Vulnerability Assessment Lab Report

Project Overview

This lab demonstrates how to perform a basic vulnerability assessment using Kali Linux and Metasploitable2 virtual machines. The workflow includes setting up vulnerable targets, running network scans with Nmap, identifying open ports and services, and documenting findings for security analysis.

Step 1: Environment Setup

- Open Kali Linux VM in VMware Workstation
- Open Metasploitable2 VM as the vulnerable target
- Warning: Never expose Metasploitable2 to an untrusted network

Step 2: IP Address Identification

- Use ifconfig on both Kali and Metasploitable2 to check IP addresses
- Confirm connectivity between attacker and target machines

Step 3: Nmap Scanning

- Run basic scan: nmap 127.0.0.1
- Run detailed scan with service detection: nmap -sV -sC -A <target-ip>

Step 4: Vulnerability Identification

- Identify open ports such as SSH, Telnet, HTTP, MySQL, PostgreSQL
- Document services that are outdated or misconfigured

Screenshots to Include

- Opening Kali Linux VM
- Opening Metasploitable2 VM login screen
- ifconfig output from Kali Linux
- ifconfig output from Metasploitable2
- Basic Nmap scan results
- Detailed Nmap scan results showing open ports and services

Vulnerability Assessment Lab Report

Technologies Used

- Kali Linux (attacker machine)
- Metasploitable2 (vulnerable target)
- Nmap (network scanning tool)
- VMware Workstation (virtualization platform)

Author

Aziz Ul Haq

Cybersecurity & Data Science Enthusiast

Rawalpindi, Pakistan

GitHub:

https://github.com/Azizulhaq-professional/Aziz-Cybersecurity-Labs/tree/main/01_Vulnerability_Assessment_Lab