Section Quiz

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 3/8/2022 6:47:23 pm • Time spent: 02:07

Score: 70% Passing Score: 80%

Question 1: ✔ Correct

A birthday attack focuses on which of the following?

- 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 produce the same message digest. This is also known as exploiting collision. If two different messages or files produce the same hashing digest, a collision has occurred.

REFERENCES

7.3.3 Hashing Facts

q_cryp_hash_birthday_01_secp7.question.fex

Question 2: ✕ Incorrect

An attacker is attempting to crack a system's password by matching the password hash to a hash in a large table of hashes he or she has.

Which type of attack is the attacker using?

- RIPEMD
- Cracking
- ~~Brute force~~
- Rainbow

EXPLANATION

A rainbow attack uses rainbow tables. A rainbow table is a table of passwords and their generated hashes. A hacker can use this table to try to match hashes instead of the actual password.

Cracking is the process of finding a password.

A brute force attack does not use a table of hashes.

RIPEMD is a family of cryptographic hash functions that was first developed in 1992 as part of the EU's RIPE project.

REFERENCES

7.3.3 Hashing Facts

q_cryp_hash_birthday_02_secp7.question.fex

Question 3: ✔ Correct

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

- High amplification
- Collision
- Birthday attack
- Hash value

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

7.3.3 Hashing Facts

q_cryp_hash_collision_secp7.question.fex

Question 4: ✔ Correct

Hashing algorithms are used to perform which of the following activities?

- Provide for non-repudiation.
- Provide a means for exchanging small amounts of data securely over a public network.
- Encrypt bulk data for communications exchange.
- ➡ 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 that are transmitted. The receiver performs the same action on the data received and compares the two message digests. If they are the same, 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 non-repudiation.

REFERENCES

- 7.1.5 Symmetric and Asymmetric Encryption Facts
- 7.2.5 Cryptographic Implementation Facts
- 7.3.1 Hashing
- 7.3.2 Hashing Algorithms
- 7.3.3 Hashing Facts
- 7.3.4 Using Hashes
- 7.3.5 Compare an MD5 Hash

q_cryp_hash_digest_secp7.question.fex

Question 5: ✔ Correct

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

- Hash
- Private key
- Symmetric encryption
- Asymmetric encryption

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

7.1.5 Symmetric and Asymmetric Encryption Facts

7.2.5 Cryptographic Implementation Facts

7.3.1 Hashing

7.3.2 Hashing Algorithms

7.3.3 Hashing Facts

7.3.4 Using Hashes

7.3.5 Compare an MD5 Hash

q_cryp_hash_hash_01_secp7.question.fex

Question 6: ✔ 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 are 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, 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

- 7.1.5 Symmetric and Asymmetric Encryption Facts
- 7.2.5 Cryptographic Implementation Facts
- 7.3.1 Hashing
- 7.3.2 Hashing Algorithms
- 7.3.3 Hashing Facts
- 7.3.4 Using Hashes
- 7.3.5 Compare an MD5 Hash

q_cryp_hash_hash_02_secp7.question.fex

Question 7: ✕ Incorrect

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

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

EXPLANATION

SHA-1 produces hash values of 160 bits.

MD5 and MD2 both produce hash values of 128 bits.

RIPEMD is a family of cryptographic hash functions that was first developed in 1992 as part of the EU's RIPE project.

REFERENCES

7.1.5 Symmetric and Asymmetric Encryption Facts

7.2.5 Cryptographic Implementation Facts

7.3.1 Hashing

7.3.2 Hashing Algorithms

7.3.3 Hashing Facts

7.3.4 Using Hashes

7.3.5 Compare an MD5 Hash

q_cryp_hash_hash_03_secp7.question.fex

Question 8: ✔ Correct

Which of the following is a message authentication code that allows a user to verify that a file or message is legitimate?

- RIPEMD
- HMAC
- SHA
- MD5

EXPLANATION

Hash-Based Message Authentication Code (HMAC) is a type of message authentication code. Like a digital signature, HMAC allows a user to verify that a file or message is legitimate.

SHA is a family of hashes that is used in many different security protocols.

MD5 was developed in 1991 and is no longer viable for security purposes.

RIPEMD is a family of cryptographic hash functions that was first developed in 1992 as part of the EU's RIPE project.

REFERENCES

7.3.3 Hashing Facts

q_cryp_hash_hmac_secp7.question.fex

Question 9: ✔ Correct

What is the process of adding random characters at the beginning or end of a password to generate a completely different hash called?

- Avalanche
- Collision
- Deterministic
- Salting

EXPLANATION

Salting is the process of adding random characters at the beginning or end of the password to generate a completely different hash. If a hacker intercepts the hash, he or she would need to also know which portion is the salt before beginning to crack the hash.

Deterministic is a characteristic of a hash function that means the same data always generates the same hash.

A collision is when two different pieces of data generate the same hash.

The avalanche effect states that changing any bit of data results in a completely different hash.

REFERENCES

7.3.3 Hashing Facts

11.7.2 Password Attack Facts

q_cryp_hash_salting_secp7.question.fex

Question 10: ✕ Incorrect

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

7.3.3 Hashing Facts

q_cryp_hash_weak_secp7.question.fex