USN | | | | | | | | | | |

RV COLLEGE OF ENGINEERING
Autonomous Institution affiliated to VTU
V Semester B.E. Examinations
DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING
Vulnerability Assessment & Penetration Testing
(2022 SCHEME) Model Question Paper

Time: 03 Hours ***Maximum Marks: 100***

Instructions to candidates:

1. Answer all questions from Part A. Part A questions should be answered in first three pages of the answer book only.
2. Answer FIVE full questions from Part B. In Part B question number 2 is compulsory. Answer any one full question from 3 and 4, 5 and 6, 7 and 8, and 9 and 10.

		PART-A	
1	1.1	_____ is an industry-standard that vendors used to determine the severity of a vulnerability.	01
	1.2	_____ is the heart of every social engineering attack without which the attacks will not work.	01
	1.3	How do you handle zero-day vulnerabilities?	02
	1.4	List the commonly targeted ports during penetration testing. Give example.	02
	1.5	A _____ is a decoy system designed to attract attackers and collect malicious software for analysis.	01
	1.6	The process of running malware in a controlled environment to observe its behavior is called _____ analysis.	01
	1.7	A _____ attack involves injecting malicious scripts into web pages viewed by users.	01
	1.8	Differentiate between a black box, white box, and grey box penetration test.	02
	1.9	List any two measures to protect yourself from client-side exploits.	02
	1.10	Name any two tools commonly used for static source code analysis.	02
	1.11	During the execution of a penetration test, testers simulate _____ activities to identify and exploit vulnerabilities.	01
	1.12	Return-Oriented Programming (ROP) is a technique used to bypass _____ protections during buffer overflow exploits.	01
	1.13	Differentiate between static and dynamic malware analysis.	02

	1.14	List the steps involved in writing a Windows exploit.	01
PART-B			
UNIT-I			
2	a	Discuss any two common types of attacks used in penetration testing. Explain the purpose of each attack and their role in identifying vulnerabilities in an organization's security posture.	10
	b	Differentiate between Vulnerability Assessment and Penetration Testing.	06
UNIT-II			
3	a	Why is physical penetration testing important? Describe the key steps involved in conducting a physical penetration test.	08
	b	How can organizations defend against physical penetration attacks? Explain the strategies and measures organizations can implement to protect themselves from physical security breaches.	08
OR			
4	a	Describe the steps involved in planning and executing an insider attack simulation.	08
	b	What is client-side exploitation in Metasploit, and how is it performed?	08
UNIT-III			
5	a	What are the key considerations when planning a penetration test? Explain Three-Phase Penetration testing plan.	08
	b	Describe the process of exploiting a local buffer overflow vulnerability in a Linux application.	08
OR			
6	a	Explain how Structured Exception Handling (SEH) works in Windows applications and how attackers can exploit it for arbitrary code execution.	08
	b	Illustrate the significance of Data Execution Prevention (DEP) in Windows and how it can be bypassed.	08

UNIT-IV			
7	a	Illustrate the SQL Injection vulnerabilities and how they can be exploited.	08
	b	Describe the purpose and overview of OWASP Top Ten web application security vulnerabilities.	08
OR			
8	a	Explain the process of source code analysis for identifying vulnerabilities.	08
	b	Discuss the challenges of automated source code analysis. How does automated source code analysis contribute to secure software development lifecycle (SDLC)?	08

UNIT-V			
9	a	Explain the key security concepts of Internet Explorer and their role in mitigating vulnerabilities.	08

	b	Describe the evolution of client-side exploits and the latest trends in browser-based attacks.	08
		OR	
10	a	Define malware and discuss its impact on systems, organizations, and individuals. Highlight its role in modern cyberattacks.	08
	b	Explain the advancements in Honeynet and their use in malware analysis research.	08

Signature of Scrutinizer: Signature of Chairman

Name: Name: