REG.NO.:

SLOT: C2+TC2

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
FALL SEMESTER 2025-2026

Programme Name & Branch	: B.Tech. CSE
Course Code and Course Name	: BCSE410L, Cyber Security
Faculty Name(s)	: MEENAKSHI S P, SATISH C.J., JAYAKUMAR K, ILAYARAJA V, PRAKASH G
Class Number(s)	: VL2025260101802, VL2025260101781, VL2025260101777, VL2025260101874, VL2025260101786
Date of Examination	: 19-Aug-2025
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)
  CO1: Understand the emerging cybersecurity attacks and their adversarial risk
  CO2: Identify the emerging vulnerabilities and attacks, and countermeasures in cyber-physical systems.

Q. No	Question	M	CO	BL
1.	"The Indian Railway Catering and Tourism Corporation (IRCTC) has reported a serious cybersecurity breach involving unauthorized access to two of its official email accounts: tourismlko@irctc.com and mculko@irctc.com. An FIR was lodged, following a formal complaint by IRCTC officials, who alleged that the compromised emails were used to send fake complaints to government authorities." Build an attack tree to know the motive of the attackers with respect to the overarching security concerns.	10	CO1	3
2.	How will you use the Nmap tool to obtain the following information through various scanning procedures? (Each subdivision carries 2 marks) (a) Discovery of ports that are listening (b) Identify a host's OS that is useful for an inventory sweep of your network. (c) Determine whether a remote host has a firewall enabled, and which ports are filtered (d) Check the weak points of a host through the analysis of well-known open ports (e) Perform a stealth scan for TCP information.	10	CO1	3
3.	a) Differentiate between DNS Amplification and DNS Reflection attack.	5	CO2	4
	b) Your organization operates a popular e-commerce website. Suddenly, your website becomes unresponsive, and customers flood your support channels with complaints. What kind of attack scenario would this be? How will you assess your organization's ability to mitigate this attack?	5		

VIT®
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 - I
FALL SEMESTER 2025-2026

4.	a) Recently, your HR department reported receiving seemingly authentic requests for employee tax records. Upon closer inspection, these requests were found to be masquerading as those of senior executives. The situation warrants immediate attention, given the sophisticated nature of the attack and potential risks to employees' personal information. How will you identify and deal with this type of attack? Explain your assessment methodologies.	5	CO2	4
	b) Using any specific tool, perform the reconnaissance and enumerate the sub-domains of the vit.ac.in.	5		
5.	Compare and contrast the three social engineering attacks: (i) Phishing, (ii) Spear Phishing, and (iii) Whaling. "A bad actor may leave a USB drive infected with malware lying in an office lounge, intending for an employee to take it and install it." What type of attack is it, and how is it initiated? Justify your answer briefly.	10	CO1	4

****