

Task 1

Basic Vulnerability Scan Using Nmap

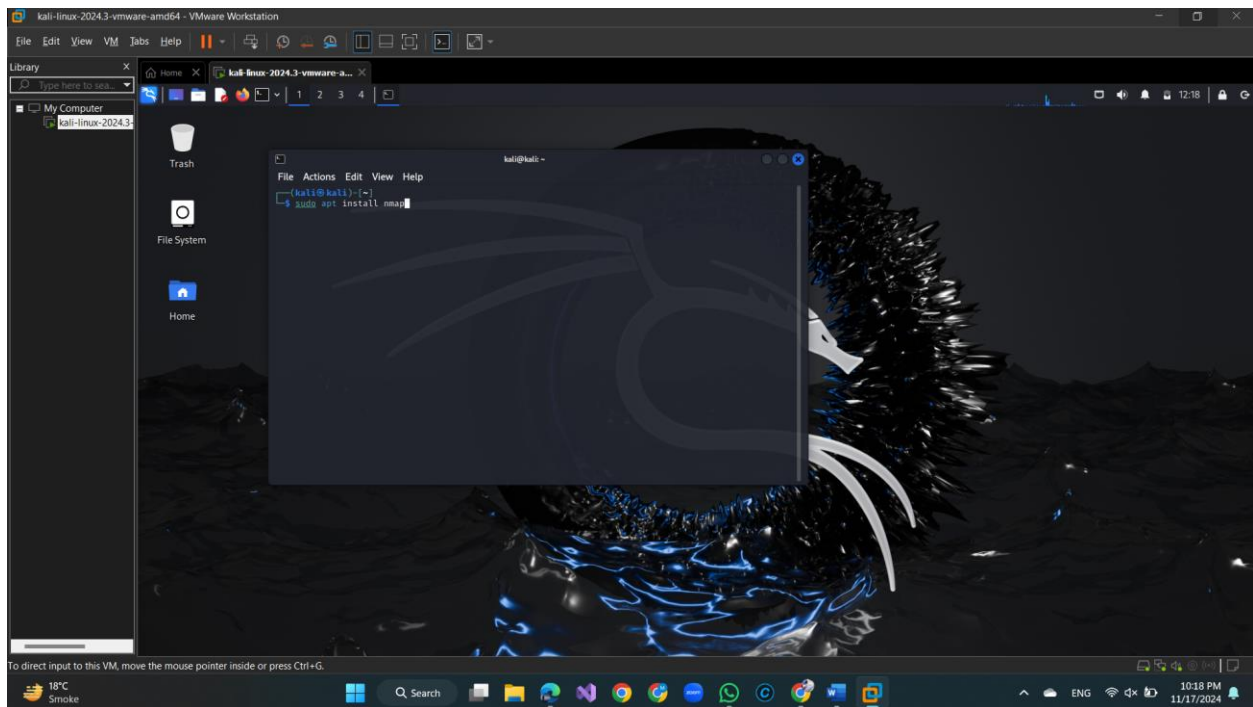
➤ Overview

In this task, I performed a basic vulnerability scan on the target IP 192.168.x.x using **Nmap**, an open-source network scanning tool. The goal was to identify open ports, detect service versions, and check for vulnerabilities.

