

Unit 8 - Week 6

Course outline

How to access the portal

Week 0 Assignment 0

Week 1

Week 2

Week 3

Week 4

Week 5

Week 6

Lecture 28: Security categories

Lecture 29: Security terminologies

Lecture 30: Digital signature

Lecture 31: Protocols for security: TLS

Lecture 32: Impact of security protocol on server performance

Week 6: Lecture Material

Quiz : Assignment 6

Feedback For Week 6

Week 7

Week 8

Week 9

Week 10

Week 11

Week 12

Download Videos

Assignment Solution

Assignment 6

The due date for submitting this assignment has passed.

Due on 2019-09-11, 23:59 IST.

As per our records you have not submitted this assignment.

1) Protecting the content of messages or data transmitted over the Internet from the unauthorized people is known as 2 points

- a. Nonrepudiation
- b. Integrity
- c. Authentication
- d. Confidentiality

- a
 b
 c
 d

No, the answer is incorrect.

Score: 0

Accepted Answers:

d

2) Hash function is used for: 2 points

- a. Encryption and decryption
- b. Decryption and authentication
- c. Data integrity and decryption
- d. Authentication and data integrity

- a
 b
 c
 d

No, the answer is incorrect.

Score: 0

Accepted Answers:

d

3) If the following information is given about a web server then what will be its throughput? 2 points

- Average size of a file requested by the client = 16,384 bytes
 - Average CPU time for accessing a file at the server when secure connection is not required = 0.002 sec
 - Average time for a disk access = 0.02 sec
 - Average Network Delay = 0.001737 sec
- a. 25 requests per second
 - b. 50 requests per second
 - c. 75 requests per second
 - d. 100 requests per second

- a
 b
 c
 d

No, the answer is incorrect.

Score: 0

Accepted Answers:

b

4) Which of the following is not an activity under TLS handshake procedure? 2 points

- a. Negotiation of cryptographic and compression algorithms
- b. Exchange of secrets through public key operations
- c. Secret key transfer using symmetric key cryptography
- d. Generation of secrete key

- a
 b
 c
 d

No, the answer is incorrect.

Score: 0

Accepted Answers:

c

5) The difference between Sniffing and IP Spoofing is? 2 points

- a. In the latter the attacker simply reads the message from data link frames and in the former case he/she modifies the destination IP address
- b. In both the cases the attacker simply reads the message from data link frames
- c. In the former the attacker simply reads the message from data link frames and in the latter case he/she modifies the destination IP address
- d. In both the cases the attacker modifies the destination IP address in the data link frames

- a
 b
 c
 d

No, the answer is incorrect.

Score: 0

Accepted Answers:

c

6) The encrypted text in Cryptography is called 2 points

- a. Plaintext
- b. Ciphertext
- c. Both a and b
- d. Neither (a) nor (b)

- a
 b
 c
 d

No, the answer is incorrect.

Score: 0

Accepted Answers:

b

7) Which of the following security issues cannot be resolved using digital signature? 2 points

- a. Confidentiality
- b. Integrity
- c. Non-repudiation
- d. Authentication

- a
 b
 c
 d

No, the answer is incorrect.

Score: 0

Accepted Answers:

a

8) Which of the following protocol is responsible for making a persistent connection between hosts during data transmission? 2 points

- a. Transmission Control Protocol (TCP)
- b. User Datagram Protocol (UDP)
- c. Broader Gateway Protocol (BGP)
- d. None of above

- a
 b
 c
 d

No, the answer is incorrect.

Score: 0

Accepted Answers:

a

9) Which of the following is independent malicious program that need not have any host program? 2 points

- a. Virus
- b. Worm
- c. Trap doors
- d. Trojan horse

- a
 b
 c
 d

No, the answer is incorrect.

Score: 0

Accepted Answers:

b

10) Which protocols can be used for the session key exchange and bulk data transfer in TLS protocol? 2 points

- a. DES followed by RSA
- b. DES followed by DES
- c. RSA followed by DES
- d. RSA followed by RSA

- a
 b
 c
 d

No, the answer is incorrect.

Score: 0

Accepted Answers:

c