VIT
Vellore Institute of Technology

REG.NO.:

SLOT: A1

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	**: BCSE319L, Penetration Testing and Vulnerability Analysis**
Faculty Name(s)	**: KUMARESAN A, PRAKASH G**
Class Number(s)	**: VL2025260101445, VL2025260101449**
Date of Examination	**: 17-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. Familiarized with the basic principles for Information Gathering and Detecting Vulnerabilities in the system.
  CO2. Gain knowledge about the various attacks caused in an application.
  CO3. Acquire knowledge about the tools used for penetration testing.

Q. No	Question	M	CO	BL
1.	Suppose a Hacker is trying to hack a company's server to gain access to all the data. How a good Penetration Tester will assess the vulnerabilities and test the server through the various steps present in the Ethical Hacking process? List the testing tools associated with each phase of Ethical Hacking.	10	CO3	4
2.	"Cybersecurity alone is no longer enough. If your business is to protect itself, it must develop cyber resilience." What must be incorporated to achieve this objective and to reduce the threats? Explain its role in the Penetration Testing Analysis.	10	CO1	4
3.	You are attacking an enterprise environment. Within this environment, you'll typically have dedicated servers that provide DNS service. Given this scenario, how will you identify the hosts that provide this service across the subnet?	5	CO1	3
	How will you enumerate the information in the mail system that is predominantly employed for dispatching emails?	5		
4.	What are all the different things you can accomplish with the Nmap port scanner? Suppose your laptop is only hosting the `sshd` and `httpd` server daemons. Assuming a standard install for these servers, which ports will be found to be open on your laptop by the Nmap port scanner?	5	CO3	3

	Why might it be unwise to scan a network too frequently with a vulnerability scanner? Write down the legal implications of using any vulnerability scanner.	5		
5.	"Someone claiming to be from an IT support company shows up at the office. They bypassed security by claiming to work with a trusted IT vendor and were called in to respond to an IT emergency. They then manage to gain access to this company's physical hardware and use a "USB Rubber Ducky" to execute malicious software on the company's computer." What is this type of attack scenario? Explain the impact of the above use case with your justifications.	10	CO2	4

****