REG.NO.: 21BC10046

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
WINTER SEMESTER 2024-2025

SLOT: F2

Programme Name & Branch	**: B.Tech. & BCI**
Course Code and Course Name	**: BCSE319L & Penetration Testing and Vulnerability Analysis**
Faculty Name(s)	**: Dr. Prakash G**
Class Number(s)	**: VL2024250501984**
Date of Examination	**: 21/03/2025**
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
  CO4 Learn the knowledge into practice for testing the vulnerabilities and identifying threats
  CO5 Determine the security threats and vulnerabilities in computer networks using penetration testing techniques

Q. No	Question	M	CO	BL
1.	Dresdner Bank is a major European bank with 368 different job functions and 1,300 roles. The challenge is that each employee's access privileges were manually handled at the application level. The increased use of internal apps led to significant administrative overheads. Maintaining several application-level privacy files for each user was inefficient and did not align with the overall security policy structure. What kind of Access Control mechanism can be considered for this problem? List out any 2 outcomes that the bank could achieve by implementing this Access Control system.	10	CO4	4
2.	"Hackers can change the operating system's functionality simply by adding their own programs, making it easy for hackers to steal the personal information of targeted users". What type of Rootkit is incorporated here? Explain the preventive measures that can be followed to avoid Rootkit attacks.	10	CO3	2
3.	a) How will you overcome the Ping Flood attack? Develop a strategy to protect against this attack.	5	CO3	3
	b) What is the Ping-of-Death? How will you perform a Ping-of-Death attack using the command prompt as a batch file?	5		
4.	a) Why do supplicants often get de-authenticated in a Wireless network? What tool can be used to launch this attack?	5	CO5	3
	b) Can the WPA2/WPA3 security protocols be hacked easily? If not, what is the strength of these protocols? Elucidate your justification for the same.	5		

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 - II
WINTER SEMESTER 2024-2025

SLOT: F2

5.	Consider a simple 'C' program that accepts user input to fill a character array:
	
	`void vulnerable_function(char *user_input) {`
	`  char buffer[10];`
	`  strcpy(buffer, user_input);`
	`}`
	What kind of attack can be initiated in the above code snippet? How will this code become a vulnerable function? In what ways can this attack be resolved?
		10	CO4	4

****