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

CompTIA Security+ Certification

Pass CompTIA JK0-022 Exam with 100% Guarantee

QUESTION 1

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 2

A large corporation has data centers geographically distributed across multiple continents. The company needs to securely transfer large amounts of data between the data center. The data transfer can be accomplished physically or electronically, but must prevent eavesdropping while the data is on transit. Which of the following represents the BEST cryptographic solution?

A. Driving a van full of Micro SD cards from data center to data center to transfer data

B. Exchanging VPN keys between each data center via an SSL connection and transferring the data in the VPN

C. Using a courier to deliver symmetric VPN keys to each data center and transferring data in the VPN

D. Using PKI to encrypt each file and transferring them via an Internet based FTP or cloud server

Correct Answer: B

A virtual private network (VPN) is an encrypted communication tunnel that connects two systems over an untrusted network, such as the Internet. They provide security for both authentication and data transmission through a process called encapsulation. Secure Sockets Layer (SSL) can be used to exchange the VPN keys securely. SSL is used to establish secure TCP communication between two machines by encrypting the communication.

Incorrect Answers:

A: The data centers are geographically distributed across multiple continents. This makes it difficult to transport the data by driving a van.

C: Symmetrical keys are rendered useless when the key is stolen as the same key is used for encryption and decryption. D. PKI can be used to encrypt the data but transferring the data via FTP or a cloud server is not advisable. FTP is inherently insecure while cloud servers are used for storage.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 45, 304-305, 310-311
http://www.networkworld.com/article/2263539/compliance/vpn-security----do-you-know-where- your-keys-are-.html

---

QUESTION 3

The string:

` or 1=1--

Represents which of the following?

A. Bluejacking

B. Rogue access point

C. SQL Injection

D. Client-side attacks

Correct Answer: C

The code in the question is an example of a SQL Injection attack. The code `1=1\\' will always provide a value of true. This can be included in statement designed to return all rows in a SQL table.

SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application\\'s software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.

Incorrect Answers:

A: Bluejacking is the sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or laptop computers, sending a vCard which typically contains a message in the name field (i.e., for bluedating or bluechat) to another Bluetooth- enabled device via the OBEX protocol. The code in the question is not an example of bluejacking. Therefore, this answer is incorrect.

B: A rogue access point is a wireless access point that has either been installed on a secure company network without explicit authorization from a local network administrator, or has been created to allow a hacker to conduct a man-in-themiddle attack. Rogue access points of the first kind can pose a security threat to large organizations with many employees, because anyone with access to the premises can install (maliciously or non-maliciously) an inexpensive wireless router that can potentially allow access to a secure network to unauthorized parties. Rogue access points of the second kind target networks that do not employ mutual authentication (client-server server-client) and may be used in conjunction with a rogue RADIUS server, depending on security configuration of the target network. A rogue access point would not create the code shown in the question. Therefore, this answer is incorrect.

D: Client-side attacks target vulnerabilities in client applications interacting with a malicious data. The difference is the client is the one initiating the bad connection. The code in the question is much more likely to be part of a SQL statement in a SQL Injection attack. Therefore, this answer is incorrect. References: http://en.wikipedia.org/wiki/SQL_injection http://en.wikipedia.org/wiki/Bluejacking http://en.wikipedia.org/wiki/Rogue_access_point

QUESTION 4

Company A submitted a bid on a contract to do work for Company B via email. Company B was insistent that the bid did not come from Company A. Which of the following would have assured that the bid was submitted by Company A?

A. Steganography

B. Hashing

C. Encryption

D. Digital Signatures

Correct Answer: D

A digital signature is similar in function to a standard signature on a document. It validates the integrity of the message and the sender. The message is encrypted using the encryption system, and a second piece of information, the digital signature, is added to the message.

Incorrect Answers:

A: Steganography is the process of hiding a message in a medium such as a digital image, audio fi le, or other file. In theory, doing this prevents analysts from detecting the real message. You could encode your message in another fi le or

message and use that fi le to hide your message.

B: Hashing refers to the hash algorithms used in cryptography. It is used to store data, such as hash tables and its main characteristics are:

It must be one-way it is not reversible.

Variable-length input produces fixed-length output whether you has two characters of 2 million, the hash size is the same. The algorithm must have few or no collisions in hashing two different inputs does not give the same output.

C: Encryption is too wide a concept since all companies would have their bids encrypted. Encryption is part of the process when making use of digital signatures.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 248, 255, 261, 291

QUESTION 5

A recent audit has discovered that at the time of password expiration clients are able to recycle the previous credentials for authentication. Which of the following controls should be used together to prevent this from occurring? (Select TWO).

A. Password age

B. Password hashing

C. Password complexity

D. Password history

E. Password length

Correct Answer: AD

D: Password history determines the number of previous passwords that cannot be used when a user changes his password. For example, a password history value of 5 would disallow a user from changing his password to any of his previous 5 passwords.

A: When a user is forced to change his password due to a maximum password age period expiring, he could change his password to a previously used password. Or if a password history value of 5 is configured, the user could change his password six times to cycle back round to his original password. This is where the minimum password age comes in. This is the period that a password must be used for. For example, a minimum password age of 30 would determine that when a user changes his password, he must continue to use the same password for at least 30 days.

Incorrect Answers:

B: Hashing is a one-way function that creates a fixed-length output from an input of any length. C, E: Password complexity combined with password length helps produce strong passwords, but can be recycled if password age and history is not configured.

References:

https://technet.microsoft.com/enus/library/cc757692%28v=ws.10%29.aspx#w2k3tr_sepol_accou_set_kuwh Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 292, 293, 315.