Code No: 157JB **R18**

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
B. Tech IV Year I Semester Examinations, December-2023/January-2024
VULNERABILITY ASSESSMENT AND PENETRATION TESTING
(Computer Science and Engineering - Cyber Security)

Time: 3 Hours **Max. Marks: 75**

Note: i) Question paper consists of Part A, Part B.
ii) Part A is compulsory, which carries 25 marks. In Part A, Answer all questions.
iii) In Part B, Answer any one question from each unit. Each question carries 10 marks and may have a, b as sub questions.

PART - A

1.a)	What are the main targets of social engineering attacks?	[2]
b)	How a social engineering attack works? Explain.	[3]
c)	What is penetration attack?	[2]
d)	What are the stages of physical penetration testing?	[3]
e)	Give a note on planning a penetration test.	[2]
f)	Explain the XPSP3.	[3]
g)	What is the biggest security threat to a web application?	[2]
h)	Give a note on Passive Analysis.	[3]
i)	What is a Honeypot technology?	[2]
j)	Give a note on Catching Malware.	[3]

PART – B

(50 Marks)

2.a)	Why you need to understand your enemy's tactics? Explain.	
b)	Discuss the Vulnerability Assessment and Penetration Testing.	[5+5]
	OR	
3.	Explain the common attacks used in penetration testing.	[10]
4.	Discuss the Automating and Scripting Metasploit.	[10]
	OR	
5.	Write the Using the Metasploit Console to Launch Exploits.	[10]
6.a)	Give a note on information sharing during a penetration test.	
b)	Draw and explain the structuring a penetration test.	[5+5]
	OR	
7.	Give a note on a) Compiling and Debugging Windows Programs. b) Local Buffer Overflow Exploits.	[5+5]

8. Explain the OWASP Top Ten SQL Injection vulnerabilities. [10]

OR

9.a) Explain the Cross-site scripting vulnerabilities.
b) Give a note on Binary Analysis. [5+5]

10.a) Describe the Internet explorer security concepts.
b) Explain the history of client- side exploits and latest trends. [5+5]

OR

11. Discuss the client-side vulnerabilities. [10]

---oo0oo---