b.	Consider a computer system with three users: Alice, Bob and Cyndy, Alice owns the file alicerc, and Bob and Cyndy can read it. Cyndy can read and write the file bobrc, which Bob owns, but Alice can only read it. Only Cyndy can read and write the file cyndyrc, Which she owns, assume that the owner of each of these files can execute it. (i) Create the corresponding access control matrix (ii) Cyndy gives Alice permission to read lyndyrc, and Alice removes Bob's ability to read alicerc. Show the new access control matrix.	10	3	1	2
27. a.	Illustrate a model of a security policy that refers equally to confidentiality and integrity.	10	3	2	1
	(OR)				
b.	Compare and contrast bell-lapadula model with Chinese wall model.	10	4	2	4
28. a.	Discuss various malwares used by cyber attackers designed to cause extensive damage to data and systems or to gain unauthorized access to a network.	10	3	3	4
	(OR)				
b.	Point out the features of forensic duplication and investigation and also outline the problems and challenges forensic examiners face when preparing and processing investigations, including the ideas and questions they must consider (i) Analyse the concept of data acquisition methods and explain how would you work in a case of clustering (ii) Analyze the physical requirements for a computer forensics lab	10	4	3	4
29. a.	Describe various database security access points.	10	3	4	1
	(OR)				
b.	Discuss various risk mitigation policies and processes to reduce the overall risk or impact of a cyber security threats.	10	3	4	1
30. a.	Discuss the issues and actions that security policies must address.	10	3	5	1
	(OR)				
b.	Explain how authentication over a network is handled by the SSL protocol.	10	4	5	4

* * * * *

Reg. No.															

B.Tech. DEGREE EXAMINATION, NOVEMBER 2022

Sixth / Seventh Semester

18CSC364J – INFORMATION 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

		Marks	BL	CO	PO
	PART – A (25 × 1 = 25 Marks) Answer **ALL** Questions				
1.	Rule-Based Access Control (RuBAC) access is determine by rules such rules would fit with in what category of access control (A) Discretionary Access Control (DAC) (B) Mandatory Access Control (MAC) (C) Non-Discretionary Access Control (NDAC) (D) Lattice-Based Access Control	1	1	1	1
2.	Which of the following is not an access control mechanisms? (A) Serialized access control (B) Discretionary and mandatory model (C) Roll-based model (D) Task-based model	1	2	1	1
3.	The type of Discretionary Access Control (DAC) that is based on an individual's identity is also called (A) Rule-based access control (B) Identity-based access control (C) Non-discretionary access control (D) Lattice-based access control	1	2	1	1
4.	What is the type of access control where there are pairs of elements that have the least upper bound of values and greatest lower bound of values (A) Mandatory model (B) Discretionary model (C) Lattice model (D) Rule model	1	1	1	1
5.	The form of data, having an associated time interval during which it is valid is known as (A) Temporal data (B) Snapshot data (C) Chunk data (D) Point in the time data	1	1	1	1
6.	_____ is the problem of preventing a server form leaking information that the user of the service considers confidential (A) User privileges problem (B) Confinement problem (C) Access control problem (D) Server problem	1	2	2	1
7.	_____ uses a temporal or ordering relationship among accesses to a shared resource (A) Covert storage channel (B) Covert process channel (C) Covert execution channel (D) Covert timing channel	1	2	2	1

8. In the common criteria, an implementation, independent statement of security needs for a set of IT security products that could be built is called a — 1 2 2 1
   (A) Security target (ST) (B) Package
   (C) Protection profile (PP) (D) Target of evaluation (TOE)

9. When two access control list entries in the same ACL give different permissions to the subject? — 1 2 2 1
   (A) User problem (B) Conflicts
   (C) All error (D) All duplicate

10. _____ states that, unless a subject is given explicit access to an object, it should be denied access to that object — 1 1 2 1
   (A) Principle of fail-sage defaults (B) Principle of least privilege
   (C) Principle of complete mediation (D) Principle of open design

11. An intrusion detection system (IDS) is primarily designed to perform what function? — 1 2 3 1
   (A) Detect abnormal activity (B) Detect system failures
   (C) Rate system performance (D) Test a system for vulnerabilities

12. Which of the following is not a valid measure to improve protection against brute force and dictionary attack? — 1 2 3 1
   (A) Enforce strong passwords through a security policy (B) Maintain strict control over physical access
   (C) Require all users to login remotely (D) Use two-factor authentication

13. A method used by IDS that involve checking for a pattern to identify unauthorized activity — 1 1 3 1
   (A) Pattern matching (B) Session splicing
   (C) Protocol decoding (D) State table

14. A server (or application) that intercepts the requests clients make to another server, fills the requests that it can, and then forwards the requests it can't handle on to the other server thus helping to improve performance and security — 1 2 3 1
   (A) Honey pot (B) Proxy server
   (C) Packet filter (D) State table

15. _____ is the process of retaining or keeping of data at a secure place for long-term storage — 1 1 3 1
   (A) Data archiving (B) Archival storage
   (C) Disposal of data (D) Backup

16. Prevention of access to the database by unauthorized user is referred to as — 1 2 4 1
   (A) Security (B) Confidentiality
   (C) Integrity (D) Availability

17. What is the first process in the risk management methodology? — 1 1 4 1
   (A) Risk analysis (B) Likelihood
   (C) Fault tolerance (D) Record retention

18. _____ is a type of software designed to help the user computer detect viruses and avoid them — 1 2 4 1
   (A) Malware (B) Adware
   (C) Antivirus (D) Spyware

19. Which of the following is not a type of cyber security? — 1 2 4 1
   (A) Cloud security (B) Network security
   (C) Application security (D) Operating system security

20. Using the _____ account of a linux system, one can carry out administrative functions. — 1 1 4 1
   (A) Root (B) Administrative
   (C) User (D) Client

21. To ensure that users cannot misuse those roles and privileges when they are not using the application , what security concern is used? — 1 1 5 1
   (A) Establish and maintain application level security (B) Manage privileges and attributes
   (C) Establish the granularity of access control desired (D) Establish and manage the use of encryption

22. SSL also uses _____ to ensure data confidentiality, and cryptographic checksums to ensure data integrity, many of these uses of encryption are relatively transparent to a user or application — 1 1 5 1
   (A) Authentication (B) Authorization
   (C) Verification (D) Encryption

23. To track several DDL statements regardless of the table on which that are issued, you can also set _____ level auditing to audit selected users or every user in the database. — 1 1 5 1
   (A) Statement auditing (B) Privilege auditing
   (C) Schema object auditing (D) Fine-grained auditing

24. Authentication systems based on _____ digital certificates to user clients, which use them to authenticate directly to servers in the enterprise without directly involving an authentication server? — 1 2 5 1
   (A) Kerberos authentication (B) PKI-based authentication
   (C) Authentication with radius (D) Directory-based services

25. Kerberos provides the security services of protection for authentication traffic — 1 2 5 1
   (A) Availability and non repudiation (B) Confidentiality and authentication
   (C) Confidentiality and integrity (D) Availability and authorization

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

26. a. Identify the six components of an information system, which are mostly directly affected by the study of computer security? Illustrate with an example. — 10 4 1 4

(OR)