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 statements is **true** for Masquerade attack?

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

Correct Answer: c

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 (c).

QUESTION 2:

Which of the following is an example of passive security attack?

a. Traffic analysis
b. Replay
c. Modification
d. Denial of Service
e. None of these

Correct Answer: a

Detail Solution: Masquerade, replay, modification, denial of service all are active attacks. Snooping and traffic analysis comes under passive attacks.

Thus the correct option is (a).

QUESTION 3:

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

a. In symmetric key cryptography, separate keys are used by sender and receiver.
b. In symmetric key cryptography, a single key is used by sender and receiver.
c. In asymmetric key cryptography, separate keys are used by sender and receiver.
d. In asymmetric key cryptography, a single key is used by sender and receiver.

Correct Answer: b, c

Detail Solution: Encryption is the most important concept for network security, and typically two types of encryptions are used. Private key (symmetric): where the sender and receiver uses same key for encryption/decryption of the message. Public key (asymmetric): where a separate key is used for encryption and decryption of the message.

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

QUESTION 4:

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 the secrecy of the 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 secrecy of the algorithm used for encryption and decryption.

Thus correct option is (a).

QUESTION 5:

25 parties want to exchange messages securely using a private key encryption algorithm. The number of distinct key values required will be _____.

Correct Answer: 300

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, ${}^{15}C_2 = 25 \times 24 / 2 = 300$.

QUESTION 6:

Consider a cipher text "GVCTXSKVETLC" 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 alphabet (A to Z) is assigned a number (1 to 26).

(iii) The value of secret key k is 4.

What will be the plain text?

a. HAPPYNEWYEAR
b. CRYPTOGRAPHY
c. SECURENETWOR
d. CRYPTOGRAPHIC
e. None of these.

Correct Answer: b

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

Thus the correct option is (b).

QUESTION 7:

Consider a mono-alphabetic cipher with the following key value:

(A B W X E F S T I J O P M N K L Q R G H U V C D Y Z)

What will be the encrypted form of the message “ALPHABETIC” ?

a. APLTABEHIW
b. ALPHABETIC
c. WXLTABEHIC
d. None of these.

Correct Answer: a

Detail Solution: According to the specified mapping the encrypted message will be APLTABEHIW.

Hence, the correct option is (a).

QUESTION 8:

If a sender A wants to carry out encryption on a message and send it to receiver B using public-key cryptography. Which of the following key will be used for decryption at receiver end B?

a. A’s public key
b. A’s private key
c. B’s public key
d. B’s private key

Correct Answer: d

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 (d).

QUESTION 9:

The effective key length use in AES encryption algorithm can be:

a. 64 bit
b. 128 bit
c. 192 bit
d. 256 bit
e. 513 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 and 256 bits.

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

QUESTION 10:

50 parties want to exchange messages securely using some public key encryption technique like RSA. The number of distinct key values required will be _____.

Correct Answer: 100

Detail Solution: 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 = 50, the number of distinct keys required will be 50 x 2 = 100.

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