NPTEL Online Certification Courses

Indian Institute of Technology Kharagpur

Course Name: ETHICAL HACKING

Assignment- Week 6

TYPE OF QUESTION: MCQ/MSQ/SA

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

QUESTION 1:

Which of the following statement is **true** for Masquerade attack?

a. In this attack, an attacker passively captures a transaction and its reply.
b. In this attack, some portion of message is altered on its way.
c. In this attack, an attacker prevents access of resource to its legitimate users.
d. In this attack, the attacker pretends as a legitimate entity.
e. In this attack, the attacker analyzes the network traffic.

Correct Answer: d

Detail Solution: Analyzing the network traffic refers to passive attack. Masquerade is an active attack, which can be categorized in 4 categories. In Masquerade, one entity (attacker) pretends to be a different entity (legitimate). Replay involve passive capture of a transaction and subsequent replay. In modification, some portion of a message is altered on its way. Denial of service prevents access to resources.

Thus the correct option is (d).

QUESTION 2:

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

a. In private key encryption, separate keys are used by sender and receiver.
b. In private key encryption, a single key is used by sender and receiver.
c. In public key encryption, separate keys are used by sender and receiver.
d. In public key encryption, a single key is used by sender and receiver.

Correct Answer: b, c

Detail Solution: Encryption is the most important concept for network security, typically two types of encryptions are used. Private key: where the sender and receiver uses same key for

encryption/decryption of the message. Public key: where a separate key is used for encryption and decryption of the message.

Thus the true options are (b) and (c).

QUESTION 3:

Consider the following statement:
(i) In symmetric key cryptography, the security depends on secrecy of the key.
(ii) In symmetric key cryptography, the security depends on encryption/decryption algorithm.

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: a

Detail Solution: In symmetric key (private key) cryptography, the security of the data only depends on the secrecy of the key shared among sender and receiver, and not on the algorithm used for encryption and decryption.

Thus correct option is (a).

QUESTION 4:

25 parties want to exchange messages securely. The number of distinct key required by a symmetric key encryption algorithm and public key encryption technique like RSA will be _____ and _____ respectively.

a. 25 and 50
b. 50 and 50
c. 100 and 50
d. 300 and 25
e. 300 and 50

Correct Answer: e

Detail Solution: In symmetric encryption, every pair of communicating parties must have a separate key. For N parties, the number of keys will be ${}^{N}C_2$. For N = 25, ${}^{25}C_2 = 25 \times 24 / 2 = 300$.

In public-key or asymmetric encryption, every party is in possession of two keys, a public key and a private key. For N parties, the number of keys will be 2N. For N = 25, the number of distinct keys required will be 2 x 25 = 50.

Thus the correct option is (e).

QUESTION 5:

How will be the plaintext for the cipher text "LETTY CEIV" encrypted using a substitution cipher approach, where each letter is replaced by the k-th next letter. (Assumption: (i) the alphabets are wrapped around, i.e. Z is followed by A, (ii) each alphabets (A to Z) is assigned a number (1 to 26), (iii) the value of secrete key k is 4).

a. HAPPY YEAR
b. HAPPU YAER
c. HAPPY YEAR
d. None of this

Correct Answer: b

Detail Solution: k=4 indicates that for encryption, each letter is replaced by its 4^{th} following letter. If we decrypt the message we will get the plain text as HAPPU YAER.

Thus the correct option is (b).

QUESTION 6:

In data encryption standard (DES), longer plain text are processed in _____ bit blocks.

Correct Answer: 64

Detail Solution: In the DES algorithm, the key size is 56 bits, plaintext length is 64-bit. It is a block cipher; thus if the plain text are longer, then it is processed in 64-bit blocks.

QUESTION 7:

The effective key lengths used in AES encryption algorithms can be:

a. 64 bit
b. 128 bit
c. 192 bit
d. 256 bit
e. 512 bit

Correct Answer: b, c, d

Detail Solution: In AES the block length is limited to 128 bit, however the key length can be 128, 192 or 256 bit.

Thus the correct options are (b), (c) and (d).

QUESTION 8:

For decryption using public-key cryptography _____ is used.

a. Receiver's public key
b. Receiver's private key
c. Sender's public key
d. Sender's private key

Correct Answer: b

Detail Solution: If a sender A wants to carry out encryption on a message and send it to receiver B using public-key cryptography, A will encrypt the given message using B's public key, so that it can be correctly decrypted by the receiver B using B's private key.

Thus the correct option is (b).

QUESTION 9:

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

a. The security of RSA algorithm is dependent on prime factorization problem.
b. RSA algorithm is vulnerable to man-in-the middle attack.
c. Diffie-Hellman approach can be used for encryption/decryption of message.
d. Symmetric encryption approaches are faster than asymmetric encryption.
e. None of these.

Correct Answer: a, d

Detail solution: The security of the RSA algorithm depends on the complexity of factoring the product of two large prime numbers. It is not vulnerable to man-in the middle attack. Diffie-Hellman is used to exchange keys rather than encryption/decryption applications. Symmetric encryption/decryption is much faster than asymmetric encryption/decryption.

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

QUESTION 10:

Which of the following techniques **cannot** be used for message authentication?

a. Conventional encryption approach such as private key.
b. MD4
c. SHA-256
d. SHA-0
e. RIPEMD-128

Correct Answer: d

Detail Solution: For message authentication, conventional encryption approach, MD2, MD4, MD5, SHA-1, SHA-256, SHA-384, SHA512, RIPEMD-128 and RIPEMD-160 can be used. There is nothing called SHA-0.

Hence, the correct option is (d).

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