CONTINUOUS ASSESSMENT TEST - II
WINTER SEMESTER 2025-2026

ogramme Name & Branch : B. Tech & CSE
urse Code and Course Name : BCSE317L & Information Security
culty Name(s) : Prof. S M Farooq, Prof. Siva Sankari S
ass Number(s) : VL2025260502021, VL2025260502029
ate of Examination : 17-Mar-2026
xam Duration : 90 minutes

Maximum Marks: 50

eneral 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:

CO4: Differentiate the needs and application of security in Operating System and Firewalls

CO5: Analyze various method of securing databases.

Q. No	Question	M	CO	BL
1.	a) A directory is also an object to which access should be controlled. Why is it not appropriate to allow users to modify their own directories?	5	CO4	BL4
	b) If two users share access to a segment, they must do so by the same name. Must their protection rights to it be the same? Why or why not?	5	CO4	BL4
2.	a) What security advantage occurs from a packet's containing the source NIC address and not just the destination NIC address?	3	CO4	BL4
	b) Do firewall rules have to be symmetric? That is, does a firewall have to block a particular traffic type both inbound (to the protected site) and outbound (from the site)? Why or why not?	2		
	c) A distributed denial-of-service attack requires zombies running on numerous machines to perform part of the attack simultaneously. If you were a system administrator looking for zombies on your network, what would you look for?	3		
	d) Can a firewall block attacks that use server scripts, such as the attack in which the user could change a price on an item offered by an e-commerce site? Why or why not?	2		
3.	a) A multinational company hosts its e-commerce platform in a centralized data centre. Recently, the security team noticed unusual traffic patterns where a large number of requests are coming from unknown IP addresses attempting login attempts repeatedly. The firewall is allowing the traffic since it appears as normal HTTP requests. i) Identify which type of IDS would be most suitable to detect this attack. ii) Explain how the IDS would analyse the traffic and detect suspicious activity. iii) Suggest how integrating an Intrusion Prevention System (IPS) can mitigate this attack in real time.	5	CO4	BL4

Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

REG.NO.:

SLOT: C2 + TC2

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING
CONTINUOUS ASSESSMENT TEST - II
WINTER SEMESTER 2025-2026

	b) A university campus network experienced a malware outbreak that spread rapidly between student computers after one compromised machine connected to the internal network. i) Explain how a Network-based IDS (NIDS) could detect malware propagation. ii) Discuss the strengths of IDS in detecting such attacks. iii) Explain the limitations of IDS in preventing the malware from spreading.	5		
4.	a) Can a database contain two identical records without a negative effect on the integrity of the database? Why or why not?	3	CO5	BL5
	b) Suppose query Q1 obtains the median m1 of a set S1 of values, and query Q2 obtains the median m2 of a subset S2 of S1. If m1 < m2, what can be inferred about S1, S2?	4		
	c) In an airline reservation system, multiple users may attempt to reserve the same seat simultaneously. Without proper control, this may lead to double booking, where the same seat is assigned to two passengers. Using a two-step commit (or two-phase commit/locking approach) how can we ensure that seat assignments remain consistent and conflict-free.	3		
5.	An online banking web application allows users to log in using a username and password. The login page sends the following SQL query to the database: SELECT * FROM Users WHERE username = 'input_username' AND password = 'input_password'; Recently, several unauthorized users were able to log in without valid credentials by exploiting a SQL Injection vulnerability. Analyze how an attacker could manipulate the input fields to bypass the authentication mechanism using SQL Injection, explain the impact such an attack could have on the confidentiality, integrity, and availability of the database system and finally propose a secure design approach for the login module that prevents SQL Injection attacks.	10	CO5	BL6