b.	Illustrate with an example, the Diffie Hellman key exchange algorithm in detail.	10	1	3	1
29. a.	Explain in detail about SET for E-commerce transaction.	10	1	4	1
	(OR)				
b.	Discuss in detail about change cipher spec and alert protocol.	10	1	4	1
30. a.	Write in detail about IEEE 802.11 wireless LAN. Analyze its performance.	10	1	5	1
	(OR)				
b.	Describe about buffer overflow and format string attacks.	10	1	5	1

* * * * *

Reg. No.														

B.Tech. DEGREE EXAMINATION, MAY 2022
Sixth 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.	In a network, if p is the only packet being transmitted and there was no earlier transmission, which of the following delays could be zero? (A) Propagation delay (B) Transmission delay (C) Queuing delay (D) Processing delay	1	1	1	1
2.	Among the following statements, which are true with respect to signature based IDS? (A) It cannot work with an IPS (B) It only identifies on known signature (C) It detects never – before seen anomalies (D) It works best in large enterprise	1	1	1	1
3.	Bypassing a device, or performing another action, to attack or place malware on a target network without being detected is called (A) Packet filter (B) State table (C) Evasion (D) Honeypot	1	1	1	1
4.	The advantage of setting up a DMZ with two firewalls is (A) You can control where traffic goes in the three networks (B) You can do stateful packet filtering (C) You can do load balancing (D) Improved network performance	1	1	1	1
5.	Which malicious program cannot do anything until actions are taken to activate the file attached by the malware? (A) Trojan horse (B) Worm (C) Virus (D) Bots	1	1	1	1
6.	The encryption protocols used to secure the authentication of computers using IPsec is (A) Kerberos V5 (B) Certificates (C) SHA (D) HASH	1	1	2	1
7.	The mode which can be used to secure communications between two LANs is (A) AH tunnel mode (B) IKE tunnel mode (C) AH transport mode (D) ESP transport mode	1	1	2	1

8. Which of the following organizations is primarily concerned with military encryption — 1 1 2 1
   (A) NSA (B) NIST
   (C) IEEE (D) ITU

9. In tunnel model, IPsec protects the _____. — 1 1 2 1
   (A) Entire IP packet (B) IP header
   (C) IP payload (D) IP trailer

10. What is the size of the RSA signature hash after the MD5 and SHA-1 processing? — 1 1 2 1
   (A) 42 bytes (B) 32 bytes
   (C) 36 bytes (D) 48 bytes

11. _____ is a process which verifies the identity of a user who wants to access the system. — 1 1 3 1
   (A) Authentication (B) Non-repudiation
   (C) Integrity (D) Availability

12. Which algorithm provides the private key and its corresponding public key? — 1 1 3 1
   (A) Key generation algorithm (B) Signature verifying algorithm
   (C) Signing algorithm (D) DES algorithm

13. Which hashing algorithm is used to derive the PTK for PMK? — 1 1 3 1
   (A) SHA – 1 (B) SHA – 2
   (C) SHA – 3 (D) MD – 5

14. In which port forwarding technique does the client act on the server's behalf? — 1 1 3 1
   (A) Remote forwarding (B) Local forwarding
   (C) Stable forwarding (D) Packet forwarding

15. How many algorithms digital signature consists of — 1 1 3 1
   (A) 2 (B) 3
   (C) 4 (D) 5

16. Which one of the following is not a higher – layer SSL protocol? — 1 1 4 1
   (A) Alert protocol (B) Handshake protocol
   (C) Alarm protocol (D) Change cipher spec protocol

17. Which protocol is used to convey SSL related alerts to the peer entity? — 1 1 4 1
   (A) Alert protocol (B) Handshake protocol
   (C) Upper layer protocol (D) Change cipher spec protocol

18. In the alert protocol the first byte takes the value 1 or 2 which corresponds to _____ and _____ respectively. — 1 1 4 1
   (A) Select, alarm (B) Alert, alarm
   (C) Warning, alarm (D) Warning, fatal

19. Which is the key exchange algorithm used in cipher suite parameters? — 1 1 4 1
   (A) RSA (B) Fixed Diffie-Hellman
   (C) Ephemeral (D) A, B and C

20. The certificate message is required for any agreed-on key exchange method except _____. — 1 1 4 1
   (A) Ephemeral Diffie – Hellman (B) Anonymous Diffie – Hellman
   (C) Fixed Diffie – Hellman (D) RSA

21. With respect to IEEE 802.11 wireless LAN, MSDU stands for _____. — 1 1 5 1
   (A) MAC service data unit (B) Main server data user
   (C) Multiframe service datagram usage (D) MAC service device usage

22. Frequency bond definition and wireless signal encoding are functions of which layer? — 1 1 5 1
   (A) Physical layer (B) Logical link control layer
   (C) Medium access layer (D) Application layer

23. Another name for the AAA key (Authentication, Authorization and Accounting key) is _____. — 1 1 5 1
   (A) Pre-shared key (B) Pairwise transient key
   (C) Master session key (D) Key conformation key

24. In which phase of operation does the STA prove their identities to each other? — 1 1 5 1
   (A) Discovery (B) Authentication
   (C) Key generation and distribution (D) Protected data transfer

25. What was the security algorithm defined for the IEEE 802.11? — 1 1 5 1
   (A) WEP (B) RSN
   (C) WPA (D) SSL

PART – B (5 × 10 = 50 Marks) — Marks BL CO PO
Answer **ALL** Questions

26. a. Describe about IDS with its advantages and disadvantages. — 10 1 1 1

(OR)

   b. Describe different types of network layer attacks. Give an example for each. — 10 1 1 1

27. a. Explain in detail about architecture of IP security. — 10 1 2 1

(OR)

   b. Enumerate the basic combinations of security associations in detail. — 10 1 2 1

28. a. Write in detail about the security services (PGP, S |MIME for E-mail. — 10 1 3 1

(OR)