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

A company has proprietary mission critical devices connected to their network which are configured remotely by both employees and approved customers. The administrator wants to monitor device security without changing their baseline configuration. Which of the following should be implemented to secure the devices without risking availability?

A. Host-based firewall

B. IDS

C. IPS

D. Honeypot

Correct Answer: B

QUESTION 2

A security analyst has been notified that trade secrets are being leaked from one of the executives in the corporation. When reviewing this executive\\'s laptop they notice several pictures of the employee\\'s pets are on the hard drive and on a cloud storage network. When the analyst hashes the images on the hard drive against the hashes on the cloud network they do not match.

Which of the following describes how the employee is leaking these secrets?

A. Social engineering

B. Steganography

C. Hashing

D. Digital signatures

Correct Answer: B

Steganography is the process of hiding one message in another. Steganography may also be referred to as electronic watermarking. It is also the process of hiding a message in a medium such as a digital image, audio fi le, or other fi le. In theory, doing this prevents analysts from detecting the real message. You could encode your message in another file or message and use that file to hide your message.

Incorrect Answers:

A: Social engineering is the process by which intruders gain access to your facilities, your network, and even your employees by exploiting the generally trusting nature of people. A social engineering attack may come from someone posing as a vendor, or it could take the form of an email from a (supposedly) traveling executive who indicates that they have forgotten how to log on to the network or how to get into the building over the weekend.

C: Hashing refers to the hash algorithms used in Cryptography.

D: Digital Signatures is used to validate the integrity of the message and the sender.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 248, 255, 261, 355, 414

QUESTION 3

Which of the following would satisfy wireless network implementation requirements to use mutual authentication and usernames and passwords?

A. EAP-MD5

B. WEP

C. PEAP-MSCHAPv2

D. EAP-TLS

Correct Answer: C

PEAP-MS-CHAP v2 is easier to deploy than EAP-TLS or PEAP-TLS because user authentication is accomplished via password-base credentials (user name and password) rather than digital certificates or smart cards.

Incorrect Answers:

A: MD5 has been employed in a wide selection of cryptographic applications, and is also commonly used to verify data integrity.

B: Usernames and passwords are not required for WEP authentication.

D: Authenticated wireless access design based on Extensible Authentication Protocol Transport Level Security (EAP-TLS) can use either smart cards or user and computer certificates to authenticate wireless access clients. EAP-TLS does not use usernames and passwords for authentication.

References:

https://technet.microsoft.com/en-us/library/dd348500(v=ws.10).aspx https://technet.microsoft.com/en-us/library/dd348478(v=ws.10).aspx http://en.wikipedia.org/ wiki/MD5

QUESTION 4

Which of the following wireless security measures can an attacker defeat by spoofing certain properties of their network interface card?

A. WEP

B. MAC filtering

C. Disabled SSID broadcast

D. TKIP

Correct Answer: B

MAC filtering is typically used in wireless networks. In computer networking, MAC Filtering (or GUI filtering, or layer 2

address filtering) refers to a security access control method whereby the 48-bit address assigned to each network card is used to determine access to the network. MAC addresses are uniquely assigned to each card, so using MAC filtering on a network permits and denies network access to specific devices through the use of blacklists and whitelists. While the restriction of network access through the use of lists is straightforward, an individual person is not identified by a MAC address, rather a device only, so an authorized person will need to have a whitelist entry for each device that he or she would use to access the network. While giving a wireless network some additional protection, MAC filtering can be circumvented by scanning a valid MAC (via airodumping) and then spoofing one\\'s own MAC into a validated one.

Incorrect Answers:

A: WEP short for Wired Equivalent Privacy is a security protocol for wireless local area networks (WLANs) defined in the 802.11b standard. WEP is an encryption method to secure the connection. WEP uses a 40-bit or 104-bit encryption key that must be manually entered on wireless access points and devices. Although WEP is considered to be a weak security protocol, it is not defeated by spoofing. Therefore, this answer is incorrect.

C: Disabling SSID broadcast is a security measure that makes the wireless network invisible to computers; it will not show up in the list of available wireless networks. To connect to the wireless network, you need to know the SSID of the network and manually enter it. Spoofing is not used to circumvent this security measure. Therefore, this answer is incorrect.

D: TKIP (Temporal Key Integrity Protocol) is an encryption protocol included as part of the IEEE 802.11i standard for wireless LANs (WLANs). It was designed to provide more secure encryption than the notoriously weak Wired Equivalent Privacy (WEP), the original WLAN security protocol. TKIP is the encryption method used in Wi-Fi Protected Access (WPA), which replaced WEP in WLAN products. TKIP is not defeated by spoofing. Therefore, this answer is incorrect. References: http://en.wikipedia.org/wiki/MAC_filtering http://searchmobilecomputing.techtarget.com/definition/TKIP

QUESTION 5

An insurance company requires an account recovery process so that information created by an employee can be accessed after that employee is no longer with the firm. Which of the following is the BEST approach to implement this process?

A. Employee is required to share their password with authorized staff prior to leaving the firm

B. Passwords are stored in a reversible form so that they can be recovered when needed

C. Authorized employees have the ability to reset passwords so that the data is accessible

D. All employee data is exported and imported by the employee prior to them leaving the firm

Correct Answer: C

Since a user\\'s password isn\\'t stored on most operating systems (only a hash value is kept), most operating systems allow the administrator (or authorized person in this case) to change the value then the information/files/documents can be accessed. This is the safest way of recovery by an authorized person and is not dependent on those who leave the firm.

Incorrect Answers:

A: No user should be expected to share their password, regardless of the circumstances. Shared passwords goes against normal security procedures.

B: Storing passwords in a reversible form is not best practice and thus not risk avoidance.

D: This may not always be possible as the circumstances can differ vastly when employees leave the firm.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp.140-142