REG.NO.: 22BCI0160

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: F1

Programme Name & Branch	: B.Tech Computer Science and Engineering
Course Code and Course Name	: BCSE319L Penetration Testing and Vulnerability Analysis
Faculty Name(s)	: Dr. Prakash G , Dr. Satish C J
Class Number(s)	: VL2024250501988, VL2024250501983
Date of Examination	: 1-FEB-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
  1. Familiarized with the basic principles for Information Gathering and Detecting Vulnerabilities in the system
  2. Gain knowledge about the various attacks caused in an application.
  3. Acquire knowledge about the tools used for penetration testing.

Q. No	Question	M	CO	BL
1.	What is CVSS? How do you think it is significant for vulnerability assessment? Detail three different types of scans that you can perform for vulnerability assessment using Nessus.	10	1	2
2.	Elaborate on how a DNS query is resolved? Detail the various types of DNS records. List the tools and commands that you can use for DNS enumeration.	10	2	1
3.	a) What is a social engineering attack? Detail the following types of social engineering attacks and its countermeasures • Pretexting • Whaling • Baiting • Phishing. • Dumpster Diving	10	2	1
4.	A vulnerable linux machine is accepting requests on these open ports: 21, 22, and 3306. Illustrate how you can use NMAP scripts to gain further information about this system. Provide a minimum of two scripts for each service using the open ports.	10	2	4
5.	Illustrate how you would use password cracking tools to crack the password for the following scenarios: • A file containing usernames and password hashes of users as shown below *mathew:yj9T$3CQ9acVvtq.YvCdQ4Mj/q0$Ec.d5s3.9Ttws5vK4rVE7/onJc.HMGEgbx ktlbnALn1:20096:0:99999:7:::* • A system running an SSH Service that uses a commonly used username and password (for instance, the username and password may be like 'welcome' and 'qwerty')	10	3	4