Code No: 157JB **R18**

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

B. Tech IV Year I Semester Examinations, February - 2025

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

(25 Marks)

1.a)	What is Phishing? Explain.	[2]
b)	Differentiate between active and passive scanning.	[3]
c)	What are manned checkpoints?	[2]
d)	How to defend against insider attacks?	[3]
e)	What are the different types of buffer overflows?	[2]
f)	Explain the Dradis Framework.	[3]
g)	What are Command injection vulnerabilities?	[2]
h)	Write about the ethical reverse engineering.	[3]
i)	What is design vulnerability?	[2]
j)	What are the limitations of Honeypots?	[3]

PART – B

(50 Marks)

2.a)	Why do you need to understand your enemy's tactics? Explain.	
b)	What are the common attacks used in penetration testing? Discuss.	[5+5]
	OR	
3.a)	Describe the process of conducting a social engineering attacks.	
b)	How to defend against social engineering attacks? Discuss.	[5+5]
4.a)	How to exploiting Client-Side vulnerabilities with Metasploit?	
b)	With examples, explain automating and scripting Metasploit.	[5+5]
	OR	
5.a)	What are insider attack? How are they tested?	
b)	How Metasploit's Meterpreter is used for penetration testing? Explain.	[5+5]
6.a)	Write the testing plan for a penetration testing and explain.	
b)	Explain about Safe Structured Exception Handling (SafeSEH).	[5+5]
	OR	
7.a)	List and explain the steps followed for the exploit development process.	
b)	Explain the process of writing Windows Exploits with suitable illustrations.	[5+5]

8.a) Discuss about the common forms of injection vulnerabilities.
b) What is source code analysis? Explain about source code auditing tools. [5+5]

OR

9.a) What are SQL injection vulnerabilities? Discuss them in detail.
b) What is reverse engineering? Why should we bother about reverse engineering? Discuss. [5+5]

10.a) Write a detailed note on Mozilla Security team Fuzzers.
b) Define Malware and about different types of Malwares. [5+5]

OR

11.a) How to protect yourself from Client-Side exploits? Discuss.
b) Discuss about the latest trends in Honeypot technology. [5+5]

---ooOoo---