

**VIT**Vellore Institute of Technology
(Deemed to be University under Section 3 of UGC Act, 1956)**SCHOOL OF COMPUTER SCIENCE AND ENGINEERING**
CONTINUOUS ASSESSMENT TEST - II
WINTER SEMESTER 2024-2025

REG.NO.: 22BC10017

SLOT: B1

Programme Name & Branch : B.Tech CSE
Course Code and Course Name : BCSE317L Information Security
Faculty Name(s) : --
Class Number(s) : Common for all batches
Date of Examination : 17-03-2025 2 to 3.30PM
Exam Duration : 90 minutes

Maximum Marks: 50

General instruction(s):

- Answer All Questions

Q. No	Question	M
1.	Consider that you are assigned the task to design the security architecture for a new operating system intended for use in a VIT Entrance Examinations. The system will need to handle student information and support a variety of user roles with different security aspects. Additionally, the operating system will run in an environment where potential security threats, such as rootkits, are a serious concern. A) Which type of security design would you prefer for this sensitive environment, and why? Discuss the potential trade-offs of both designs in terms of security and performance (6 Marks). B) Discuss the challenges of detecting and mitigating rootkits in a trusted system. How Rootkit Evades Detection solves the challenges? (4 Marks)	10
2.	ABC Inc is a multinational cybersecurity consultant which handles sensitive client data and financial transactions. The company has recently faced multiple cyber-attacks, including attempts to exploit vulnerabilities in their internal network. To address these concerns, the company has decided to design a robust security infrastructure using firewalls. The company needs to ensure that its network is adequately protected against both internal and external threats, while maintaining high performance and scalability across its various global branches. A) What type of firewall would you recommend for the company's internal network? Discuss the advantage of your proposed system with neat diagram (6 Marks) B) Compare your proposed firewall with other types of firewalls. Discuss the pros and cons. (4 Marks)	10
3.	XYZ Inc, is a large e-commerce platform that handles sensitive customer data. Recently, the company faced several cyber-attacks including DDoS attacks. In response to the above, the company decides to implement an Intrusion Detection and Prevention System to safeguard its infrastructure. A) Which types of IDS would you recommend for monitoring traffic, detecting attacks, and ensuring system integrity? (3 Marks) B) Discuss the strengths and limitations of both IDS and IPS. (3 Marks)	10



VIT

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

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

REG.NO.:

SLOT: B1

	C) What challenges might you face in terms of false positives/negatives? How would you address these challenges to ensure that the IDS/IPS solution remains effective? (4 Marks)	
4.	Consider that you are working as a lead security consultant for a web application development agency which will handles sensitive user data (such as personal information, financial records, and login credentials). The application currently lacks proper input sanitization mechanisms, and it is identified that the login page is vulnerable to SQL Injection attacks. Provide a detailed report on: A) How can the attackers access the database using SQL queries? Describe in detail with sample SQL queries (5 Marks). B) Recommend the comprehensive mitigation strategies for addressing SQL Injection (5 Marks).	10
5.	A company processes payroll every month, where employees are paid based on their work hours, overtime, and bonuses. The payroll system must track departmental budgets to ensure that the payroll expenses are within allocated limits. Here are the steps to be followed for processing the new payroll for the month: ● The payroll department checks the employee database to gather the required information for all employees, including their regular hours worked, overtime, bonuses, and tax deductions for the current month. If the necessary information is not available or incomplete, the transaction is rejected, and the payroll processing is halted. ● Once the necessary data is confirmed, the payroll system calculates the total gross pay. ● Also, the payroll system calculates deductions for taxes, and deducts the calculated tax from the employee's gross pay to determine the net pay. The net pay is then stored in the employee database under each employee's payroll record. ● The payroll department checks the total payroll expense for the month against the available budget. If the total payroll exceeds the budget, the transaction is rejected, and raise a fund transfer request to the CEO. ● If the total payroll within the budget, the payroll department issues a payment to each employee. Provide a detailed report of two-phase update method with suitable flag for maintaining the reliability of the above database system.	10
