Exam Report: 9.9.5 Practice Questions

Date: 1/28/2020 7:05:03 pm
Time Spent: 2:14

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 60%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Incorrect

Hashing algorithms are used to perform what activity?

- Encrypt bulk data for communications exchange
- ~~Provide for non-repudiation~~
- Create a message digest
- Provide a means for exchanging small amounts of data securely over a public network

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 that will 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 for exchanging small amounts of data securely over a public network. Both symmetric and asymmetric algorithms provide for non-repudiation.

References

LabSim for Security Pro, Section 9.9.
[All Questions SecPro2017_v6.exm HASHING_01]

Question 2: Incorrect

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

- Dissimilar messages frequently result in the same hash value.
- ~~Reversing the hashing function does not recover the original message.~~
- 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.

Explanation

High amplification, also known as the *avalanche effect*, means that 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 9.9.
[All Questions SecPro2017_v6.exm HASHING_02]

Question 3: 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 9.9.
[All Questions SecPro2017_v6.exm HASHING_06]

Question 4: Correct

Which of the following is the weakest hashing algorithm?

- DES
- SHA-1
- AES
- 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. DES is weaker than AES.

References

LabSim for Security Pro, Section 9.9.
[All Questions SecPro2017_v6.exm HASHING_07]

Question 5: Correct

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

- Only 128-bit
- Only 160-bit
- 224-bit, 256-bit, 384-bit, and 512-bit
- 128-bit, 160-bit, 192-bit, 224-bit, and 256-bit

Explanation

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

MD-2 and MD-4 are both 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 9.9.
[All Questions SecPro2017_v6.exm HASHING_08]

Question 6: Incorrect

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

- MD5
- RIPEMD
- SHA-1
- ~~MD2~~

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 because it can produce a hash value of any length.

References

LabSim for Security Pro, Section 9.9.
[All Questions SecPro2017_v6.exm HASHING_09]

Question 7: Correct

A birthday attack focuses on what?

- E-commerce
- Hashing algorithms
- VPN links
- Encrypted files

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 9.9.
[All Questions SecPro2017_v6.exm HASHING_10]

Question 8: Incorrect

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

- Hash value
- ~~Birthday attack~~
- High amplification
- Collision

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 9.9.
[All Questions SecPro2017_v6.exm HASHING_03]

Question 9: Correct

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

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

References

LabSim for Security Pro, Section 9.9.
[All Questions SecPro2017_v6.exm HASHING_04]

Question 10: Correct

You have just downloaded a file. You create a hash of the file and compare it to the hash posted on the website. The two hashes match.

What do you know about the file?

- Your copy is the same as the copy posted on the website.
- No one has read the file contents as it was downloaded.
- You can prove the source of the file.
- You will be the only one able to open the downloaded file.

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 it is assumed that the data is 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 9.9.
[All Questions SecPro2017_v6.exm HASHING_05]