

Task 1: Basic Vulnerability Scan

- **OBJECTIVE**

Task: Scan a network for vulnerabilities.

Details:

Use a tool like Nmap or OpenVAS to scan for vulnerabilities.

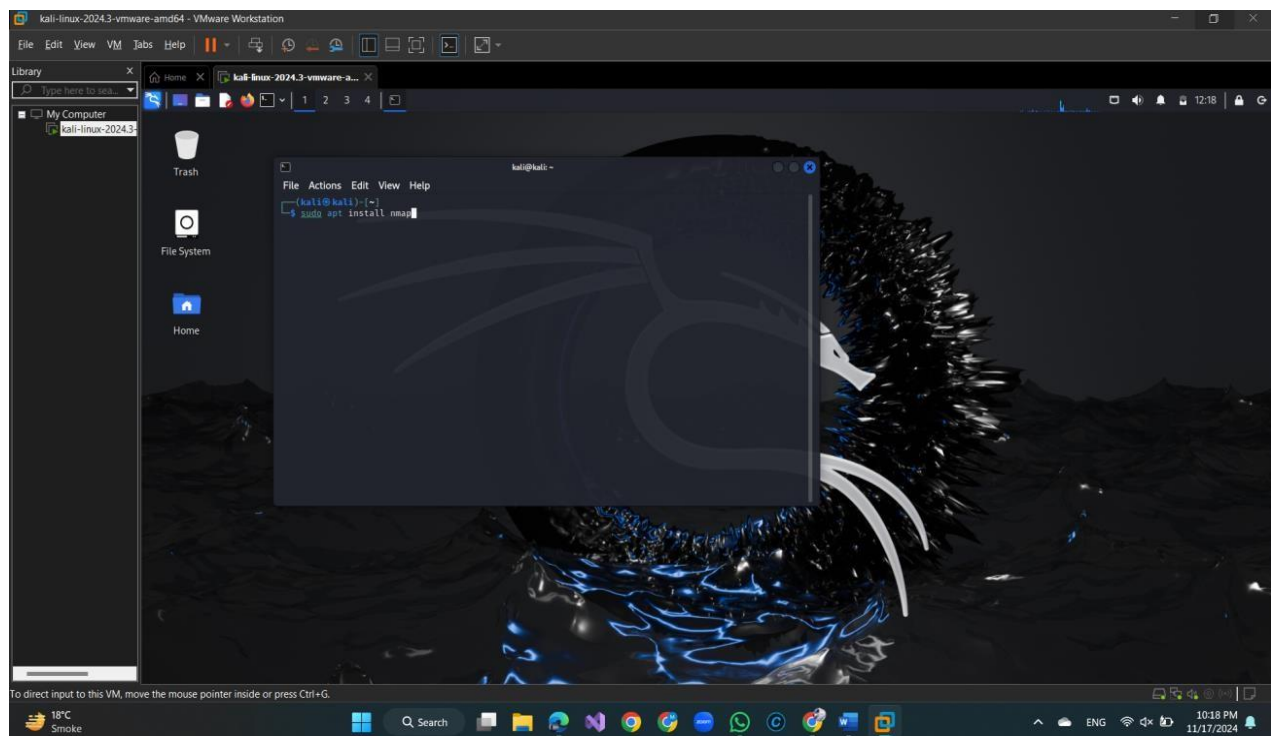
Review and interpret the scan results.

- **STEPS**

Install Nmap:

1. Installing Nmap

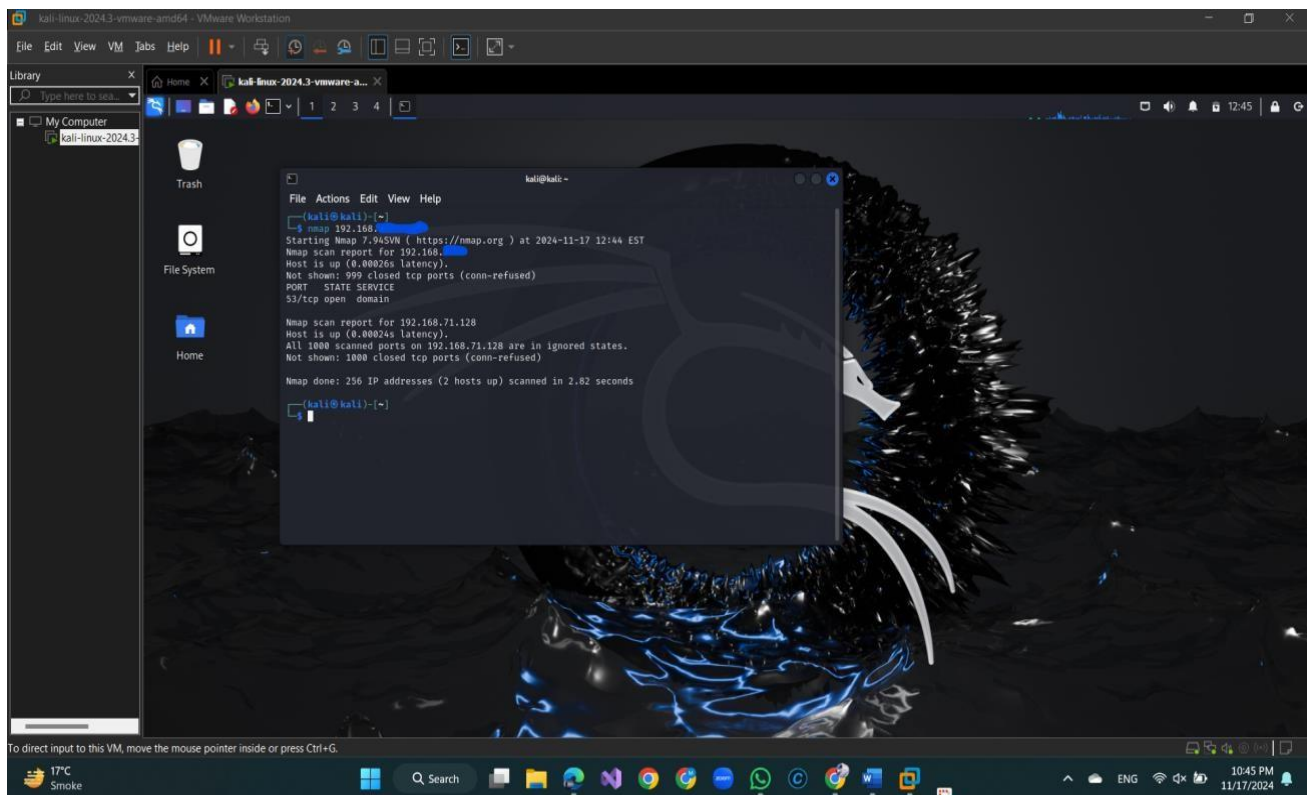
First, I made sure that **Nmap** was installed in my Kali Linux environment. I used the following command to install Nmap:



