JK0-022$^{Q\&As}$

CompTIA Security+ Certification

QUESTION 1

A system administrator wants to confidentially send a user name and password list to an individual outside the company without the information being detected by security controls. Which of the following would BEST meet this security goal?

A. Digital signatures

B. Hashing

C. Full-disk encryption

D. Steganography

Correct Answer: D

QUESTION 2

Which of the following concepts is used by digital signatures to ensure integrity of the data?

A. Non-repudiation

B. Hashing

C. Transport encryption

D. Key escrow

Correct Answer: B

Most digital signature implementations also use a hash to verify that the message has not been altered, intentionally or accidently, in transit.

Incorrect Answers:

A: Regarding digital security, the cryptographical meaning and application of non-repudiation shifts to mean:

*

A service that provides proof of the integrity and origin of data.

*

An authentication that can be asserted to be genuine with high assurance.

B: Digital signatures are not implemented through transport encryption.

D: Key escrow addresses the possibility that a third party may need to access keys. Under the conditions of key escrow, the keys needed to encrypt/decrypt data are held in an escrow account (think of the term as it relates to home

mortgages) and made available if that third party requests them.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 249, 255, 261, 262

QUESTION 3

A small company has recently purchased cell phones for managers to use while working outside if the office.

The company does not currently have a budget for mobile device management and is primarily concerned with deterring leaks if sensitive information obtained by unauthorized access to unattended phones. Which of the following would provide the solution BEST meets the company\\'s requirements?

A. Screen-lock

B. Disable removable storage

C. Full device encryption

D. Remote wiping

Correct Answer: A

Screen-lock is a security feature that requires the user to enter a password after a short period of inactivity before they can access the system again. This feature ensures that if your device is left unattended or is lost or stolen, it will be difficult for anyone else to access your data or applications.

Incorrect Answers:

B: Merely disabling removable storage will not prevent sensitive information from being accessed by unauthorized people when the phone is left unattended.

C: 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.

D: Remote wipe is the process of deleting data on a device in the event that the device is stolen. This is performed over remote connections such as the mobile phone service or the internet connection and helps ensure that sensitive data is not accessed by unauthorized people.

References:

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

QUESTION 4

In which of the following steps of incident response does a team analyse the incident and determine steps to prevent a future occurrence?

A. Mitigation

B. Identification

C. Preparation

D. Lessons learned

Correct Answer: D

Incident response procedures involves in chronological order: Preparation; Incident identification; Escalation and notification; Mitigation steps; Lessons learned; Reporting; Recover/reconstitution procedures; First responder; Incident isolation (Quarantine; Device removal); Data breach; Damage and loss control. Thus lessons are only learned after the mitigation occurred. For only then can you `step back\\' and analyze the incident to prevent the same occurrence in future.

Incorrect Answers:

A: Mitigation is accomplished anytime that any steps has been taken to reduce risk.

B: When responding to an incident the identification of the incident is essential to know how to handle the incident and then take steps. This happens way before an incident is analyzed to determine which steps to take to prevent the same occurrence in future.

C: Preparation involves all the preventative measures that are taken to prevent any risk incident. This does not means that an incident already occurred as is alluded to in the question.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 429

QUESTION 5

Which of the following protocols is vulnerable to man-in-the-middle attacks by NOT using end to end TLS encryption?

A. HTTPS

B. WEP

C. WPA

D. WPA 2

Correct Answer: B

WEP offers no end-to-end TLS encryption.

The WEP process consists of a series of steps as follows:

The wireless client sends an authentication request.

The Access Point (AP) sends an authentication response containing clear-text (uh-oh!) challenge text. The client takes the challenge text received and encrypts it using a static WEP key. The client sends the encrypted authentication packet

to the AP. The AP encrypts the challenge text using its own static WEP key and compares the result to the authentication packet sent by the client. If the results match, the AP begins the association process for the wireless client.

The big issue with WEP is the fact that it is very susceptible to a Man in the Middle attack. The attacker captures the clear-text challenge and then the authentication packet reply. The attacker then reverses the RC4 encryption in order to derive the static WEP key. Yikes! As you might guess, the designers attempted to strengthen WEP using the approach of key lengths. The native Windows client supported a 104-bit key as opposed to the initial 40-bit key. The fundamental

weaknesses in the WEP process still remained however.

Incorrect Answers:

A: HTTPS (HTTP over SSL or HTTP Secure) is the use of Secure Socket Layer (SSL) or Transport Layer Security (TLS) as a sublayer under regular HTTP application layering. HTTPS encrypts and decrypts user page requests as well as the

pages that are returned by the Web server. The use of HTTPS protects against eavesdropping and man-in-the-middle attacks.

Therefore, this answer is incorrect.

C: WPA (WiFi Protected Access) is the new security standard adopted by the WiFi Alliance consortium. WiFi compliance ensures interoperability between different manufacturer\\'s wireless equipment. WPA is a much improved encryption

standard that delivers a level of security beyond anything that WEP can offer. It bridges the gap between WEP and 802.11i (WPA2) networks. WPA uses Temporal Key Integrity Protocol (TKIP), which is designed to allow WEP to be upgraded

through corrective measures that address the existing security problems. WPA is able to achieve over 500 trillion possible key combinations and re-keying of global encryption keys is required. The encryption key is changed after every frame

using TKIP. This allows key changes to occur on a frame by frame basis and to be automatically synchronized between the access point and the wireless client. The TKIP encryption algorithm is stronger than the one used by WEP. WPA is

compatible with many older access points and network cards. WPA uses TKIP to provide TLS encryption. Therefore, this answer is incorrect.

D: WPA2 is the latest implementation of WPA and provides stronger data protection and network access control. It provides WiFi users with a higher level of assurance that only authorized users can access their wireless networks. WPA2 is

based on the IEEE 802.11i standard and provides government grade security. 802.11i describes the encrypted transmission of data between systems of 802.11a and 802.11b wireless LANs. It defines new encryption key protocols including

the Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES).

WPA2 uses TKIP or AES to provide TLS encryption. Therefore, this answer is incorrect.

References:

http://blog.ine.com/2010/10/16/wlan-security-wep/

http://searchsoftwarequality.techtarget.com/definition/HTTPS
http://www.onlinecomputertips.com/networking/wep_wpa.html