➤ Steps

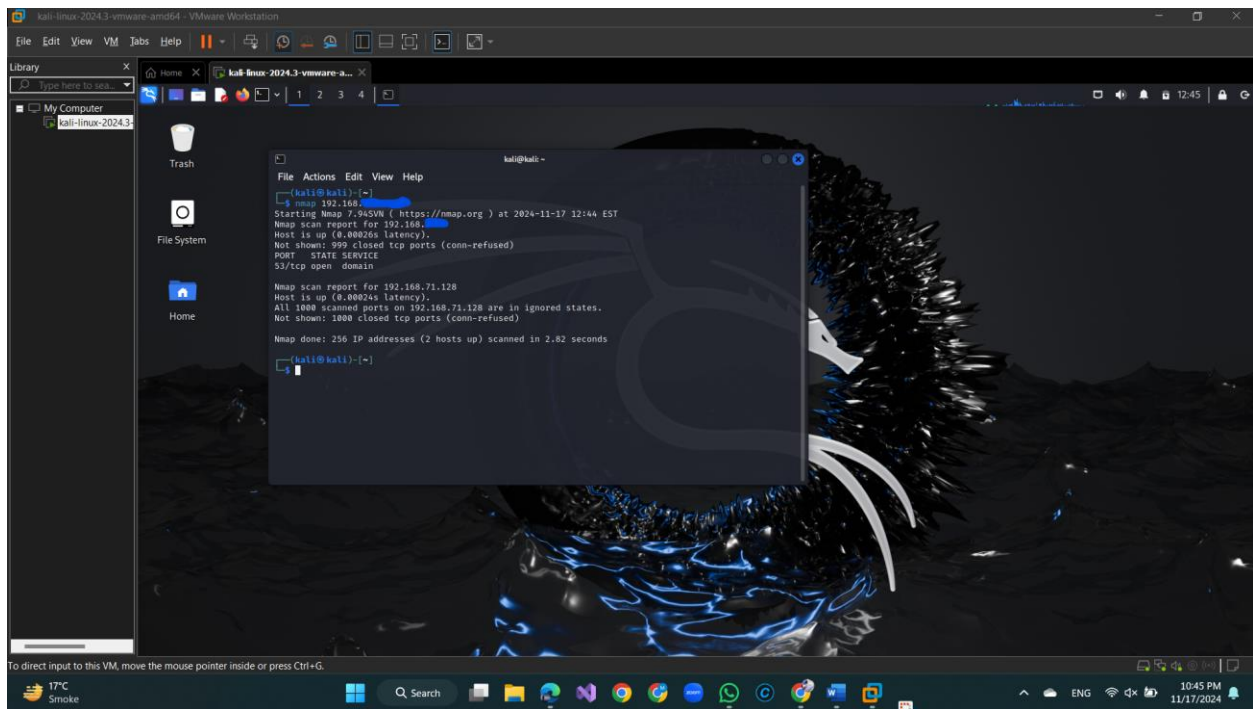
1: Installing Nmap

First, I made sure that **Nmap** was installed in my Kali Linux environment. I used the following command to install Nmap:



2: Basic Scan of the Target

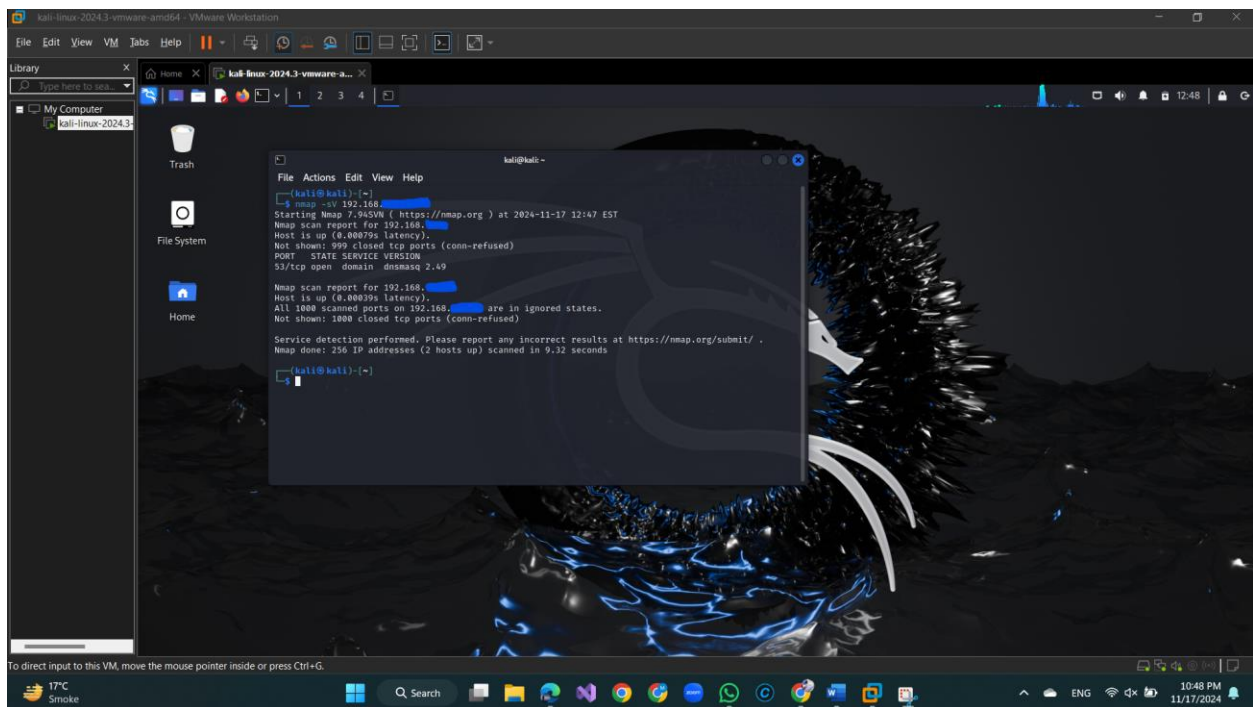
I initiated a basic scan of the target IP address to check for open ports and services:



This command provided an overview of open ports and services running on the target machine.

