REG.NO.:

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 -I
WINTER SEMESTER 2024-2025

SLOT: B2+TB2

Programme Name & Branch : **B. Tech. - ALL**
Course Code : **BCSE317L**
Course Name : **Information Security**
Faculty Name(s) : **Common to ALL**
Class Number(s) : **Common to ALL**
Date of Examination : **28.01.2025**
Exam Duration : **90 minutes** **Maximum Marks: 50**

General instruction(s): Answer ALL the questions, each carrying 10 marks. The marks for each sub-question are indicated in square brackets [ ]

Q. No	Question	Marks	Course Outcome (CO)	Bloom's Taxonomy (BL)
1.	For the VTOP web application, which automates a range of services for faculty members, students, and administrators: a. Who are the potential attackers that might target this application? [2] b. What motivations might drive these attackers to compromise the application? [2] c. What types of harm could these attackers intend to inflict on the system and its users? [2] d. What vulnerabilities could attackers exploit to achieve their malicious objectives? [2] e. What security controls and mitigation strategies would you recommend to protect the application from such attacks? [2] ANS: a. Potential attackers: Hackers, disgruntled employees, competitors, or cybercriminals. b. Motivations: Financial gain, data theft, revenge, reputation	10	CO1	BL3

	damage, or disruption of services. c. Types of harm: Data breaches, unauthorized access, system downtime, or loss of sensitive information. d. Vulnerabilities: Weak passwords, SQL injection, unpatched software, or insecure APIs. e. Security controls: Use multi-factor authentication, implement encryption, conduct regular security audits, patch vulnerabilities, and monitor for suspicious activities.			
2	You encounter the following situations: **Scenario 1**: You receive an email from a senior manager with an attached PDF for review. Upon opening, a "Launch File" dialog box appears with suspicious characteristics, such as blank lines and a scroll bar. **Scenario 2**: You receive an email claiming to be from your bank, stating that your internet banking access has been blocked due to invalid login attempts. The email urges you to click a link to restore access and avoid permanent account closure. **Scenario 3**: You find an interesting game application on a free marketplace. During installation, the app requests permissions to "Send SMS messages" and "Access your address book." **Questions:** a. What types of cybersecurity threats are present in these scenarios, and how do they exploit user behavior? [3] b. How can you verify the legitimacy of such communications or applications without compromising your security? [3] c. What preventive measures can you take as a developer to mitigate these types of cybersecurity risks? [4] ANS:	10	CO1	BL4

	a. Types of Cybersecurity Threats and Exploitation of User Behavior: Scenario 1: Phishing or malware delivery through malicious attachments. Exploits curiosity and trust in emails from senior management. Scenario 2: Phishing attack using social engineering to create urgency and fear of account loss. Scenario 3: Spyware or data theft. Exploits the user's interest in free applications and disregard for permissions. b. Verifying Legitimacy Without Compromising Security: Verify the sender's email address and check for red flags (e.g., grammar errors or unexpected requests). Contact the organization directly using official channels, avoiding links or attachments in suspicious emails. Research the app and developer, review permissions carefully, and check user reviews before installation. c. Preventive Measures for Developers: Use secure coding practices to prevent malware injections and enforce app permissions. Educate users about phishing and secure communication methods. Implement multi-factor authentication (MFA) and monitor unusual behavior in apps.			
3.	Design an authentication and key management system for a cloud-based banking application accessible through mobile devices and web browsers. The system must ensure the security of sensitive transactions and provide protection against cyber threats, including man-in-the-middle attacks, replay attacks, and unauthorized access. The authentication mechanism should incorporate robust user	10	CO1	BL3

	verification, while the key management strategy should address secure key exchange and effective key management practices. ANS: To design an authentication and key management system for a cloud-based banking application: Authentication Mechanism: Use multi-factor authentication (MFA) combining biometrics (fingerprint/face ID), device-based authentication (trusted devices), and one-time passwords (OTPs). Implement secure session management with unique tokens for each login session. Key Management: Employ asymmetric encryption (e.g., RSA or ECC) for secure key exchange, and symmetric encryption (e.g., AES) for encrypting sensitive data. Use a robust key management system (KMS) with frequent key rotation, secure storage (e.g., HSM), and policies to revoke compromised keys. Security Measures: Protect against man-in-the-middle attacks with TLS/SSL encryption, replay attacks with nonces or timestamps, and unauthorized access through continuous user behavior monitoring and session validation.			
4.	A university aims to secure its student portal's password system against brute force, dictionary, and rainbow table attacks. Answer the following: a. Why is a storing plain text password insecure? [2] b. How do rainbow table attacks work, and how does salting prevent them? [2] c. What is the difference between salt and pepper, and how do they	10	CO1	BL2

	enhance password security when used together? [2] d. If passwords are 3 uppercase letters long, how long would a brute force attack take if testing each password takes 5 seconds? [2] e. What is the recommended password length for best security practices? [2] ANS: a. Storing plain text passwords is insecure because if the database is compromised, attackers gain immediate access to all user accounts without needing further effort. b. Rainbow table attacks use precomputed hash values to quickly find the original password. Salting adds a unique, random value to each password before hashing, making precomputed tables ineffective. c. Salt is a random value unique to each password, while pepper is a secret value shared across all passwords. Together, they enhance security by countering precomputed attacks (salt) and adding an extra layer of unpredictability (pepper). d. There are 26^3=17,576 possible passwords. At 5 seconds per test, a brute force attack would take 17,576×5=87,880 seconds or approximately 24.4 hours. e. The recommended password length for best security practices is at least 12-16 characters with a mix of upper- and lowercase letters, numbers, and special symbols.			
5.	Evaluate the complexity (Easy/Moderate/Hard) of performing various operations, including **determining authorized access during execution, adding access for a new subject, deleting access for a subject, creating a new object with default access for all subjects, and revoking all access to an object.** The evaluation should consider the following access control	10	CO1	BL5

mechanisms: **per-subject access control list, per-object access control list, and access control matrix**. Provide justification for the complexity classification of each operation.

ANS:

Operation	Per-Subject ACL	Per-Object ACL	Access Control Matrix	Justification
Determine authorized access	Moderate	Easy	Easy	Per-subject ACL requires searching multiple lists; per-object ACL and matrix provide direct access.
Add access for a new subject	Easy	Moderate	Hard	Per-subject ACL updates one list; per-object ACL requires updates across objects; matrix adds a row.
Delete access for a subject	Easy	Moderate	Hard	Per-subject ACL deletes from one list; per-object ACL requires updates across objects; matrix deletes a row.
Create a new object with default access	Moderate	Easy	Hard	Per-subject ACL updates lists for all subjects; per-object ACL adds one list; matrix adds a column.
Revoke all access to an object	Hard	Easy	Moderate	Per-subject ACL requires searching all lists; per-object ACL directly deletes one list; matrix deletes a column.

****

REG.NO.:

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 -I
WINTER SEMESTER 2024-2025

SLOT: B2+TB2

NOTE*: Please refer below to the BL – Bloom's Taxonomy Levels and report the respective level in the questions for moderation. After the moderation from the school office, kindly remove the COs and BLs in the final copies, which are supposed to be distributed to the students.

Bloom's Taxonomy Levels	Category
BL1	Remembering
BL2	Understanding
BL3	Applying
BL4	Analysing
BL5	Evaluating
BL6	Creating