Reg. No.															

B.Tech. DEGREE EXAMINATION, NOVEMBER 2023

Sixth Semester

18CSC364J – INFORMATION SECURITY

(For the candidates admitted from the academic year 2020-2021 & 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. _____ means the protection of data form modification by unknown users. (A) Confidentiality (B) Integrity (C) Authentication (D) Non-repudiation	1	1	1	1
2. Suppose in a system you have 2000 files and 4 user who has access rights to these files. Which one of the following will be the best method to implement access control? (A) Using access matrix (B) Using a capability based implementation (C) Using access control lists (D) Other advanced techniques which work well	1	2	2	2
3. The type of Discretionary Access Control (DAC) that is based on an individuals identity is also called (A) Identity-based access control (B) Rule-based access control (C) Non-discretionary access control (D) Lattice-based access control	1	1	2	1
4. 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
5. What information security model formalizes the U.S department of defense multi-level security policy? (A) Biba (B) Bell-LaPadula (C) Clark-Wilson (D) Chinese-Wall				
6. A _____ is a collection of job functions. (A) User (B) Privileges (C) Profile (D) Role	1	1	3	1
7. When two access control list entries in the same Access Control List (ACL) give different permissions to the subject. (A) User problem (B) Conflicts (C) ACL error (D) ACL duplicate	1	2	3	2

8. _____ is the problem of preventing a server form leaking information that the user of the service considers confidential. 1 2 3 2
   (A) User privileges problem (B) Confinement problem
   (C) Access control problem (D) Server problem

9. _____ is the time frame from when the loophole in security was introduced till the time when the bug was fixed 1 2 4 2
   (A) Window of vulnerability (B) Time frame of vulnerability
   (C) Time-lap of vulnerability (D) Entry-door of vulnerability

10. On which is the national vulnerability database primarily built upon? 1 2 4 2
   (A) Vulnerabilities (B) NVD
   (C) Patch (D) CVE identifiers

11. What is common with most vulnerability assessment tools? 1 1 4 1
   (A) Command mode (B) GUI front end
   (C) ICMP traffic (D) Fragmented packets

12. Which of the following is true for a host-based IDS? 1 1 4 1
   (A) It monitors an entire network (B) It monitors a single system
   (C) It is invisible to attackers and authorized users (D) It is ineffective on switched networks

13. _____ is responsible for using that the database remains in a consistent state despite system failure. 1 2 5 2
   (A) Storage manager (B) Admin
   (C) End user (D) Transaction manager

14. Another term for project impact analysis is 1 1 5 1
   (A) Risk management (B) Risk assessment
   (C) Risk analysis (D) Risk benefit

15. MAC is abbreviated as 1 1 5 1
   (A) Mandatory access control (B) Machine access control
   (C) Manage account control (D) Machine accounting control

16. An audit log is an example of what type of control? 1 2 5 2
   (A) Detective control (B) Preventive control
   (C) Recovery control (D) Containment control

17. For verifying the identity of someone (A user, device, or an entity) who wants to access data, resource, or applications by using 1 2 6 2
   (A) Authentication (B) Authorization
   (C) Verification (D) Integration

18. Users (including applications, batch jobs, and scripts) connect to databases by using a standard _____ statement that specifies a database_connect_string. 1 2 6 2
   (A) Join (B) Create
   (C) Connect (D) Merge

19.	What is the first step of access control? (A) Accountability logging (B) ACL verification (C) Subject authorization (D) Subject identification	1	1	6	1
20.	Which of the following tool is used for the purpose of data auditing for SQL server only? (A) Apex SQL (B) SQL Ninja (C) SQL Audit (D) Idera	1	2	6	2

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

		Marks	BL	CO	PO
21.	Consider a computer system with three users: Alice, Bob and Cyndy. Alice owns the file alicerc, 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 cyndyrc, and Alice removes Bob's ability to read alicerc. Show the new access control matrix	4	4	2	4
22.	Write short notes about assumptions and trust.	4	3	1	3
23.	Discuss about the basics and background of Information flow with example.	4	3	3	3
24.	Categorize and explain the branches of digital forensics.	4	4	4	3
25.	Interpret the reason that why is database security important.	4	3	5	3
26.	Write short notes on risk mitigation plan.	4	3	5	3
27.	Explain the three basic security requirements.	4	3	6	3

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

		Marks	BL	CO	PO
28. a.i.	With neat sketch, explain in detail about CIA triad with examples.	9	3	1	3
ii.	Write short notes on security threats.	3	3	1	3
	(OR)				
b.	Explain in detail about the following (i) Discretionary Access Control (DAC) (ii) Mandatory Access Control (MAC) (iii) Role-Based Access Control (RBAC)	12	4	2	4
29. a.	Illustrate a model with its properties and examples for the following policies (i) Confidentiality policies (ii) Integrity policies	12	4	3	4
	(OR)				

b.i.	Explain in detail about Chinese wall model for hybrid policies.	8	3	3	3
ii.	Write short notes on system design evaluation.	4	3	3	3
30. a.	How to implement data privacy? List some methods for implementing it.	12	4	4	4
	(OR)				
b.	Discuss the various classification of intrusion detection system and illustrate the different intrusion detection techniques.	12	3	4	3
31. a.	List the essential Linux security commands and explain.	12	4	5	3
	(OR)				
b.	With neat sketch, explain in detail about database security architecture.	12	3	5	3
32. a.i.	Discuss in detail about database auditing, security considerations.	4	4	6	4
ii.	List out the various auditing types and records.	8	4	6	4
	(OR)				
b.	With neat diagram, explain in detail about security requirements, threats and concepts.	12	3	6	3

* * * * *