Full device encryption.

B. Special permissions on the file system.

C. Trusted Platform Module integration.

D. Access Control Lists.

Correct Answer: A

Device encryption encrypts the data on the device. This feature ensures that the data on the device cannot be accessed in a useable form should the device be stolen.

Incorrect Answers:

B: Permissions on the file system define the level of access logged on users have to files and folders. However, should

an unauthorized user gain access to an authorized user\\'s user account, they would gain access to the files and folders.

C: Trusted Platform Module (TPM) is a hardware-based encryption solution that is embedded in the system\\'s motherboard. It helps with hash key generation and stores cryptographic keys, passwords, or certificates.

D: Access Control Lists (ACLs) define the level of access logged on users have to resources. However, should an unauthorized user gain access to an authorized user\\'s user account, they would gain access to the data.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 156, 237, 418-419 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 236,

QUESTION 3

The information security technician wants to ensure security controls are deployed and functioning as intended to be able to maintain an appropriate security posture. Which of the following security techniques is MOST appropriate to do this?

A. Log audits

B. System hardening

C. Use IPS/IDS

D. Continuous security monitoring

Correct Answer: D

A security baseline is the security setting of a system that is known to be secure. This is the initial security setting of a system. Once the baseline has been applied, it must be maintained or improved. Maintaining the security baseline requires continuous monitoring.

Incorrect Answers:

A: Auditing logs is good practice. However, it is only one aspect of maintaining security posture. This question asks for the MOST appropriate answer. Continuous security monitoring covers all aspects of maintaining security posture so it is a more appropriate answer.

B: Hardening is the process of securing a system by reducing its surface of vulnerability. Reducing the surface of vulnerability typically includes removing or disabling unnecessary functions and features, removing or disabling unnecessary user accounts, disabling unnecessary protocols and ports, and disabling unnecessary services.

C: An IPS/IDS (intrusion prevention system/intrusion detection system) is used to detect and prevent malicious activity on a network or a host. However, there is more to maintaining security posture that this one aspect and should be a part of continuous security monitoring.

References:

Stewart, James Michael, Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, Sybex, Indianapolis, 2014, p 12, 61, 130 Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition,

Sybex, Indianapolis, 2014, pp 208, 215-217, 222

QUESTION 4

A computer is put into a restricted VLAN until the computer\\'s virus definitions are up-to-date. Which of the following BEST describes this system type?

A. NAT

B. NIPS

C. NAC

D. DMZ

Correct Answer: C

Network Access Control (NAC) means controlling access to an environment through strict adherence to and implementation of security policies. The goals of NAC are to prevent/reduce zero-day attacks, enforce security policy throughout the network, and use identities to perform access control.

Incorrect Answers:

A: NAT serves as a basic firewall by only allowing incoming traffic that is in response to an internal system\\'s request.

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

D: A demilitarized zone (DMZ) is an area of a network that is designed specifically for public users to access.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 39, 40.

http://en.wikipedia.org/wiki/Intrusion_prevention_system

QUESTION 5

Which of the following is used by the recipient of a digitally signed email to verify the identity of the sender?

A. Recipient\\'s private key

B. Sender\\'s public key

C. Recipient\\'s public key

D. Sender\\'s private key

Correct Answer: B

When the sender wants to send a message to the receiver. It\\'s important that this message not be altered. The sender uses the private key to create a digital signature. The message is, in effect, signed with the private key. The sender then sends the message to the receiver. The recipient uses the public key attached to the message to validate the digital signature. If the values match, the receiver knows the message is authentic. Thus the recipient uses the sender\\'s public key to verify the sender\\'s identity.

Incorrect Answers:

A: The recipient\\'s private key is not required to check the identity of the sender.

C: The public key must be sent to the recipient by the sender, the recipient cannot use their own public key.

D: The sender must use the private key to create the digital signature.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 261