VIT

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

REG.NO.:

SLOT: A1

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING
CONTINUOUS ASSESSMENT TEST - II
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	: 05/10/2025
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)

  CO3: Acquire knowledge about the tools used for penetration testing

  CO5: Determine the security threats and vulnerabilities in computer networks using penetration testing techniques.

Q. No	Question	M	CO	BL
1.	List the various red flags that will point to the MAC spoofing attack. What are the steps that should be taken if you have fallen victim to this attack?	10	CO3	2
2.	Which ARP can be used to update the ARP mappings of the other hosts on the network, and can announce its existence to the network? Discuss the use cases and their implications.	10	CO5	3
3.	a) Malice decides to perform a brute-force attack on a single 8-character, all-lowercase-letter password. The algorithm can compute and test 100,000 hashes per second. How long would this attack theoretically take?	5	CO3	4
	b) Bob spent a month generating a rainbow table for the same password criteria defined in 3 (a), which takes up 200GB of storage. With the rainbow table, each hash lookup takes only a few milliseconds. After obtaining a hash, how quickly can Bob find the password compared to the brute-force method?	5		
4.	a) For a small business without a dedicated authentication server, what is the recommended wireless security mode, and what encryption standard should be used?	5	CO5	3
	b) Why is WEP considered fundamentally broken, and what is the primary attack method used against it?	5		
5.	What payloads are used in Metasploit for the following use cases, and briefly outline how they can be used for exploitation? (i) To gain remote access to a compromised Windows OS system, (ii) To use when firewalls block outbound traffic but allow inbound connections,	10	CO5	4

REG.NO.:

SLOT: A1

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 - II
FALL SEMESTER 2025-2026

		(iii) To help bypass firewalls and deep packet inspection systems, (iv) To maintain access, escalate privileges, and run scripts, (v) To use in web application penetration testing to gain server access.				

****