Reg. No			
2108.1.0		 	

B.Tech DEGREE EXAMINATION, DECEMBER 2023

Sixth & Seventh Semester

18CSE354T - NETWORK SECURITY

(For the candidates admitted during the academic year 2020 - 2021 & 2021 - 2022)

Note:

i. Part - A should be answered in OMR sheet within first 40 minutes and OMR sheet should be handed over to hall invigilator at the end of 40th minute.

ı. Pa	rt - B and Part - C should be answered in al				
Time	2: 3 Hours	N	Max. N	Aarks	: 100
	$PART - A (20 \times 1 = Answer all Que$		Mark	s BL	CO
1.	The purpose of is to make the cipher text as complex as possible	e relation between the encryption key and	1	2	1
	(A) Diffusion (C) Collision	(B) Confusion (D) Ciphering			
2.	Which one of the following statements is in (A) Hub operates on physical layer	ncorrect? (B) Switch operates on physical and data link layer	1	1	1
	(C) Router operates on physical, data link and network layer	(D) Router operates on data link layer only			
3.	Which of the following statement is correct (A) External attacker only has access to the hosts in the DMZ and not to any other internal networks	t with respect to DMZ? (B) Stateful packet filtering is done at DMZ	1	2	1
	(C) Load balancing is done at DMZ	(D) DMZ means Dedicated Military Zone			
4.	An attack that uses a fake identity to gain (A) Masquerade (C) Fabrication	unauthorized access is called (B) Alteration (D) Replay attack	1	1	1
5.	(A) AH (C) ESP	or the tunnel mode. (B) SSL (D) PGP	1	1	2
6.	Internet Key Exchange (IKE) uses (A) Oakley (C) ISAKMP	(B) SKEME (D) Oakley, SKEME and ISAKMP	1	1	2
7.	Which one of the statements is incorrect v of IPSec (A) SA is one-way sender-recipient relationship (C) SA is uniquely identified by SPI,	(B) SA determines the cryptographic algorithm used for processing the packets (D) SA will not help to avoid the replay	1	2	2
8.	Destination IP, flag The IPsec header includes a field known a	attack as the which identifies the security	1	1	2
	association in SA database (A) State index (C) Sequence index	(B) Security parameter index (D) Flag			

9.	The function of mail Transfer Agent (MTA		1	1	3	
	(A) help in reading the emails(C) detect the emails carrying the virus	(B) resolve the mail ID(D) receive and deliver the messages				
10	Which of the following is not a secured ma		1	2	3	
	(A) POP3	(B) SMTP	•	_	3	
	(C) Mail using PGP	(D) S/MIME				
11.	PGP provides in E-Mail		1	2	3	
	(A) Privacy	(B) Privacy and integrity				
	(C) Privacy, Integrity and	(D) Privacy, Integrity, Authentication				
	Authentication	and Access Control				
12.	As an alternate to the use of RSA for key e		1	2	3	
	(A) DES (C) ElGamal	(B) AES				
		(D) IDEA				
13.	SSL works between and	(D) W 1 1	1	2	4	
	(A) Web browser, Web server(C) Web server, application server	(B) Web browser, application server				
		(D) Application server, database server				
14.	In TLS, padding can be upto a maximum o		1	1	4	
	(A) 63 bytes (C) 255 bytes	(B) 127 bytes				
1.5		(D) 511 bytes				
15.	Which of the following is true about Public		1	2	4	
	(A) PKI is a combination of digital certificates, public-key	(B) PKI uses two-way symmetric key				
	cryptography, and certificate	encryption with digital certificates, and Certificate Authority.				
	authorities that provide enterprise-	and Certificate Authority.				
	wide security.					
	(C) PKI uses private and public keys	(D) PKI uses CHAP authentication				
	but does not use digital certificates					
16.	In SET protocol a customer encrypts credit	card number using	1	2	4	
	(A) his private key	(B) bank's public key				
	(C) bank's private key	(D) merchant's public key				
17.	Which of the following usually stores all us		- 1	1	5	
	(A) VLR	(B) HLR				
	(C) CMR	(D) SIM				
18.	Point out the correct statement.		1	2	5	
	(A) Parameterized data cannot be	(B) Procedure that constructs SQL				
	manipulated by a skilled and determined attacker	statements should be reviewed for				
	(C) The primary form of SQL injection	injection vulnerabilities (D) SQL injection is an attack in which				
	consists of indirect insertion of code	redundant code is inserted into				
		strings that are later passed to an				
		instance of SQL Server				
19.	Which of the following is a Wireless traffic		1	1	5	
	(A) Maltego	(B) BurpSuit		1	_	
	(C) Nessus	(D) Wireshark				
20.	Buffer-overflow may remain as a bug in app	os if are not done fully.	1	1	5	
	(A) Boundary hacks	(B) Memory checks			_	
	(C) Boundary checks	(D) Buffer checks				
	$PART - B (5 \times 4 = 20)$	0 Marks)	Marks	BL	СО	
	Answer any 5 Que					

Page 2 of 3

21.	Describe phishing attack and suggest a method to avoid it		2	1
22.	Demonstrate how the IP address Spoofing is done by an attacker		2	1
23.	Identify the various types of services provided by the IPSec and explain anyone in detail	4	1	2
24.	Compare the tunnel mode and transport mode of IPSec with neat diagram	4	4	2
25.	Differentiate PGP and S/MIME	4	3	3
26.	Analyze the primary need of public key infrastructure (PKI). Show how it is implemented	4	2	4
27.	Compare the WEP and WPA.	4	4	5
	PART - C ($5 \times 12 = 60$ Marks) Answer all Questions	Mark	ks BL	CO
28.	(a) Explain how the application proxy firewall protects a network from the attackers with neat diagram and compare application proxy firewall with other firewalls.	12	2	1
	(OR) (b) Discuss Signature-based IDS and Policy-based IDS with a neat diagram.			
29.	(a) Draw the Authentication header (AH) and state the purpose of each field of authentication header. Explain how it provides security to the IP header. (OR)	12	2	2
	(b) State the importance of IKE and describe the Phases of IKE.			
30.	(a) Discuss the step taken by PGP to create a secure e-mail at the sender side and receiver side with neat diagram.	12	1	3
	(OR) (b) Identify the services provided by PGP. Suggest and explain the mechanism or the algorithm used for these services.			
31.	(a) Show the sequence of message exchange used in SSL handshake for establishing the new session between client and server. (OR)	12	2	4
	(b) Describe how dual signature improves the security in SET with neat diagram.			
32.	(a) Elaborate how the authentication and key agreement are performed in IEEE 802.11.	12	1	5
	(OR)			
	(b) What is SQl injection? Explain how the attack and its remedies are implemented.			

* * * *

