VIT

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

REG.NO.:

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

SLOT:B1+TB1

Programme Name & Branch	: B.Tech (CSE) & BCE,BCI
Course Code and Course Name	: BCSE317L & Information Security
Faculty Name(s)	: Common to ALL
Class Number(s)	: VL2024250501840 & others
Date of Examination	: 27/01/25
Exam Duration	: 90 minutes

Maximum Marks: 50

General instruction(s):

Answer All Questions

Q. No	Question	M
1.	Name and narrate the approach of the cybersecurity model that is a foundation for developing security policies to protect data and access. (7) Also, categorise the below-mentioned vulnerabilities whichever meet the above said potentials. (3) Man-in-the-middle attacks Phishing attacks Spyware *Unpatched software* Weak passwords *Excessive user privileges* *Ransomware* *SQL injection attacks* *Distributed denial of service (DDoS)* attacks Hardware failures *Misconfigurations* *Software bugs*	10
2.	*If a user logs in from an unusual location, the system can flag this as a potential security risk and prompt for additional authentication in real- time. Frame the necessary roles played by "Asset Management" & "Security Controls" to maintain the information security baseline for the context and point out attacker strategies involved if weak authentication found in the context.*	10
3.	*IT infrastructure services are the services that support a company's IT infrastructure, which is the collection of hardware, software, networks, and other resources that enable a company to operate. IT infrastructure services include monitoring, troubleshooting, and optimization of IT systems. And "collaborative business model" refers to a business strategy where multiple entities, like companies, individuals, or communities, work together to achieve shared goals by pooling resources, expertise, and ideas, often leveraging partnerships, networks, and shared platforms to develop products, services, or solutions that are better than what any single entity could achieve alone.* To meet the above scenario, we need directory servers that use a flexible schema. They can store a variety of attributes, including user credentials, phone numbers, group associations, and more, in a format that meets the organization's needs. In this case, what type of authentication model do you prefer to meet modern organization identity	10

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 - 1
WINTER SEMESTER 2024-2025

SLOT:B1+TB1

	management and resource-sharing needs? Illustrate with a necessary sketch.	
4	Law enforcement agencies need to visit criminal records frequently to get access to those records, in this case, Scenario 1: From a social engineering perspective, threat actors attempt to capitalize on a few key human traits to meet their goals: Trustworthiness, Credulity, Sincerity, Curiosity, Laziness Scenario 2:Malware can be installed on a resource via: Vulnerability and exploit combinations Legitimate installers or bootlegged software or media Weaknesses in the supply chain Social engineering via phishing or drive-by Internet attacks. Scenario 3:Poor misconfiguration security settings like below, Blank or default passwords for administrator or root accounts established upon initial configuration. Insecure access that is not locked down after an initial installation (often due to lack of expertise). The above techniques leads to escalate the wrong access to gain sensitive information. What all are the key components you prefer to take action against above all. Elucidate different practices and their roles available to cover the scenario.	10
5.	i) As a security analyst, we know implementing an information security policy is a nightmare. How do organizations find the compliance needed for them? Explore them in a detailed manner.(5) ii) Define comprehensive IT security policies for our VTOP. (5) Access control policy Network security policy Data security policy Physical security policy Password policy	10

****