Reg. No.															

B.Tech. DEGREE EXAMINATION, MAY 2024

Sixth Semester

18CSC364J – INFORMATION 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. Which phase of the security life cycle involves implementing security controls and measures? (A) Assessment (B) Design (C) Implementation (D) Evaluation	1	2	1	1
2. Which access control model grants access rights based on the roles individuals hold with in an organization? (A) Roll-based model (B) Task-based model (C) Unified model (D) Temporal model	1	2	1	1
3. Which of the following is not considered on of the CIA triad principles? (A) Confidentiality (B) Integrity (C) Authorization (D) Availability	1	2	1	1
4. What is the main difference between discretionary and mandatory access control models? (A) Discretionary models are based on roles, which mandatory models are based on tasks (B) Discretionary models allow users to control access while mandatory models do not (C) Discretionary models are static, while mandatory models are dynamic (D) Discretionary models require users to have clearance while mandatory models do not	1	1	1	1
5. Which aspect of security architecture deals with controlling the flow of access to resources? (A) Control of access flow (B) Representing identity (C) Information flow (D) Confinement problem	1	2	2	1
6. What is the main objective of confinement problem implementation? (A) Ensuring data integrity (B) Enforcing access flow policies (C) Controlling unauthorized access (D) Mitigating security threats	1	1	2	1
7. Which approach involves the use of mathematical techniques to ensure system correctness? (A) Design principles (B) Formal methods (C) Evaluation system design (D) Informed methods	1	2	2	1

8. What is the primary purpose of evaluating systems in security architecture? 1 1 2 1
   (A) To identify vulnerability (B) To ensure data confidentiality
   (C) To verify policy compliance (D) To access system performance

9. What is the primary objective of enterprise security specification? 1 1 3 1
   (A) Protecting user accounts (B) Defining security requirements for organized
   (C) Securing network infrastructure (D) Implementing intrusion detection system

10. Which security measure focuses on securing access to programs and resources within an operating system? 1 2 3 1
   (A) Operating system security (B) Network security
   (C) User security (D) Program security

11. Which phase of program security involves implementing security measures within software applications? 1 2 3 1
   (A) Program security implementation (B) Program vulnerability
   (C) Program security application analysis (D) Vulnerability analysis

12. What is the primary objective of user security measures? 1 1 3 1
   (A) Protecting system files (B) Securing user accounts and permissions
   (C) Encrypting data transmission (D) Monitoring network traffic

13. What aspect of security focuses on managing access to resource and information within an organization? 1 1 4 1
   (A) Establish strong identity controls (B) Risk mitigation
   (C) Disaster recovery (D) Access management control

14. What is the main goal of a disaster recovery plan? 1 1 4 1
   (A) Preventing cyber attacks (B) Detecting security vulnerabilities
   (C) Recovering from system failures or disaster (D) Ensuring regulatory compliance

15. What is the purpose of a risk mitigation plan? 1 1 4 1
   (A) Assessing system performance (B) Monitoring network traffic
   (C) Identifying and addressing security risks (D) Enhancing user authentication

16. Which security measures focuses on protecting against on unauthorized or abnormal data traffic? 1 2 4 1
   (A) Cyber security measure (B) Anomalous data traffic
   (C) Disaster recovery (D) Access management control

17. What type of action does DMC refer to in database management? 1 1 5 1
   (A) Data manipulation language (B) data migration layer
   (C) Data modeling language (D) Data management life cycle

18.	What does the configuration of grained auditing entail? (A) Configuring user authentication settings (B) Defining fine-grained access control policies (C) Managing database schema objects (D) Optimizing database storage	1	2	5	1
19.	What type of security measure involves storing passwords in a secure location outside of the database? (A) Secure external password store (B) Secure hashing algorithm (C) Encryption key managements (D) Single sign-on authentication	1	1	5	1
20.	Which authentication-related action involves managing user accounts and access permissions? (A) Administering authentication (B) Creating policies (C) Configuring gained auditing (D) DML actions	1	2	5	1

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

		Marks	BL	CO	PO
21.	Outline key components of security policies and procedure, highlighting their role in organizational security management.	4	3	1	1
22.	Explain assumptions and trust in security, discussing their implications for system design and implementation.	4	3	2	1
23.	Define hybrid policies in information security, providing examples of their advantages over single focused policies and challenges in implementation.	4	3	2	1
24.	Define malicious systems and discuss the importance of vulnerability analysis in identifying and mitigating security weakness, with an example.	4	3	3	1
25.	Define security architecture and its importance in ensuring overall organizational IT infrastructure security. Explain the process and key consideration for its implementation.	4	3	4	1
26.	Describe key pillars of database security architecture and their implementation strategies provide examples of database security types and their role in safe guarding data.	4	3	5	1
27.	Define security requirements and threats in database management systems, giving examples of common threats and strategies for mitigation.	4	3	5	1

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

		Marks	BL	CO	PO
28. a.	Analyze a real-world security breach and assess its impact on confidentiality, integrity and availability.	12	4	1	1
	(OR)				
b.	Critically evaluate the influence of emerging technologies on traditional security models, focusing on confidentiality, integrity and availability.	12	4	1	1

29. a.	Design a comprehensive security policy framework for a multinational corporation, integrating confidentiality, integrity and hybrid policies and discuss composition considerations and implementation challenges.	12	4	2	1
	(OR)				
b.	Propose an innovative approach for addressing the confinement problem in multi-label security systems, combining policy-based controls, non-interface composition techniques and formal methods.	12	4	2	1
30. a.	Design and implement a logic-based intrusion detection system for a financial institution, evaluating its effectiveness in detection and mitigating threats.	12	4	3	1
	(OR)				
b.	Conduct a vulnerability analysis of critical infrastructure networks and propose mitigation strategies assessing the feasibility of implementing intrusion detection and digital forensics measures.	12	4	3	1
31. a.	Design a comprehensive security architecture framework for large-scale enterprise environments, incorporating access management control, disaster recovery and risk mitigation plans.	12	3	4	1
	(OR)				
b.	Evaluate the role of linux commands in enhancing system security, analyzing common commands and proposing best practices for their secure configuration.	12	3	4	1
32. a.	Develop an auditing strategy for a mission-critical database system, covering various auditing types and focusing on security and privacy auditing.	12	4	5	1
	(OR)				
b.	Design and implement a Role-Based Access Control (RBAC) system for a database application assessing its benefits, challenges and integration with fine-grained auditing.	12	4	5	1

* * * * *