LAB-12 ASSIGNMENT

-J.S.R JAYANTH

-19BCE7170

Lab experiment – Automated Vulnerability/Pentesting Report Generation using pwndoc

Experiment and Analysis

- **Deploy pwndoc in local or remote (public)**
- **For installation**
- **https://github.com/pwndoc/pwndoc**
- **Installation procedure**
- **https://skandashiled.medium.com/pwndoc-complete-guide-b927956d06d5**
- **For document template, you can use Default Template _ Sibi_pwndoc.docx file available in teams.**
- **Generate automated report for Lab 7 – 11**
- **Submit the auto-generated report**

Jayanth Jammula

VULNERABILITY REPORT

FRIDAY, JUNE 11,2021

MODIFICATIONS HISTORY

Version	Date	Author	Description
1.0	11-06-2021	Jayanth Jammula	Initial Version

TABLE OF CONTENTS

1. General Information 5
1.1 Scope 5
1.2 Organisation 5
2. Executive Summary 6
3. Technical Details 7
3.1 title ..... **Error! Bookmark not defined.**
4. Vulnerabilities summary 7

GENERAL INFORMATION

SCOPE

Prof. Sibi Chakkaravarthy has given us a task to perform secuirity tests

- Lab 7 to Lab 11 experiments

ORGANISATION

The testing activities were performed between 11-06-2021 and 11-06-2021.

EXECUTIVE SUMMARY{#SUMMARY}

VULNERABILITIES SUMMARY

Following vulnerabilities have been discovered:

Risk	ID	Vulnerability	Affected Scope
High	IDX-002	DDOS	
High	IDX-001	Buffer overflow	
Medium	VULN-003	Ransomware	

TECHNICAL DETAILS{#FINDINGS}

DDOS

CVSS SEVERITY	High		CVSSv3 SCORE	8.3
CVSSv3 CRITERIAS	Attack Vector :	**Network**	Scope :	**Changed**
	Attack Complexity :	**High**	Confidentiality :	**High**
	Required Privileges :	**None**	Integrity :	**High**
	User Interaction :	**Required**	Availability :	**High**
AFFECTED SCOPE				
DESCRIPTION	This is used to crash a website using multiple pinging			
OBSERVATION				
TEST DETAILS				
REMEDIATION				
REFERENCES				

Buffer overflow

CVSS Severity	High		CVSSv3 Score	8.3
CVSSv3 criterias	Attack Vector :	**Network**	Scope :	**Changed**
	Attack Complexity :	**High**	Confidentiality :	**High**
	Required Privileges :	**High**	Integrity :	**High**
	User Interaction :	**Required**	Availability :	**High**
Affected scope				
Description	This is a code level error normally made by humans due to the type casting errors. It leads to the crass of rocket ariane-5.			
Observation	This is done using steam ripper			
Test details				
Remediation				
References				

CVSS Severity	Medium		CVSSv3 Score	6.2
CVSSv3 criterias	Attack Vector :	**Physical**	Scope :	**Unchanged**
	Attack Complexity :	**High**	Confidentiality :	**High**
	Required Privileges :	**Low**	Integrity :	**High**
	User Interaction :	**Required**	Availability :	**High**
Affected scope				
Description	This is used to infect the navie windows to get the ransom.			
Observation				
Test details				
Remediation				
References				