NSS Quiz-1 (01/03/2023)

Each question is of 1 mark.

The respondent's email (**u19cs012@coed.svnit.ac.in**) was recorded on submission of this form.

✓ Block size of AES is :

○ 64

● 128 ✓

○ 259

○ 512

Identify the incorrect statement(s) for SSL/TLS.

☑ TLS protocol sits below the TCP layer and above the IP layer in the networking layers stack.

☑ SSLv3 and TLS protocol have similar architecture.

☑ SSL Provides high security as compared to TLS

□ SSL suffers from high latency than TLS.

✗ Match the following.

(a) Access control lists	(a) decomposed by column
(b) Capability tickets	(b) decomposed by row

(a)->(a), (b)->(b) ✗

✕ Identify the correct statemet(s)

a) In transport mode, only the payload of the IP packet is encrypted and/or authenticated.

b) Tunnel mode provides protection to the entire IP packet.

c) In transport mode, a new IP header is associated with original IP packet.

d) IPsec AH offers both encryption as well as authentication.

(a) & (b) ✕

✓ Verification and Identification for biometric systems are same.

(a) True

(b) False

○ a

● b ✓

✓ Find Inverse of 49 in GF(37)

○ -3

○ 3

● 34 ✓

○ 1

✗ IPsec works above the _______ and below the ______ layer of the networking layers stack.
a) Transport, Data Link
b) Data Link, Transport
c) Transport, Application
d) Network, Transport

○ a

○ b

● c ✗

○ d

✓ Find out the greatest common divisor GCD of 96256 and 432 :

○ (a) 8

● (b) 16 ✓

○ (c) 4

○ (d) 12

✓ A _________ is a sequential segment of the memory location that is allocated for containing some data such as a character string or an array of integers.

○ Stack

● Buffer ✓

○ Queue

○ External Storage

✓ ____ is a computer crime in which a criminal breaks into a computer system for exploring details of information etc.

○ Phishing

○ Eavesdropping

○ Spoofing

● Hacking ✓

✗ During TLS handshaking, each entity changes its side of connection into secure state by sending __________ message.

○ ChangeCipherSpec

○ Server_Key_Change

○ Client_Key_Exchange

● Server_hello_done ✗

✓ HTTPS is used to implement secure communication between a Web browser and a Web server using ____ port.

443 ✓

✓ Select correct statement/statements :

Cryptanalysis -

○ rely on nature of the algorithm

○ some knowledge of plaintext characteristics

○ even some sample plaintext-ciphertext pairs

○ exploits characteristics of algorithm to deduce specific plaintext or key

● All of the above ✓

✓ In _________ attack, the victim unknowingly remains logged into a web service.

○ SSL Stripping

● TLS truncation ✓

○ SSL Hijacking

○ PODDLE attack

✓ Level 3 in Assurance Level for Risk assessment is :

(a) little confidence

(b) some confidence

(c) High confidence

(d) Very high confidence

○ A

○ B

● C ✓

○ D

✗ Digital Envelops uses concepts of :

(a) Symmetric Key Cryptography

(b) Asymmetric Key Cryptography

(c) Both

● a ✗

○ b

○ C

✓ Buffer-overflow may remain as a bug in apps if _________ are not done fully.

○ boundary hacks

○ memory checks

● boundary checks ✓

○ buffer checks

✗ Bloom filter based password checking comes under the category of :

(a) user education

(b) computer-generated passwords

(c) reactive password checking

(d) proactive password checking

○ A

○ b

● c ✗

○ d

In a typical Internet E-Mail architecture, the communication between two Message Transfer Agents(MTA) is done by ________ protocol whereas communication between the Message Store (MS) and Message User Agent (MUA) is done by ____________ .

● SMTP, IMAP

○ IMAP, SMTP

○ IMAP, POP

○ SMTP, SMTP

Identify the correct statement(s) for the clear-singed function supported by S/MIME. (Multiple select)

□ a) The original content is encrypted.

☑ A digital signature of the content is formed.

☑ A recipient without S/MIME capability can view the

□ A recipient without S/MIME capability can verify the

✗

Which statement is false with respect to the need for salt value in password?

(a) Prevents duplicate passwords from being visible in the password file

(b) Decrease the difficulty of offline dictionary attacks

(c) Nearly impossible to tell if a person used the same password on multiple systems

(d) None

○ a

○ b

● c ✗

○ d

✓ In which of the following attack(s), the attacker tricks a web server into negotiating connections with the older version of TLS/SSL.

☑ PODDLE attack ✓

☑ Freak attack ✓

□ SSL Hijacking attack

□ SSL Stripping

✓ 1)Under __________ , the attacker creates and sends an email with the modified sender’s address

○ Email Spamming

○ Email Jamming

● Email Spoofing ✓

○ Email warm

This form was created inside of Sardar Vallabhbhai National Institute of Technology, Surat.

Google Forms