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:

Consider the following statements:
(i) Steganography refers to a set of methods to hide some secrete information in an audio/image/executable files.
(ii) Steganography and digital watermarking shares same operational and functional behaviors.

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: Steganography refers to a set of methods where some information is hidden within some other file (like image, audio, video, executable, etc.). Digital watermarking embeds copyright, ownership, license and similar information in a medium such as audio, video, image etc. Digital watermarking is different from steganography only in the intent of hiding. They share same operational and functional behavior.

The correct option is (c).

QUESTION 2:

Consider a gray-level image of size 2000 x 2000, where each pixel is stored in 24-bits (containing red, green, and blue components as 8-bit 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*).

Correct Answer: 1500000

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.

QUESTION 3:

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

a. Biometrics refers to an automated method for hiding information in a media like audio, video, image etc.
b. Biometrics refers to embedding copyright, ownership, license and similar information in a medium such as audio, video, image etc.
c. Biometrics refers to an automated method for recognizing individuals based on measurable biological and behavioral characteristics.
d. None of these.

Correct Answer: c

Detail Solution: Hiding information is referred to as steganography, hiding information such as copyright is known as digital watermarking. Biometrics refers to an automated method for recognizing individuals based on measurable biological and behavioral characteristics.

The correct option is (c).

QUESTION 4:

Which of the following is/are example(s) of behaviour biometric?

a. Retina scan
b. Fingerprint recognition
c. Facial recognition
d. None of these

Correct Answer: d

Detail Solution: Physical biometrics refers to physiological features on the human body such as a fingerprint, retina scan whereas behavioral biometrics analyzes parameters such as keystroke pattern, typing speed, mouse movement, signature styles etc.

The correct option is (d).

QUESTION 5:

Which of the following statement(s) 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 application, a user template is compared against a specific single template stored in the database.
c. Biometric systems 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 6:

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 7:

In which of the following denial-of-service attacks, the attacker attempts to crash/freeze target computer/service by sending oversized packet in simple ping command?

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

Correct Answer: c

Detail Solution: In the ping-of-death attack, attacker uses larger than maximum packet size (65536) ping packets that are broken into smaller segments and resembled at receiver end. Systems that are unable to handle such abnormalities either crash or reboot.

The correct option is (c).

QUESTION 8:

Which of the following statement(s) is/are true for HTTP Flood attack?

a. It is a type of Distributed-Denial-of-Service (DDoS) attack.
b. It overwhelms a target server by accumulating large number of TCP half-open connections.
c. It overwhelms a target server using oversized ping packets.
d. It overwhelms a target server with HTTP request.
e. None of these.

Correct Answer: a, d

Detail Solution: HTTP Flood attack is a type DDoS attack which is designed to overwhelm the target server with HTTP requests. Once the target is saturated with HTTP requests, it does not respond to HTTP request from legitimate users.

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

QUESTION 9:

Which of the following approach can be used to mitigate HTTP flood attack?

a. Use captcha test.
b. Use JavaScript computational challenge.
c. Use web application firewall.
d. Block ping requests.
e. Block TCP connections.
f. None of these.

Correct Answer: a, b, c

Detail Solution: To protect web server from HTTP flood attack a simple method can be giving challenge to the requesting machine in order to test whether it is a bot or a legitimate user. For this we can use captcha test or simple JavaScript computational challenge.

The other way to mitigate HTTP flood attack is to use web application firewall that can identify an authentic source of traffic and selectively block all malicious traffic.

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

QUESTION 10:

Which of the following is true for 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 the correct option is (b).

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