3: Service Version Detection

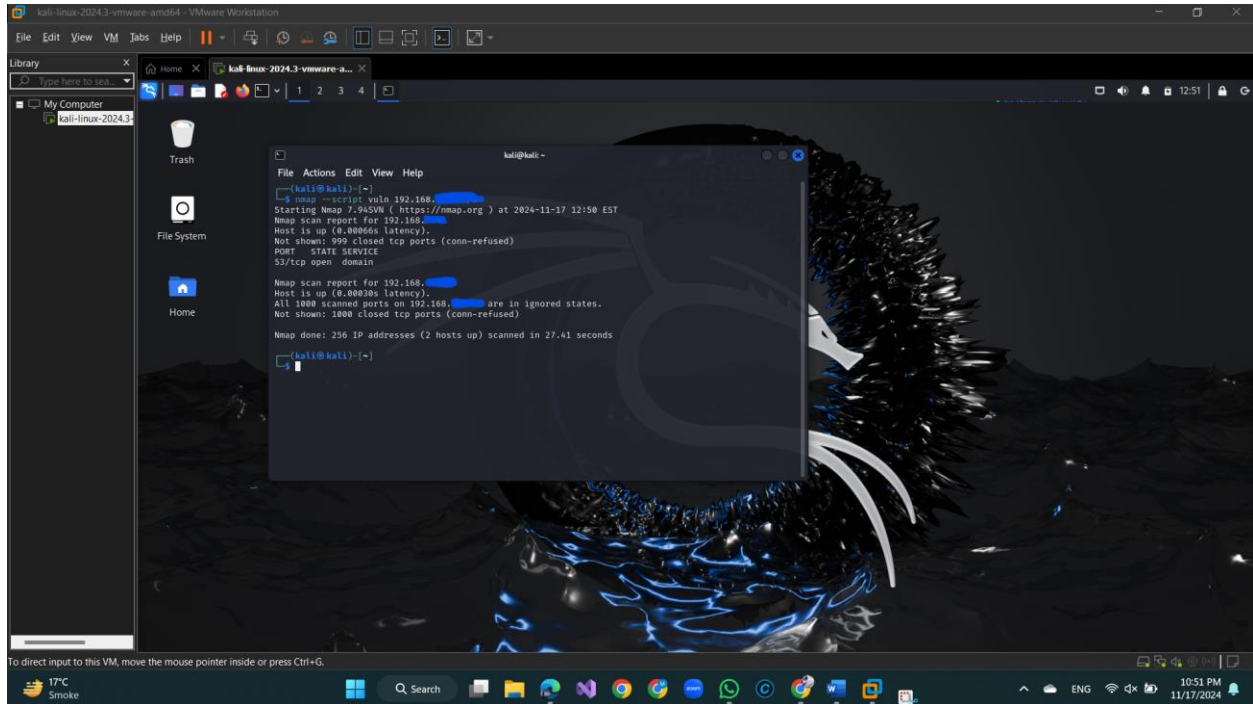
To gather more details about the services running on the open ports, I used the `-sV` flag to detect service versions:



1. This step allowed me to identify the specific versions of the services, which could be crucial for identifying vulnerabilities.

4: Vulnerability Scan

Finally, I performed a vulnerability scan using the Nmap **vuln** script:



The screenshot shows a Kali Linux virtual machine running in VMware Workstation. A terminal window is open, displaying the output of an Nmap scan using the **vuln** script. The scan was performed on the IP address 192.168.1.100. The results show that the host is up, and the scan completed successfully. The terminal output is as follows:

```
kali@kali:~$ nmap -sV 192.168.1.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-17 12:50 EST
Nmap scan report for 192.168.1.100
Host is up (0.0000ms latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
53/tcp    open  domain

Nmap scan report for 192.168.1.100
Host is up (0.0000ms latency).
All 1000 scanned ports on 192.168.1.100 are in ignored states.
Not shown: 1800 closed tcp ports (conn-refused)

Nmap done: 256 IP addresses (2 hosts up) scanned in 27.41 seconds
kali@kali:~$
```