NPTEL Online Certification Courses

Indian Institute of Technology Kharagpur

Course Name: ETHICAL HACKING

Assignment- Week 8

TYPE OF QUESTION: MCQ/MSQ/SA

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

QUESTION 1:

Which of the following are examples of steganography?

a. Hiding some text information within an image file.
b. Hiding some text information within an audio clip.
c. Hiding some secret information within an executable file.
d. Encrypting an image file so that only the intended recipient can view it.

Correct Answer: a, b, c

Detail Solution: Steganography refers to a set of methods where some information is hidden within some other file (like image, audio, video, executable, etc.). It does not involve encryption for secure access. The correct options are (a), (b) and (c).

QUESTION 2:

Which of the following statements correctly represents the term steganography?

a. Encrypting some information such that it will not be legible to an unauthorized person.
b. A low-cost alternative to encryption and decryption.
c. Secure way of communicating without sharing any key.
d. None of these.

Correct Answer: d

Detail Solution: Steganography refers to a set of methods where some information is hidden within some other file (like image, audio, video, etc.). It does not concern encryption or decryption, and also secure communication. The correct option is (d).

QUESTION 3:

Which of the following correspond to behavioral biometrics?

a. Biometrics that relate to human behavior.
b. Biometrics that relate to human body.
c. Biometrics that rely on the use of a powerful computer system.
d. None of these

Correct Answer: a

Detail Solution: Behavioral biometrics refers to biometrics that relate to human behavior, like signature (hand and finger movement) and Gait (walking style). However, fingerprint, Iris scan and Retina scan are properties of the human body and not dependent on the behavior. It does not rely on computing power. Hence, the correct option is (a).

QUESTION 4:

Consider a gray-level image of size 1000 x 1000, where each pixel is stored in 8-bits (representing a gray scale). How many bits of information can be hidden in the image by using LSB steganography technique? Assume 1K = 1000, and 1M = 1,000,000.

a. 100 Kbits
b. 500 Kbits
c. 1 Mbits
d. None of these.

Correct Answer: c

Detail Solution: Each pixel consists 1 byte, and hence 1 bit of information can be stored in each pixel. The number of bits of hidden information that can be stored in the whole image will be:

1000 x 1000 x 1 bits = 1,000,000 bits = 1 Mbits

The correct answer is (c).

QUESTION 5:

What is denial-of-service attack?

a. An attack on a system whereby stored files get modified or deleted.
b. An attack that destroys users information from a system.
c. An attack that destroys the stored password information in a system.
d. None of these.

Correct Answer: d

Detail Solution: In a denial-of-service attack, some service running on a victim machine is rendered inaccessible from legitimate users of the service. The correct option is (d).

QUESTION 6:

Which of the following attacks refer to the situation where an attacker gains entry into the victim machine (or spoofs the IP address) and then sends a ping request to a broadcast address?

a. SYN flooding attack.
b. Smurf denial-of-service attack.
c. DNS spoofing attack.
d. None of these.

Correct Answer: b

Detail Solution: In the Smurf DoS attack, the victim gains entry into the victim machine (or spoofs the IP address) and then sends a ping request to a broadcast address. A large number of ping response packets are received, which can overload the victim. The correct option is (b).

QUESTION 7:

Which of the following attacks rely on some vulnerability in the TCP connection establishment phase?

a. SYN flooding attack.
b. DNS spoofing attack.
c. Smurf DoS attack.
d. None of these.

Correct Answer: a

Detail Solution: The SYN flooding attack tries to exploit a weakness in the TCP connection establishment phase. The attacker floods the victim machine with a large number of TCP connection requests, each of which is left as half-open (i.e. the third packet in 3-way handshake is not sent). Each connection request will take up some resources on the victim machine (e.g. port number, buffer space, etc.), and ultimately genuine requests will not get processed.

The correct option is (a).

QUESTION 8:

Which of the following is/are true for Botnet?

a. A Botnet refers to a host connected to the Internet that is under control of the attacker.
b. A Botnet host runs a number of bots that are repetitive code segments with some malicious intent.
c. It relies on IP spoofing to mount attacks.
d. All of these.

Correct Answer: a, b

Detail Solution: Many of the network-based attacks (DoS and DDoS in particular) are based on so-called Botnets. A Botnet refers to a host connected to the Internet that is under the control of the attacker. The Botnet host runs a number of "bots" that are repetitive code segments with some malicious intent, typically used to mount an attack. It does not spread from one machine to another.

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

QUESTION 9:

Which of the following is true for iterative name resolution?

a. A host may have to send multiple DNS requests to several DNS servers.
b. A host sends a single DNS request to its next higher-level DNS server.
c. Name resolution happens iteratively within the host itself without sending any DNS request messages.
d. None of these.

Correct Answer: a

Detail Solution: The DNS server receives a DNS request from a host containing a domain name, and it returns the corresponding IP address. In iterative name resolution, in response to a DNS request, the DNS server sends back a response specifying the next DNS server to send the query. In this way, the host may have to send a number of DNS requests before it gets resolved. In recursive name resolution, the host sends a DNS request to the next higher level DNS server. The DNS server in turn recursively forwards the request to its next higher-level DNS server, and so on, until the request gets resolved. The final reply gets back to the host. Here, the host sends a single DNS request.

Thus, option (a) is true.

QUESTION 10:

What is the full form of PGP?

a. Packet Group Protocol
b. Port Group Protocol
c. Pretty Good Privacy
d. All of these.

Correct Answer: c

Detail Solution: PGP stands for Pretty Good Privacy. The correct option is (c).

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