Date: 11/23/2015 1:03:17 am
Time Spent: 14:56

Candidate: Belskis, Tomas
Login: t0mas9lt

Overall Performance

Your Score: 42%

Passing Score: 80%

Certification Ranking

Within your class: Within your school: Nationally:

View results by: ○ Objective Analysis ● Individual Responses

Individual Responses

Question 1: Correct

Hashing algorithms are used to perform what activity?

○ Provide a means to exchange small amounts of data securely over a public network

○ Encrypt bulk data for communications exchange

○ Provide for non-repudiation

➡ ● Create a message digest

Explanation

Hashing algorithms are used to create a message digest to ensure that data integrity is maintained. A sender creates a message digest by performing the hash function on the data files to be transmitted. The receiver performs the same action on the data received and compares the two message digests. If they are the same then the data was not altered.

Symmetric algorithms are used to encrypt bulk data for communications exchange. Asymmetric algorithms provide a means to exchange small amounts of data securely over a public network. Both symmetric and asymmetric algorithms provide for non-repudiation.

References

LabSim for Security Pro, Section 3.2.
[Questions.exm SP02_4-1 [5]]

Question 2: Incorrect

Which of the following best describes *high amplification* when applied to hashing algorithms?

➡ ○ A small change in the message results in a big change in the hash value.

● ~~Hashes produced by two different parties using the same algorithm result in the same hash value.~~

○ Reversing the hashing function does not recover the original message.

○ Dissimilar messages frequently result in the same hash value.

Explanation

High amplification, also known as the *avalanche effect*, means a small change in the message results in a big change in the hashed value.

Hashes are one-way functions, meaning that once you hash a message, you cannot reverse the hashing algorithm to extract the data. Data integrity is proven when the same hashing algorithm performed on a message results in the same hash value. A *collision* results when two different messages produce the same hash value (a low number of collisions is desirable).

References

LabSim for Security Pro, Section 3.2.
[Questions.exm SSCP-2 NEW [98]]

▼ Question 3: Incorrect

When two different messages produce the same hash value, what has occurred?

○ Birthday attack

◉ ~~Hash value~~

➡ ○ Collision

○ High amplification

Explanation

A *collision* occurs when two different messages produce the same hash value.

A birthday attack is a brute force attack in which the attacker hashes messages until one with the same hash is found. A hash value is the result of a compressed and transformed message (or some type of data) into a fixed-length value. High amplification means a small change in the message results in a big change in the hashed value.

References

LabSim for Security Pro, Section 3.2.
[Questions.exm SSCP-2 NEW [114]]

▼ Question 4: Correct

Which of the following is used to verify that a downloaded file has not been altered?

➡ ◉ Hash

○ Symmetric encryption

○ Asymmetric encryption

○ Private key

Explanation

A *hash* is a function that takes a variable-length string (message) and compresses and transforms it into a fixed-length value. Hashes ensure the data integrity of files and messages in transit. For example, when users post files for download, they often create a hash value for the file. After you download the file, you can create a hash using the same algorithm. If the hash values match, you know that the file you have matches the original file.

Symmetric encryption is typically used for fast encryption of data. Asymmetric encryption is used for encrypting small amounts of data or for exchanging keys used with symmetric encryption. A private key is one of the keys used in asymmetric encryption.

References

LabSim for Security Pro, Section 3.2.
[Questions.exm SP08_5-2 1]

▼ Question 5: Incorrect

You have just downloaded a file. You create a hash of the file and compare it to the hash posted on the Web site. The two hashes match. What do you know about the file?

● ~~You can prove the source of the file.~~

○ You will be the only one able to open the downloaded file.

○ No one has read the file contents as it was downloaded.

➡ ○ Your copy is the same as the copy posted on the website.

Explanation

A *hash* is a function that takes a variable-length string (message) and compresses and transforms it into a fixed-length value. Hashes ensure the data integrity of files and messages in transit. The sender and the receiver use the same hashing algorithm on the original data. If the hashes match, then the data can be assumed to be unmodified.

Hashes do *not* ensure confidentiality (in other words, hashes are not used to encrypt data). Non-repudiation proves the source of a file, and is accomplished using digital signatures.

References

LabSim for Security Pro, Section 3.2.
[Questions.exm SP08_5-2 2]

▼ Question 6: Correct

Which of the following is the strongest hashing algorithm?

○ LANMAN

○ NTLM

○ MD5

➡ ● SHA-1

Explanation

SHA-1 is the strongest hashing algorithm. SHA-1 generates a message digest of 160 bits.

