REG.NO.:

SLOT: G1

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING
CONTINUOUS ASSESSMENT TEST - II
FALL SEMESTER 2024-2025

Programme Name & Branch	**:**	**B.TECH (CSE)**	
Course Code and Course Name	**:**	**BCSE317L INFORMATION SECURITY**	
Faculty Name(s)	**:**	**Dr. T. JOSHVA DEVADAS**	
Class Number(s)	**:**	**VL2024250102071**	
Date of Examination	**:**	**19/10/2024**	
Exam Duration	**:**	**90 minutes**	**Maximum Marks: 50**

General instruction(s):

- Answer All Questions
- M - Max mark; CO – Course Outcome; BL – Blooms Taxonomy Level (1 – Remember, 2 – Understand, 3 – Apply, 4 – Analyse, 5 – Evaluate, 6 – Create)
- Course Outcomes (Type the CO statements covered in this question paper. Use the CO number as per the syllabus copy)

Q. No	Question	M	CO	BL
1.	You are tasked with designing a Trusted Operating System (TOS) for a healthcare organization that manages sensitive patient information. This organization must comply with strict regulations such as HIPAA, ensuring that patient data is kept confidential, secure, and accessible only to authorized personnel. The system should also facilitate efficient workflows for healthcare providers while minimizing the risk of data breaches. What key design principles and mechanisms would you implement in the Trusted Operating System to ensure compliance with healthcare regulations, protect patient data, and maintain usability for healthcare professionals? Provide a detailed explanation of your approach, including specific features and technologies that would address these requirements.	10	CO4	BL3
2.	You are the IT manager for a small e-commerce company that operates primarily online and has recently begun to expand its customer base. The company wants to improve its network security without incurring significant costs. The main concerns are protecting the internal network from external threats and managing access to specific services based on IP addresses. The company processes sensitive customer information, including payment details, and needs a reliable solution to mitigate basic threats. Given the company's budget constraints and security requirements, would you recommend implementing a packet-filtering gateway as the primary firewall solution? Justify your choice by discussing how a packet-filtering gateway works and how it addresses the company's specific needs.	10	CO4	BL4
3.	A financial services company, FinSecure Corp., has a network that processes sensitive financial data. The company has recently experienced unauthorized access attempts on its internal servers, raising			

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING
CONTINUOUS ASSESSMENT TEST - II
FALL SEMESTER 2024-2025

---

	concerns about potential data breaches. To enhance security, FinSecure decides to implement an Intrusion Detection System (IDS). For the given the scenario, which type of Intrusion Detection System (IDS) would be most appropriate for FinSecure Corp. to protect its internal servers, and how would it be implemented to effectively monitor and respond to unauthorized access attempts?	10	CO4	BL3
4	a) A healthcare organization, HealthSecure, manages a large database containing sensitive patient information, including personal identification, medical history, and treatment records. Recently, the organization has experienced increasing concerns about data privacy and the risk of unauthorized access to this sensitive information. Discuss the various strategies HealthSecure can implement to prevent the disclosure of database information, focusing on both technical and organizational measures.	6	CO5	BL4
	b) Illustrate how the database reliability and integrity can be viewed? Explain with an example	4		

5	A university library management system allows users to search for books by title or author through a web application. The application uses a database to store information about books, including their titles, authors, and availability. The search feature directly constructs an SQL query using user input without any sanitization or parameterization. For instance, the code looks like this:
	`SELECT * FROM books WHERE title LIKE '%{user_input}%';`
	When a user enters a search term, `user_input` is directly incorporated into the SQL query. An attacker can exploit this vulnerability by entering the following input in the search bar:
	`' OR '1'='1`
	This input transforms the SQL query to:
	`SELECT * FROM books WHERE title LIKE '%'' OR '1'='1'%';`
	The modified query now returns all records from the `books` table because the condition `'1'='1'` is always true, allowing the attacker to retrieve all book records, including sensitive information.
	With this SQL Injection the attacker can view all book records, including private information if any exists. Also, If the application has additional vulnerabilities, the attacker might exploit this to gain access to more sensitive data or manipulate the database. Explain how the Prevention of SQL Injection Attack is applied to the given scenario.
		10	CO5	BL5

****