29. a.i. Identify and describe the model which corresponds to military style classification in confidentiality policy. 8 4 3 4

ii. Explain in detail about security assurance. 4 3 3 3

(OR)

b. Discuss in detail about different types of design principles in information security with suitable examples. 12 4 3 4

30. a. How enterprise security can be implemented? Explain the best practices for enterprise security. 12 3 4 3

(OR)

b.i. Organize the types of network security. 6 4 4 4

ii. Explain in detail about operating system security. 6 3 4 3

31. a.i. Describe the most common and far-reaching vulnerabilities in default Linux installations. 6 4 5 4

ii. With neat sketch, explain in detail about Linux's security model. 6 3 5 3

(OR)

b.i. Describe database security. 3 3 5 3

ii. Why database security is important? 4 4 5 4

iii. Categorize the common threats and challenges to database. 5 4 5 4

32. a.i. Describe the use of audit records and audit trails. 8 4 6 4

ii. List out the information contained in the audit trail. 4 4 6 4

(OR)

b. Explain in detail about the following 12 3 6 3
(i) Statement auditing
(ii) Privilege auditing
(iii) Schema object auditing
(iv) Fine grained auditing

* * * * *

Reg. No.

B.Tech. DEGREE EXAMINATION, MAY 2023
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. Information security is designed and implemented on basis of sphere of protection into 1 2 1 1
(A) Policies, people, technology (B) Protection, people, technology
(C) Protection, policy, technology (D) Policies, protocols, technology

2. Which is not an objective of network security? 1 1 1 1
(A) Identification (B) Authentication
(C) Access control (D) Lock

3. Information security system must be protected in case of an attack, it must 1 2 2 2
(A) Shutdown once the attack is confirmed (B) Provide enough information to assess the damage caused by the attack
(C) Do nothing (D) Try to get back

4. The process of verifying the identity of a user 1 1 1 1
(A) Authentication (B) Identification
(C) Validation (D) Verification

5. A computer system that employs the necessary hardware and software assurance measures to enable it to process multiple levels of classified or sensitive information is called a 1 2 3 2
(A) Closed system (B) Open system
(C) Trusted system (D) Sale system

6. The principle of separation of privilege states that a system should not grant permission based on 1 1 3 2
(A) User requirements (B) User constraints
(C) User privileges (D) Single conditions

7. What does the Bell-LaPadula model not allow? 1 2 3 2
(A) Subjects to read from a higher level and security relative to their level of security (B) Subjects to read from level of security relative to their level of security
(C) Subjects to write to a higher level of security relative to their level of security (D) Subjects to read at their same level of security

8. _______ is an environment in which the actions of a process are restricted according to a security policy. 1 2 3 2
(A) Virtual machine (B) Virtual box
(C) Sand box (D) Kernel

9. Which of the following is a program that copy themselves throughout a computer or network? 1 2 4 2
(A) Worms (B) Trojans
(C) Viruses (D) Rootkits

10. _______ is the cyclic practice for identifying and classifying and then solving the vulnerabilities in a system. 1 1 4 1
(A) Bug protection (B) Vulnerability management
(C) Bug bounty (D) Vulnerability measurement

11. It is necessary to use ______ for maintaining searched data privacy. 1 2 4 2
(A) Private email service (B) Private search engines
(C) Tor browser (D) Private browser window

12. _______ is the process of retaining or keeping of data at a secure place for long term storage. 1 1 4 1
(A) Data archiving (B) Archival storage
(C) Disposal of data (D) Backup

13. To protect system, how many levels of security is required? 1 2 5 2
(A) One (B) Two
(C) Three (D) Four

14. The security of a system can be improved by 1 1 5 1
(A) Audit log (B) Threat monitoring
(C) Security checking (D) Backup files

15. Prevention of access to the database by unauthorized user is referred to as 1 1 5 1
(A) Confidentiality (B) Integrity
(C) Availability (D) Security

16. Another term for project impact analysis is 1 2 5 2
(A) Risk assessment (B) Risk analysis
(C) Risk benefit (D) Risk management

17. ______ allows for the use of certain operations on database objects as authorized by another user. 1 1 6 1
(A) System privileges (B) Object privileges
(C) Admin privileges (D) Class privileges

18. Which of the following option can be considered a target for SQL injection? 1 1 6 1
(A) Misconfigured databases (B) Excessive privileges
(C) Network connectivity (D) Stored procedures

19. “No unauthorized disclosure” is an objective of which aspect of database security? 1 2 6 2
(A) Confidentiality (B) Integrity
(C) Availability (D) Accountability

20. ______ mechanisms are used to protect data from indirect detections. 1 2 6 2
(A) Inference control (B) Cryptography
(C) Access control (D) Data masking

PART – B (5 × 4 = 20 Marks)

Answer **ANY FIVE** Questions

Marks BL CO PO

21. Consider the set of rights {read, write, execute, append, list, modify, own}. 4 3 2 3
(i) Using the above syntax, write a command, delete_all_rights (p,q,s). This command causes ‘p’ to delete all rights the subject ‘q’ has over an object ‘s’.
(ii) Modify your command so that the deletion can occur only if ‘p’ has modify right over ‘s’.

22. On your personal computer, who can install programs? Who can change operating systems data? Who can replace portions of the operating system? Can any of these actions be performed remotely? 4 4 1 4

23. Interpret the concept of international standards for information security. 4 3 3 3

24. Distinguish between intrusion prevention system (IPS) and Intrusion detection system (IDS). 4 4 4 4

25. List out any four Linux capabilities with descriptions. 4 3 5 3

26. Write short notes on anomalous data traffic. 4 3 5 3

27. Explain the purpose of database auditing. 4 3 6 3

PART – C (5 × 12 = 60 Marks)

Answer **ALL** Questions

Marks BL CO PO

28. a.i. Information security is a major concern for the software industry today as the number of internal threats is nearly 80%. Discuss on the statement highlighting the various attacks. 8 4 1 4

ii. Discuss some ways in which data security may be violated. 4 3 1 3

(OR)

b. Explain in detail about the following 12 4 2 4
(i) Role-based model
(ii) Task-based model
(iii) Unified models