

b. Construct the prevention mechanism and web security attacks of client authentication with a neat sketch. 12 5 4 1

32. a. Assess the functions of security in UMTS (3G) with suitable example. 12 6 5 1

(OR)

b. Discriminate the authentication and confidentiality of wireless network security in detail. 12 6 5 1

* * * * *

Reg. No.

B.Tech. DEGREE EXAMINATION, JUNE 2023

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

PART – A (20 × 1 = 20 Marks)

Answer **ALL** Questions

- | | Marks | BL | CO | PO |
|--|-------|----|----|----|
| 1. It is used to keep subjects accountable for their actions while they are authenticated to a system.
(A) Access controls (B) Monitoring
(C) Account lockout (D) Performance reviews | 1 | 1 | 1 | 1 |
| 2. The one which is most useful in sorting through large log files when searching for intrusion related events
(A) Text editor (B) Vulnerability scanner
(C) Password cracker (D) IDS | 1 | 1 | 1 | 1 |
| 3. A true one regarding vulnerability scanners
(A) They actively scan for intrusion attempts (B) They serve as a form of enticement
(C) They locate known security holes (D) They automatically reconfigure a system to a more secured state | 1 | 1 | 1 | 1 |
| 4. While using penetration testing to verify the strength of your security policy
(A) Mimicking attacks previously perpetrated against your system (B) Performing the attacks without managements consent
(C) Using manual and automated attack tools (D) Reconfiguring the system to resolve any discovered vulnerabilities | 1 | 1 | 1 | 1 |
| 5. Range of class a in public IPv4.
(A) 0.0.0.0 to 223.255.255.255 (B) 0.0.0.0 to 192.0.0.0
(C) 0.0.0.0 to 127.255.255.255 (D) 0.0.0.0 to 128.0.0.0 | 1 | 1 | 2 | 1 |
| 6. Find the valid private IP addresses
(A) 172.30.255.255 (B) 10.210.220.254
(C) 172.16.21.240 (D) 172.32.250.254 | 1 | 1 | 2 | 1 |
| 7. When sending packet to a destination, the source host send queries to
(A) Dual stack (B) Domain name server
(C) Header information (D) Transport layer | 1 | 1 | 2 | 1 |

8. When two computers want to communicate using IPv6 with each other and the packet must pass through a region that uses IPv4 in	1	1	2	1
(A) Stack				
(B) Tunneling				
(C) Header translation				
(D) Conversion				
9. A major way of stealing email information	1	1	3	1
(A) Stealing cookies				
(B) Reverse engineering				
(C) Password phishing				
(D) Social engineering				
10. Method for keeping sensitive information in email communication and accounts secure against unofficial access, loss or compromise	1	1	3	1
(A) Email security				
(B) Email scrutiny				
(C) Email protection				
(D) Email safeguarding				
11. A stored cookie which contains all your personal data about that website can be stolen away by	1	1	3	1
(A) Attackers and malware				
(B) Hackers and antivirus				
(C) Penetration testers and malware				
(D) Penetration testers and virus				
12. A technique used for tricking users to disclose their username and passwords through fake pages.	1	1	3	1
(A) Social engineering				
(B) Phishing				
(C) Coolie stealing				
(D) Banner grabbing				
13. The following one is not a session state parameter	1	1	4	1
(A) Master secret				
(B) Cipher spec				
(C) Peer certificate				
(D) Server write key				
14. Difference between HMAC algorithm and SSLV3 is that Pad1 and Pad2 in SSLV3 but whereas in HMAC.	1	1	4	1
(A) Nanded, XORed				
(B) Concatenated, XORed				
(C) XORed, Nanded				
(D) XORed, XOed				
15. In TLS padding can be up to a maximum of	1	1	4	1
(A) 79 bytes				
(B) 127 bytes				
(C) 255 bytes				
(D) 256 bytes				
16. An alert codes is not supported by SSLV3	1	1	4	1
(A) Record_overflow				
(B) No_certificate				
(C) Internal_error				
(D) Decode_error				
17. An UMTS does not has backward compatibility with	1	1	5	1
(A) GSM				
(B) IS-136				
(C) IS-95				
(D) GPRS				
18. A chip rate or W-CDMA	1	1	5	1
(A) 1.2288 Mcps				
(B) 3.84 Mcps				
(C) 270.833 Mcps				
(D) 100 Mcps				

19. Not a proper standard of wireless LAN	1	1	5	1
(A) HIPER-LAN				
(B) HIPERLAN/2				
(C) IEE 802.11b				
(D) Amps				
20. A wireless LAN standard has been named Wi-Fi for	1	1	5	1
(A) IEEE 802.6				
(B) IEEE 802.15.4				
(C) DSSS IEEE 802.11 b				
(D) IEEE 802.11G				

PART – B (5 × 4 = 20 Marks)

Answer ANY FIVE Questions

	Marks	BL	CO	PO
21. Discuss packet filtering and its features.	4	2	1	1
22. Identity the different phases and scenario of IKE.	4	2	2	1
23. Extend the security services for E-mail.	4	2	3	1
24. Distinguish the advantages and disadvantages of client authentication.	4	2	4	1
25. Express briefly about cross site scripting.	4	2	5	1
26. Recognize the authentication of the source in network.	4	2	3	1
27. Indicate the vulnerabilities in wireless LAN.	4	2	5	1

PART – C (5 × 12 = 60 Marks)

Answer ALL Questions

	Marks	BL	CO	PO
28. a. Illustrate in detail about IP address spoofing with a neat diagram.	12	3	1	1
(OR)				
b. Write in detail about the malicious software with example.	12	3	1	1
29. a. Interpret the encoding process of ISAKMP/IKE.	12	4	2	1
(OR)				
b. Analyze the key exchange strategies of internet in detail.	12	4	2	1
30. a. Discover a public key technology with distribution list for the detection of attacks in email.	12	4	3	1
(OR)				
b. Dramatize public and secret key for establishing the security services with appropriate examples.	12	4	3	1
31. a. Categorize the basic protocols of SSL/TLS for web security attacks.	12	5	4	1

(OR)