(vii) Henry spoofs Julie's IP address to gain access to her computer

(OR)

b.	Discuss the CIA triad which is used as a model designed to guide policies for information security within an organization.	10	3	1	1
27. a.	Illustrate BIBA model which is used to study the nature of integrity systems.	10	3	2	4

(OR)

b.	Describe any two security models used for implementing confidentiality and integrity policy.	10	3	2	1
28. a.	Discuss the various classification of intrusion detection system and illustrate different intrusion detection techniques.	10	4	3	4

(OR)

b.	Discuss in detail about digital forensics implementation.	10	4	3	1
29. a.	Explain in detail the key pillars of database security.	10	3	4	1

(OR)

b.	How can we establish the strong identity control in the database security architecture with a neat diagram?	10	4	4	4
30. a.	Describe the use of audit records and audit trails.	10	3	5	4

(OR)

b.	Illustrate the implementation of application security policies in virtual private database.	10	3	5	4

* * * * *

Reg. No.														

B.Tech. DEGREE EXAMINATION, MAY 2022

Sixth 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

PART – A (25 × 1 = 25 Marks)

Answer **ALL** Questions

		Marks	BL	CO	PO
1.	According to the CIA triad, which of the below mentioned element is not considered in the triad? (A) Confidentiality (B) Integrity (C) Authenticity (D) Availability	1	1	1	1
2.	This is the model designed for guiding the policies of information security within a company, firm or organization, what is this referred to here? (A) Confidentiality (B) Non-repudiation (C) CIA triad (D) Authenticity	1	2	1	1
3.	_____ means the protection of data from modification by unknown users (A) Confidentiality (B) Integrity (C) Authentication (D) Non-repudiation	1	2	1	1
4.	B received a message from A, it can neither confirm if A sent it nor as certain that the message was untampered. The two are violations of (A) Confidentiality and authentication (B) Confidentiality and message integrity (C) Authentication and message integrity (D) Authentication and availability	1	1	1	1
5.	Access control lists include _____. (A) Specific configuration codes entered into security systems to guide the execution of the system (B) Collection of all memory locations (C) Capability tables governing the rights and privileges of a particular user to a particular system (D) Security policy and mechanism	1	1	1	1
6.	The Clark-Wilson model defines data subject to its integrity controls as (A) Constrained data items (B) Unconstrained data items (C) User data items (D) User procedure	1	2	2	1
7.	Which of the following does the Clark-Wilson model not involve? (A) Constrained data items (B) Transformational procedures (C) Confidentiality items (D) Well-formed transactions	1	1	2	1

8. The change the state of the data in the system from one valid state to another, _____ implement well-formed transactions. 1 1 2 1
   (A) Integrity verification process (B) Transformation process
   (C) Integrity constraints procedures (D) Constrained verification procedures

9. What information security model formalizes the US department of defense multi-level security policy? 1 2 2 1
   (A) Clark-Wilson (B) Stark-Wilson
   (C) BIBA (D) Bell-Lapadula

10. In the access control matrix, the rows are 1 2 2 1
   (A) Access control lists (ACLS) (B) Tuples
   (C) Domains (D) Capability lists

11. _____ is the time frame from when the loop hole in security was introduced till the time when the bug was fixed. 1 1 3 1
   (A) Time-frame of vulnerability (B) Window of vulnerability
   (C) Time-lap of vulnerability (D) Entry-door of vulnerability

12. Which is a dictionary of common names for publicly known information security vulnerabilities? 1 1 3 1
   (A) Vulnerability (B) Zero day
   (C) SANS top 20 controls (D) Common vulnerabilities and exposures

13. Control in design of an information on system is used to 1 2 3 1
   (A) Inspect the system and check that it is built as per specifications
   (B) Protect data from accidental or intentional loss
   (C) Ensure that the system processes data as it was designed to and that the results are reliable
   (D) Ensure privacy of data processed by it

14. In auditing with a computer 1 2 3 1
   (A) Auditing programs are designed and used to check a system
   (B) The hardware of the computer is thoroughly checked for malfunctions
   (C) System software is thoroughly checked to ensure error free operations
   (D) Auditors check system with a computer

15. An audit trial is established in a system to 1 1 3 1
   (A) Detect errors in a system (B) Enable auditing of a system
   (C) Localize the source of an error in a system (D) Trail a program

16. Two forms of risk assessment are 1 1 4 1
   (A) Technical and procedural (B) Subjective and objective
   (C) Analytics and assessment (D) Qualitative and quantitative

17. Another term for project impact analysis is 1 2 4 1
   (A) Risk assessment (B) Risk analysis
   (C) Risk benefit (D) Risk management

18. An audit log is an example of what type of control 1 1 4 1
   (A) Detection (B) Preventive
   (C) Recovery (D) Containment

19. Which of the following is considered as the unsolicited commercial email 1 1 4 1
   (A) Virus (B) Malware
   (C) Spam (D) Adware

20. Which of the following is not a type of scanning? 1 1 4 1
   (A) Xams tree scan (B) Cloud scan
   (C) Null scan (D) DFD scan

21. Which of the following option can be considered a target for SQL injection 1 1 5 1
   (A) Mis configured databases (B) Excessive privileges
   (C) Network connectivity (D) Stores procedures

22. _____ ensures that all direct accesses to the system objects occur base on modes and rules fixed by protection policies 1 2 5 1
   (A) Access control (B) Database monitoring
   (C) Inference control (D) Data administration

23. _____ mechanisms are used to protect data from indirect detections. 1 1 5 1
   (A) Inference control (B) Cryptography
   (C) Access control (D) Data masking

24. _____ allows for the use of certain operations on database objects as authorized by another user 1 2 5 1
   (A) System privileges (B) Object privileges
   (C) Admin privileges (D) Class privileges

25. _____ is achieved by distributing privileges for accomplishing a task to different people. 1 1 5 1
   (A) Principle of least privilege (B) Privilege escalation
   (C) Separation of duties (D) Principle of maximum privilege

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

26. a. Classify each of the following as a violation of confidentiality, of integrity, of availability or of some combination thereof. 10 4 1 4
   (i) John copies Mary's homework
   (ii) Paul crashes Linda's system
   (iii) Carol changes the amount of Angelo's check from $100 to $10,000
   (iv) Give Forges Roger's signature on a deed
   (v) Rhonda registers the domain name "Person.com" and refuses to let he publishing house buy or use the domain name
   (vi) Jonah obtains peter's credit card number and has the credit card company cancel the card and replace it with another card bearing a different account number