NPTEL Online Certification Courses

Indian Institute of Technology Kharagpur

Course Name: ETHICAL HACKING

Assignment- Week 7

TYPE OF QUESTION: MCQ/MSQ/SA

Number of questions: 10 **Total mark: 10 x 1 = 10**

QUESTION 1:

Which of the following is/are **true** for Unkeyed hash function (Modification Detection Code)?

a. Unkeyed hash function is used to preserve integrity of message.

b. Unkeyed hash function is used to authenticate source of message.

c. Unkeyed hash function produces an output that depends only on the input data.

d. None of these.

Correct Answer: a, c

Detail Solution: Unkeyed hash function takes an input of variable length and converts it to a fixed-length output. It does not use any key, and thus the output only depends on the input data. Unkeyed hash function is used to preserve data integrity. It is impossible to figure out the sender of the message when we use Unkeyed hash function.

Thus the correct options are (a) and (c).

QUESTION 2:

Two messages M1 and M2 are fed to a hash function HASH to generate the hash values:

H1 = HASH (M1)

H2 = HASH (M2)

When do we say there is a collision?

a. H1 = H2.

b. M1 = M2.

c. H1 = HASH (H2).

d. None of these.

Correct Answer: a

Detail Solution: With respect to hashing, collision refers to the situation where more than one messages (here M1 and M2) map to the same hash value.

The correct option is (a).

QUESTION 3:

Which of the following corresponds to second preimage resistance in the context of hash functions?

a. Except of few hash values H, it should be difficult to find a message M1 such that HASH(M1) = H.
b. Given a message M1, it should be difficult to find another message M2 such that HASH(M1) = HASH(M2).
c. It should be difficult to find two messages M1 and M2 such that HASH(M1) = HASH(M2).
d. None of these.

Correct Answer: b

Detail Solution: When we use hash function then it is expected that it should be computationally infeasible to identify the input data; for this preimage resistance and collison rules are used.

The first preimage resistance is defined as: Except for few hash values H, it should be difficult to find a message M1 such that HASH(M1) = H. This means that for all pre-specified outputs, it should be computationally infeasible to find any input which hashes to that output.

The second preimage resistance is defined as: Given a message M1, it should be difficult to find another message M2 such that HASH(M1)=HASH(M2), which means it should be computationally infeasible to find any second input which has the same output as any specified input.

Collison resistance is defined as: It should be difficult to find two messages M1 and M2 such that HASH(M1)=HASH(M2). This means it should be difficult to find two messages with same hash values.

The properties of second preimage resistance and collision resistance may seem similar but the difference is that in the case of second preimage resistance, the attacker is given a message to

start with, but for collision resistance no message is given; it is simply up to the attacker to find any two messages with same hash values.

The correct option is (b).

QUESTION 4:

What is the message digest length of MD5 and SHA-1 hash functions?

a. 32-bit, 64-bit.
b. 64-bit, 128-bit.
c. 128-bit, 160-bit.
d. 128-bit, 256-bit.
e. None of these.

Correct Answer: c

Detail Solution: MD5 and SHA-1 hash function results in 128-bit and 160-bit hash values that is often termed as message digest.

The correct option is (c).

QUESTION 5:

Which of the following is/are not hash functions?

a. MD5
b. Triple-DES
c. SHA-1
d. RSA.

Correct Answer: b, d

Detail Solution: MD5 and SHA-1 are examples of hash function, while Triple-DES is a symmetric key encryption algorithm, and RSA is a public key encryption algorithm.

The correct options are (b) and (d).

QUESTION 6:

Hash functions are faster than symmetric and public key encryption?

a. True
b. False

Correct Answer: a

Detail Solution: Computation of hash function is the fastest. Computation of public-key encryption is the slowest. Symmetric-key encryption lies in between the two.

Hence, the correct option is (a).

QUESTION 7:

Which of the following is/are **false** for digital signature?

a. Digital signature is legally equivalent to hand-written signature.
b. In digital signature, signer uses his public key to sign.
c. Anybody having access to the signer's public key can verify the signature.
d. None of these.

Correct Answer: b

Detail Solution: Digital signature is an example of authentication where the signer uses his private key to sign any document, a receiver or anybody having the access of public key of the signer can identify the signer, digital signature is equivalent to hand written signature.

The correct option is (b).

QUESTION 8:

Which of the following statement(s) is/are **true**?

a. Secure Socket Layer (SSL) provides security to the data transferred between web browser and server.
b. SSL can be used for any network service running over TCP/IP.
c. SSL Handshake Protocol provides mutual authentication.
d. None of these.

Correct Answer: a, b, c

Detail Solution: SSL is used to provide secure channel for data transfer. It uses TCP to provide reliable end-to-end secure service and can be used for any network service running over TCP/IP. SSL is responsible for data security and integrity; it can also perform some other functionalities such as fragmentation and encryption. SSL Handshake Protocol is used to initial session between server and client and provides mutual authentication.

The correct options are (a), (b) and (c).

QUESTION 9:

Which of the following statement(s) is/are **true** for SSL Alert Protocol?

a. If the first byte is 1 then it indicates that this alert has no impact on the connection between sender and receiver.
b. If the fist byte is 1 then the SSL connection is terminated.
c. If the first byte is 2 then it indicates that this alert has no impact on the connection between sender and receiver.
d. If the first byte is 2 then the SSL connection is terminated.

Correct Answer: a, d

Detail Solution: SSL Alert protocol is used to send session messages associated with data exchange and functioning of the protocol. Each SSL alert message consists of two bytes. The first byte can be either 1 or 2. The value 1 indicates warning such as bad certificate, no certificate, certificate expired, unsupported certificate etc. This alert does not have any impact on the session. The value 2 indicates the fatal error such as handshake failure, incorrect MAC etc. which leads to connection termination. The second byte describes the error.

Thus the correct options are (a) and (d).

QUESTION 10:

Consider the following statements:

(i) SSL is designed to establish secure connection between two hosts.

(ii) s-HTTP is designed to send individual messages securely.

a. Only (i) is true
b. Only (ii) is true

c. Both (i) and (ii) are true
d. Both (i) and (ii) are false.

Correct Answer: c

Detail Solution: Secure HTTP is an extension of HTTP protocol that is used to send data securely over the web. The main difference between SSL and s-HTTP is that SSL is designed to establish a secure connection between two hosts whereas s-HTTP is designed to send individual messages securely.

The correct option is (c).

**********END*******