MD-5 is weaker than SHA-1, producing a message digest of 128 bits. LANMAN and NTLM both use hashing to protect authentication credentials, but these protocols are not used for creating hashes of data. LANMAN is less secure than NTLM, with either method being less secure than MD-5 (NTLM uses either MD-4 or MD-5 to produce the hash).

References

LabSim for Security Pro, Section 3.2.
[Questions.exm SP08_5-1 6]

▼ Question 7: Incorrect

Which of the following is the weakest hashing algorithm?

● ~~DES~~

○ AES

○ SHA-1

➡ ○ MD5

Explanation

MD5 is the weakest hashing algorithm. It produces a message digest of 128 bits. The larger the message digest the more secure the hash. SHA-1 is more secure because it produces a 160 bit message digest.

Both DES and AES are symmetric encryption algorithms, with DES being weaker than AES.

References

LabSim for Security Pro, Section 3.2.
[Questions.exm SP08_5-1 7]

▼ Question 8: Incorrect

SHA-1 uses which of the following bit length hashing algorithms?

● ~~128-bit, 160-bit, 192-bit, 224-bit, and 256-bit~~

➡ ○ Only 160-bit

○ Only 128-bit

○ 224-bit, 256-bit, 384-bit, and 512-bit

Explanation

SHA-1 is only a 160-bit hashing algorithm. It is capable of producing 2160 different combinations.

MD-2 and MD-4 both are 128-bit hashing algorithms. HAVAL is a 128-bit, 160-bit, 192-bit, 224-bit, and 256- bit hashing algorithm. SHA-2, a newer version of SHA-1, is a 224-bit, 256-bit, 384-bit, 512-bit hashing algorithm.

References

LabSim for Security Pro, Section 3.2.
[Questions.exm NEW [106]]

▼ Question 9: Incorrect

Which of the following does not or cannot produce a hash value of 128 bits?

➡ ○ SHA-1

● ~~MD2~~

○ MD5

○ RIPEMD

Explanation

SHA-1 produces hash values of 160 bits.

MD5 and MD2 both produce hash values of 128 bits. Haval can produce 128 bit hash values, but it can produce a hash value of any length.

References

LabSim for Security Pro, Section 3.2.
[Questions.exm CP [371]]

▼ Question 10: Correct

A birthday attack focuses on what?

○ E-commerce

➡ ◉ Hashing algorithms

○ Encrypted files

○ VPN links

Explanation

A birthday attack focuses on hashing algorithms. Birthday attacks exploit the probability that two messages using the same hash algorithm will produce the same message digest. This is also known as exploiting collision. If two different messages or files produce the same hashing digest, then a collision has occurred.

References

LabSim for Security Pro, Section 3.2.
[Questions.exm SP [603]]

▼ Question 11: Correct

If two different messages or files produce the same hashing digest, then a collision has occurred. What form of cryptographic attack exploits this condition?

○ Adaptive chosen ciphertext attack

➡ ◉ Birthday attack

○ Meet in the middle attack

○ Statistical attack

Explanation

Birthday attacks exploit collisions. Birthday attacks exploit the probability that two messages using the same hash algorithm will produce the same message digest.

An adaptive chosen ciphertext attack is used to discover the encryption key. Meet in the middle attack is used to determine the algorithm used. Statistical attack is used to exploit computer based cryptosystems, such as the inability to produce true random numbers.

References

LabSim for Security Pro, Section 3.2.
[Questions.exm SP [611]]

Question 12: Incorrect

If a birthday attack is successful, meaning the attacker discovers a password that generates the same hash as that captured from a user's logon credentials, which of the following is true? (Select two.)

□ The user is forced to change their password at their next logon attempt

□ The discovered password is always the same as the user's password

➡ ☑ A collision was discovered

➡ □ The discovered password will allow the attacker to log on as the user, even if it is not the same as the user's password

Explanation

The discovered password will allow the attacker to log on as the user, even if it is not the same as the user's password. This is because the birthday attack (i.e. password cracking) will discover a collision. A collision is when two messages produce the same hash. Collision does not guarantee that the two messages are the same. Thus, another password could be discovered that has the same hash as the original user's password. Since the authentication system checks only for matching hashes, the attacker could log on with a different password as long as it produces the correct hash.

The discovered password might not be the same as the user's password since collision only ensures that two messages produce the same hash, not that the two messages are the same. The attack component of the birthday attack is collision not collusion. Collusion is when two or more people agree to work together to commit a security violation. The act of an attacker discovering a user's password does not automatically force the user to change their password upon the next logon attempt. Instead, this is a good security practice to implement if a password compromise is discovered or suspected by the information security team.

References

LabSim for Security Pro, Section 3.2.
[Questions.exm CP [627]]