Reg. No.														

B.Tech. DEGREE EXAMINATION, DECEMBER 2022
Sixth/ Seventh Semester

18CSE354T – NETWORK SECURITY
(For the candidates admitted from the academic year 2018-2019 to 2019-2020)

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.
(ii) **Part - B** should be answered in answer booklet.

Time: 2½ Hours Max. Marks: 75

PART – A (25 × 1 = 25 Marks)
Answer **ALL** Questions

	Marks	BL	CO	PO
1. Which of the following is a malicious software that, on execution runs in own code and modifies other computer programs? (A) Spam (B) Virus (C) Spyware (D) Adware	1	1	1	1
2. Which of the following VPN topologies establishes a persistent connection between an organizations main office and its branch using a third-party network or the internet? (A) Hub and spoke (B) Full mesh (C) Start (D) Point to point	1	2	1	1
3. A firewall is installed at the point where the secure internal network and untrusted external network meet which is also known as _____. (A) Clock point (B) Meeting point (C) Firewall point (D) Secure point	1	2	1	1
4. This attack is made possible due to applications not property logging and traveling user's action, thus allowing malicious manipulation of actions that the user did (or) did not commit like logging of wrong data to log files. Identity which type of attack is this. (A) Replay (B) Active attack : repudiation (C) Passive attack : traffic analysis (D) Masquerade	1	2	1	1
5. A stand alone malware computer program that replicates itself in order to spread to other computer. (A) Virus (B) Worms (C) Trojan (D) Bots	1	1	1	1
6. In _____, there is a single path from the fully trusted authority to any certificate. (A) X509 (B) PGP (C) KDC (D) TSL	1	1	2	1

PART – B (5 × 10 = 50 Marks)
Answer **ALL** Questions

	Marks	BL	CO	PO
26. a. State the technical details of firewall and describe the process by which filtering firewall can successfully secure the system.	10	3	1	1
(OR)				
b. Identify a few malicious programs that need a host program for their existence.	10	2	1	1
27. a. With neat sketch show the actual ISAKMP packets that are exchanged between initiator and a responder using the pre-shared key method in main model.	10	3	2	1
(OR)				
b. Define AH in tunnel and transport model and state the difference between AH and ESP.	10	1	2	1
28. a. Elaborate the functions included in MIME in order to enhance the security? How they are done?	10	3	3	1
(OR)				
b. Articulate how the source authentication is provided based on public key, secret key and distribution list exploders.	10	3	3	1
29. a. Illustrate and describe the actions involved in SSL record protocol.	10	2	4	1
(OR)				
b. Explain in detail about SET for E-commerce transaction.	10	1	4	1
30. a. Elaborate on the various 802.11i phases of operation analyze its performance.	10	3	5	1
(OR)				
b. Discuss about the XSS vulnerabilities and explain the solutions to overcome the XSS.	10	2	5	1

* * * * *

7. IKE is a complex protocol based on _____ other protocols. 1 2 2 1
   (A) Two (B) Three
   (C) Four (D) Five

8. _____ is the protocol designed to create security associations, both inbound and outbound. 1 2 2 1
   (A) SA (B) CA
   (C) KDC (D) IKE

9. The IPsec header includes a field known as the _____ which identifies the security association in SAD [Security Association Database]. 1 2 2 1
   (A) State index (B) Security parameter index
   (C) Sequence index (D) Flag

10. _____ provides either authentication or encryption (or) both for packets at the IP level. 1 2 2 1
   (A) AH (B) ESP
   (C) PGP (D) SSL

11. A sender 'S' sends a message 'm' to receiver 'R', which is digitally signed by S with its private key. In this scenario one (or) more of the following security violations can take place. 1 3 3 1
   (i) S can launch a birthday attack to replace m with fraudulent message
   (ii) A third party attacker can launch a birthday attack to replace m with a fraudulent message
   (iii) R can launch a birthday attack to replace m with a fraudulent message,
   Which of the following are possible security violations?
   (A) (i) and (ii) only (B) (i) only
   (C) (ii) only (D) (ii) and (iii) only

12. Which of the following are used to generate a message digest by the network security protocols? 1 3 3 1
   (P) RSA (Q) SHA-1 (iii) DES (S) MDS
   (A) P and R only (B) R and S only
   (C) Q and R only (D) Q and S only

13. Mention the size of the message integrity code key 1 1 3 1
   (A) 64 bits (B) 128 bits
   (C) 256 bits (D) 512 bits

14. Which operation is used in encryption using IDEA? 1 2 3 1
   (A) Addition modulo 216 (B) Bit wise XOR
   (C) Addition modulo 216 and bit wise XOR (D) Addition modulo 216 and bit wise AND

15. _____ uniquely identifies the MIME entities uniquely with reference to multiple contents. 1 1 3 1
   (A) Content description (B) Content ID
   (C) Content type (D) Content transfer encoding

16. SSL primarily focuses on _____. 1 1 4 1
   (A) Integrity and non-repudiation (B) Integrity and authenticity
   (C) Authenticity and privacy (D) Confidentiality and integrity

17. In the SSL protocol, which protocol consists of only 1 byte? 1 2 4 1
   (A) Alert protocol (B) Handshake protocol
   (C) Upper-layer protocol (D) Change cipher spec protocol

18. In SSL handshake, server hello messages typically contains _____. 1 1 4 1
   (A) List of ciphers for the session and extensions list (B) Selected cipher for the session and random bytes
   (C) Selected cipher for the session and public key for server (D) Random bytes and public key server

19. _____ layer security protocol provides end to end security services for applications. 1 2 4 1
   (A) Data link layer (B) Network
   (C) Transport (D) Application

20. The combination of key exchange, hash and encryption algorithms defines a _____ for each SSL session. 1 1 4 1
   (A) List of protocols (B) Cipher suites
   (C) List of keys (D) Handshake

21. Which layer keep tracks of the frames that have been transmitted and received? 1 1 5 1
   (A) Physical layer (B) Medium access layer
   (C) Logic link control layer (D) Transport layer

22. Which of the stored procedure is used to test the SQL injection attack? 1 2 5 1
   (A) XP_write (B) XP_regwrite
   (C) XP_reg (D) XP_cmdshell

23. SQL injection is an attack in which _____ code is inserted into strings that are later passed to instance of SQl server. 1 2 5 1
   (A) Malicious (B) Redundant
   (C) Clean (D) Non-malicious

24. IEEE 802.11 defines _____ services that need to be provided by the wireless LAN to achieve functionality equivalent to that which is inherent to wired LANs. 1 2 5 1
   (A) 4 (B) 7
   (C) 5 (D) 9

25. When a station moves only within the direct communication range of the communication stations of a single BSS, it is referred to as _____. 1 1 5 1
   (A) No transition (B) BSS transition
   (C) ESS transition (D) MS transition