CSS Quiz and Course Exit Survey 2020-21

Total points 10/10

The respondent's email (**19313063prathamesh@viva-technology.org**) was recorded on submission of this form.

CSS 2020-21 0 of 0 points

Name *

Prathamesh Sadashiv Parab

Roll No. *

38

CSS 2020-21 Quiz 10 of 10 points

10.The purpose of a firewall on computer networks is to * 1/1

- ○ Prevent computers from overheating
- ◉ Prevent unwanted network connections from being made
- ○ Allow more than 4 computers to share the same Internet connection
- ○ Allow pictures and video to be downloaded from a camera to a computer

4.The DES algorithm has a key length of * 1/1

- ○ 128 Bits
- ○ 32 Bits
- ◉ 64 Bits
- ○ 16 Bits

8. _____ allows administrators to define and limit the resources and operations that a user can access. * 1/1

- ○ Access
- ○ Authentication
- ○ Authorization
- ◉ All of the mentioned

6.What is the PGP stand for? * 1/1

- ○ Permuted Gap Permission
- ○ Permuted Great Privacy
- ○ Pretty Good Permission
- ◉ None of the mentioned

7.For a client-server authentication, the client requests from the KDC a _____ for access to a specific asset. * 1/1

- (◉) ticket
- ( ) local
- ( ) token
- ( ) user

5.Which one of the following is not a public key distribution means? * 1/1

- ( ) Public-Key Certificates
- (◉) Hashing Certificates
- ( ) Publicly available directories
- ( ) Public-Key authority

2.An encryption scheme is unconditionally secure if the ciphertext generated does not contain enough information to determine uniquely the corresponding plaintext, no matter how much cipher text is available. * 1/1

- (◉) True
- ( ) False

1.If the sender and receiver use different keys, the system is referred to as conventional cipher system. * 1/1

- ○ True
- ◉ False

9.What does SSL stand for? * 1/1

- ◉ Secure Socket Layer
- ○ Special Security License
- ○ Secure Space Layer
- ○ Straight Socket Loop

3.The Data Encryption Standard (DES) and It's Strength". DES follows * 1/1

- ○ Hash Algorithm
- ○ Caesars Cipher
- ◉ Feistel Cipher Structure
- ○ SP Networks

CSS 20-21 : Course Exit Survey Theory 0 of 0 points

3 HIGH 2 MEDIUM 1 LOW

CO6: Analyze and apply system security concept to recognize malicious code. *

1	2	3
○	○	◎

CO4: Apply different digital signature algorithms to achieve authentication and design secure applications *

1	2	3
○	○	◎

CO5: Understand network security basics, analyze different attacks on networks and evaluate the performance of firewalls and security protocols *

1	2	3
○	○	◎

CO1. Understand system security goals and concepts, classical encryption techniques *

1	2	3
○	○	◎

CO2: Compare and apply different encryption and decryption techniques to solve problems related to confidentiality and authentication *

1	2	3
○	○	◎

CO3: Apply the knowledge of cryptographic checksums and evaluate the performance of different message digest algorithms for verifying the integrity of varying message sizes. *

1	2	3
○	○	◎

SSL 20-21: Course Exit Survey LAB 0 of 0 points

3 HIGH 2 MEDIUM 1 LOW

CO5: To explore and use tools like sniffers, port scanners and other related tools for analyzing packets in a network *

1	2	3
○	○	◎

CO1. To be able to apply the knowledge of symmetric cryptography to implement simple ciphers. *

1	2	3
○	○	◎

CO2: To be able to analyze and implement public key algorithms like RSA and El Gamal. *

1	2	3
○	○	◎

CO6: To be able to set up firewalls and intrusion detection systems using open source technologies and to explore email security *

1	2	3
○	○	◎

CO3: To analyze and evaluate performance of hashing algorithms. *

1	2	3
○	○	◎

CO7: To be able to explore various attacks like buffer-overflow, and web-application attacks. *

1	2	3
○	○	◎

CO4: To explore the different network reconnaissance tools to gather information about networks. *

1	2	3
○	○	◉