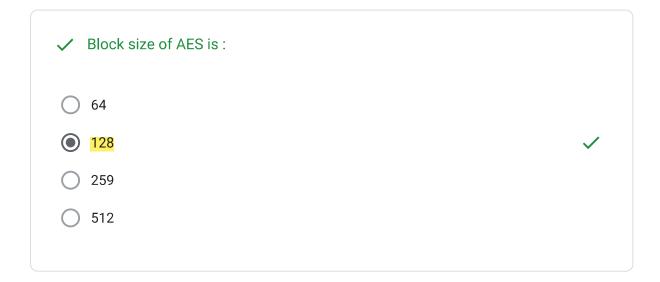
NSS Quiz-1 (01/03/2023)

Each question is of 1 mark.

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



- TLS protocol sits below the TCP layer and above the IP layer in the networking layers stack.
- SSLv3 and TLS protocol have similar architecture.

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

- SSL Provides high security as compared to TLS
- SSL suffers from high latency than TLS.

X Match the following.

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

(a)->(a), (b)->(b)

X

	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.		
	d) if sec Air offers both encryption as well as authentication.		
<u>(a)</u>	& (b)	×	
✓	Verification and Identification for biometric systems are same. (a) True (b) False		
C) a		
•) b	~	
~	Find Inverse of 49 in GF(37)		
) -3		
C) 3		
() () () () () () () () () ()) 3) <mark>3</mark> 4	✓	

 IPsec works above the and below the the networking layers stack. a) Transport, Data Link b) Data Link, Transport c) Transport, Application d) Network, Transport 	layer of
а	
O b	
	×
O d	
 Find out the greatest common divisor GCD of 96256 are (a) 8 (b) 16 (c) 4 (d) 12 	nd 432 :
✓ A is a sequential segment of the memory logarity for containing some data such as a character string or	
○ Stack	
Buffer	~
Queue	
External Storage	

	is a computer crime in which a criminal breaks into a computer sy for exploring details of information etc.	/stem
0	Phishing	
0	Eavesdropping	
0	Spoofing	
•	Hacking	✓
0	ChangeCipherSpec	
\cup	ChangeCipherSpec	
\bigcirc	Server Key Change	
0	Server_Key_Change Client_Key_Exchange	
	Server_Key_Change Client_Key_Exchange Server_hello_done	×
	Client_Key_Exchange	×

✓ 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	
O PODDLE attack	

✓ Level 3 in Assurance Level for Risk assessment is:	
(a) little confidence	
(b) some confidence	
(c) High confidence(d) Very high confidence	
O A	
ОВ	
	✓
O D	
★ Digital Envelops uses concepts of :	
(a) Symmetric Key Cryptography	
(b) Asymmetric Key Cryptography	
(c) Both	
а	×
O b	
○ ^C	

✓ Buffer-overflow may remain as a bug in apps if are not dor	ne fully.
oboundary hacks	
memory checks	
boundary checks	✓
buffer checks	
 Bloom filter based password checking comes under the category of the company of the category of t	
(b) computer-generated passwords	
(c) reactive password checking(d) proactive password checking	
O A	
O 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 passwore	d?
	(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 multip systems	ole
	(d) None	
0	a	
\bigcirc	b	
•	c	×
0	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 SpammingEmail JammingEmail Spoofing	✓
Email warm	

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

Google Forms