Reg. No.															

B.Tech. DEGREE EXAMINATION, MAY 2024

Sixth & Seventh Semester

18CSE354T – NETWORK SECURITY

(For the candidates admitted during the academic year 2018-2019 to 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.

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

Time: 3 hours | Max. Marks: 100

	Marks	BL	CO	PO

PART – A (20 × 1 = 20 Marks)

Answer **ALL** Questions

1. Which of the following is the exact function of switch? | 1 | 1 | 1 | 1

   (A) Receives traffic in a port and repeats the traffic out all the other ports
   (B) Makes it forwarding decisions based on the destination (MAC) address
   (C) Can store website information for a configurable amount of time
   (D) Makes forwarding decisions based on IP addressing

2. _____ is the term used in computer security to protect your data from getting disclosed. | 1 | 1 | 1 | 1

   (A) Integrity
   (B) Authentication
   (C) Confidentiality
   (D) Availability

3. Which type of attack specifically aims to disrupt services and block legitimate users from accessing systems and information? | 1 | 1 | 1 | 1

   (A) Replaying
   (B) Modification
   (C) Stealing
   (D) Denial of service

4. Which of the following statements about malware are true? | 1 | 1 | 1 | 1

   (i) Trojan horse is malware disguised as legitimate software
   (ii) A virus insert itself into another program
   (iii) A worm is similar to a virus except that it does not need a program in order to run

   Choose the correct answer from the options

   (A) (i) and (ii) only
   (B) (i) and (iii) only
   (C) (ii) and (iii) only
   (D) (i), (ii) and (iii)

5. IPsec is a collection of protocols designed by Internet Engineering Task Force to provide security for a packet at the _____ level. | 1 | 1 | 2 | 1

   (A) Transport layer
   (B) Data link layer
   (C) Network layer
   (D) Physical layer

6. In the _____ mode, the IPsec header is added between the IP header and the rest of the packet. | 1 | 1 | 2 | 1

   (A) Transport
   (B) Tunnel
   (C) Transition
   (D) Non-disclosure

7. The _____ protocol provides message authentication, integrity and privacy 1 1 2 1
   (A) Authentication header (B) Encapsulating security payload
   (C) Security parameter index (D) Security association

8. Identity the protection provided in ISAKMP main mode 1 1 2 1
   (A) Encryption (B) Hashing
   (C) Digital signature (D) Key exchange

9. Using email backing illicit, hackers can send and spread _____ virus, _____ and spam emails. 1 1 3 1
   (A) Antivirus, patches (B) Cracked software, redirected malicious URLS
   (C) Trojans, redirected malicious URLS (D) Malware, security patches

10. In public key cryptosystem which is kept as public 1 1 3 1
   (A) Encryption keys (B) Decryption keys
   (C) Support keys (D) Both encryption and decryption keys

11. The total key size allowed in PGP is _____. 1 1 3 1
   (A) 1024-1056 (B) 1024-4096
   (C) 1024-2048 (D) 1024-4056

12. Which of the following standards does S/MIME use? 1 1 3 1
   (A) PKCS #4 (B) PKCS #7
   (C) X.509 (D) TLS

13. In the SSL protocol, each upper layer message is fragmented into a maximum of _____ bytes. 1 1 4 1
   (A) 2^{16} (B) 2^{32}
   (C) 2^{12} (D) 2^{14}

14. What is the purpose of the "Public key Infrastructure" in SSL/TLS? 1 1 4 1
   (A) To encrypt data transmission (B) To issue SSL/TLS certificates to websites
   (C) To establish secure connections (D) To manage the trust and distribution of public keys

15. In the handshake protocol, which is the message type first sent between client and server? 1 1 4 1
   (A) Client-hello (B) Server-hello
   (C) Certificate-request (D) Hello-request

16. The _____ protocol is used for the purpose of copying the pending state into the current state? 1 1 4 1
   (A) Alert (B) Upper-layer
   (C) Change cipher spec (D) Handshake

17.	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. (A) 4 (B) 7 (C) 5 (D) 9	1	1	5	1
18.	What technique do hackers use to make fake websites that look real? (A) Social engineering (B) Cookie stealing (C) Phishing (D) Cyberstalking	1	1	5	1
19.	In a stored cross-site scripting attack, where does the malicious script typically reside? (A) In the user's browsers (B) On the server-side database (C) In the URL (D) In web application's source code	1	1	5	1
20.	At which of the following stage does SQL injection occurs? (A) When the user is asked to logout (B) When the user is asked to input password (C) When the user is asked to input captcha (D) When the user is asked to input user name	1	1	5	1

PART – B (5 × 4 = 20 Marks)
Answer **ANY FIVE** Questions

		Marks	BL	CO	PO
21.	Discuss IP address spoofing with example.	4	2	1	1
22.	Describe the fields in authentication header and ESP packet format with a neat diagram.	4	2	2	1
23.	Explain the steps for non-repudiation with secret keys.	4	2	3	1
24.	Illustrate the approaches to verify a public key.	4	2	4	1
25.	Comment on how authentication and confidentiality achieved in IEEE 802.11 WLAN.	4	2	5	1
26.	Illustrate the steps involved in IKE phase 1.	4	2	2	1
27.	Explain briefly about format string attacks.	4	2	5	1

PART – C (5 × 12 = 60 Marks)
Answer **ALL** Questions

		Marks	BL	CO	PO
28. a.	List the characteristics of a good firewall implemented on a network. How is circuit gateway different from application gateway?	12	1	1	1
	(OR)				
b.	Explain the technical details of Intrusion Prevention System (IPS) and describe all its types with neat diagrams.	12	1	1	1

29. a.	Interpret how ESP and AH is applied to transport and tunnel mode authentication in IP.	12	2	2	1
	(OR)				
b.	Analyze Oakley key determination protocol in detail with example.	12	2	2	1
30. a.	Dramatize end-to-end privacy, privacy with distribution list exploiters with appropriate examples.	12	2	3	1
	(OR)				
b.	Evaluate the performance of PGP and its operational description compare it with S/MIME.	12	3	3	1
31. a.	Generalize the steps involved in the simplified form of the SSL/TLS protocol and the methodology involved in computing the keys.	12	2	4	1
	(OR)				
b.	Elaborate how Secure Electronic Transaction (SET) protocol enables e-transaction. Explain the components involved in detail.	12	2	4	1
32. a.	Assess the various security mechanisms in cellphone technology and GSM (2G) with appropriate example.	12	2	5	1
	(OR)				
b.	Identify the type of attack generated by UPDATE statement. Detail the methods used to prevent SQL injection attacks.	12	2	5	1

* * * * *