## 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 statements correctly represents the term steganography?

a. Encrypting information so that it will not be legible to an unauthorized person.
b. Hiding information within some cover media file.
c. Secure way of communicating without sharing any key.
d. None of these.

**Correct Answer: b**

**Detail Solution:** Steganography refers to a set of methods where some information is hidden within some other file (like image, audio, video, etc.). The correct option is (b).

---

**QUESTION 2:**

Which of the following is/are not instances of behavioral biometrics?

a. Fingerprint
b. Signature
c. Gait
d. Iris scan
e. Retina scan

**Correct Answer: a, d, e**

**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. Hence, the correct options are (a), (d) and (e).

---

**QUESTION 3:**

Consider a color image of size 2000 x 2000, where each pixel is stored in 24-bits (containing red, green and blue components as 8-bits each). How many bytes of information can be hidden in the image by using LSB steganography technique? *Assume that only the least significant bit in each 8-bit color component is modified*.

a. 12,000,000 bytes
b. 8,000,000 bytes
c. 7,500,000 bytes
d. None of these.

**Correct Answer: d**

**Detail Solution:** Each pixel consists of 24 bits or 3 bytes, and hence 3 bits 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:

2000 x 2000 x 3 bits = 2000 x 2000 x 3 / 8 bytes = 15, 00,000 bytes.

The correct answer is (d).

---

**QUESTION 4:**

Which of the following statements is/are true in biometric systems?

a. For authentication application, a user template is compared against all possible templates stored in the database.
b. For verification / identification application, a user template is compared against a specific single template stored in the database.
c. They can provide 100% accuracy in security applications.
d. None of these.

**Correct Answer: d**

**Detail Solution:** When biometric is used for authenticating a known person, his/her biometric template is compared against the corresponding template stored in the database.

However, for identifying a person whose id is not known, his/her biometric template has to be compared with all the templates stored in the database.

None of the biometric systems can provide 100% accuracy.

Thus, option (d) is true.

**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 prevents legitimate users from accessing some service.
c. An attack that destroys the stored password information in a system.
d. None of these.

**Correct Answer: b**

**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 (b).

**QUESTION 6:**

How does a Smurf denial-of-service attack work?

a. A ping request is sent from the victim machine to a broadcast address.
b. The attacker sends a large number of ICMP ping messages to the victim machine.
c. It exploits a vulnerability in the TCP connection establishment process.
d. None of these.

**Correct Answer: a**

**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 (a).

**QUESTION 7:**

Which of the following attacks rely on the accumulation of TCP half-open connections on the server?

a. Ping of death attack.
b. SYN flooding attack.
c. Smurf attack.
d. None of these.

**Correct Answer: b**

**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 (b).

---

**QUESTION 8:**

Which of the following is/are true for Botnet?

a. A large number of Botnets are often used to attack a victim machine.
b. It is a malicious software that spreads from one machine to another.
c. It can be used to mount distributed denial-of-service attack.
d. All of these.

**Correct Answer: a, c**

**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 (c).

---

**QUESTION 9:**

What is meant by recursive 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 recursively within the host itself.
d. All of these.

**Correct Answer: b**

**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 (b) is true.

## QUESTION 10:

How does PGP provide security in email transmission?

a. It provides authentication.
b. It provides non-repudiation.
c. It ensures availability.
d. All of these.

**Correct Answer: a**

**Detail Solution:** PGP provides a set of services for secure email transmission. It provides services like authentication and confidentiality, using a combination of hash functions and encryption techniques. However, it does not address availability or non-repudiation issues. The correct option is (a).

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