Basic Nmap Scan Commands:

2. Basic Scan of the Target

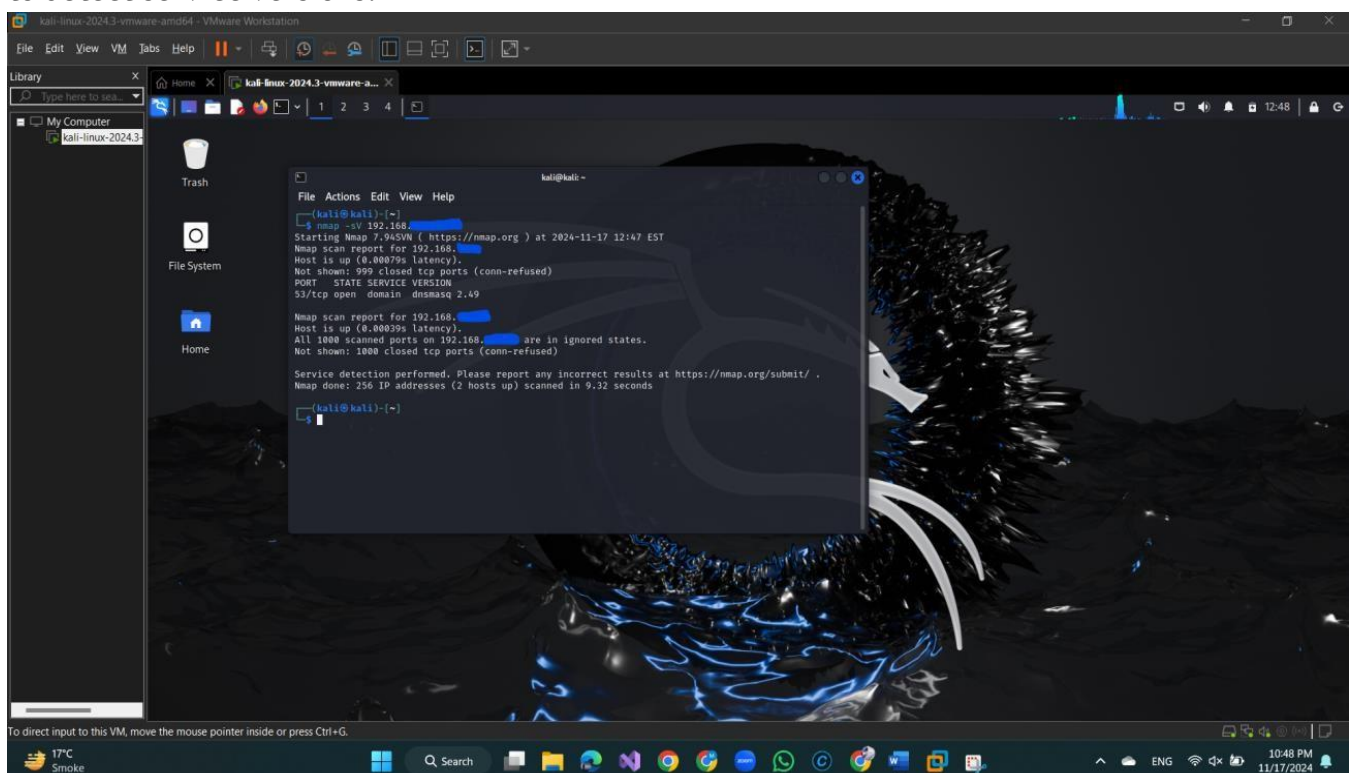
I initiated a basic scan of the target IP address to check for open ports and services:



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:

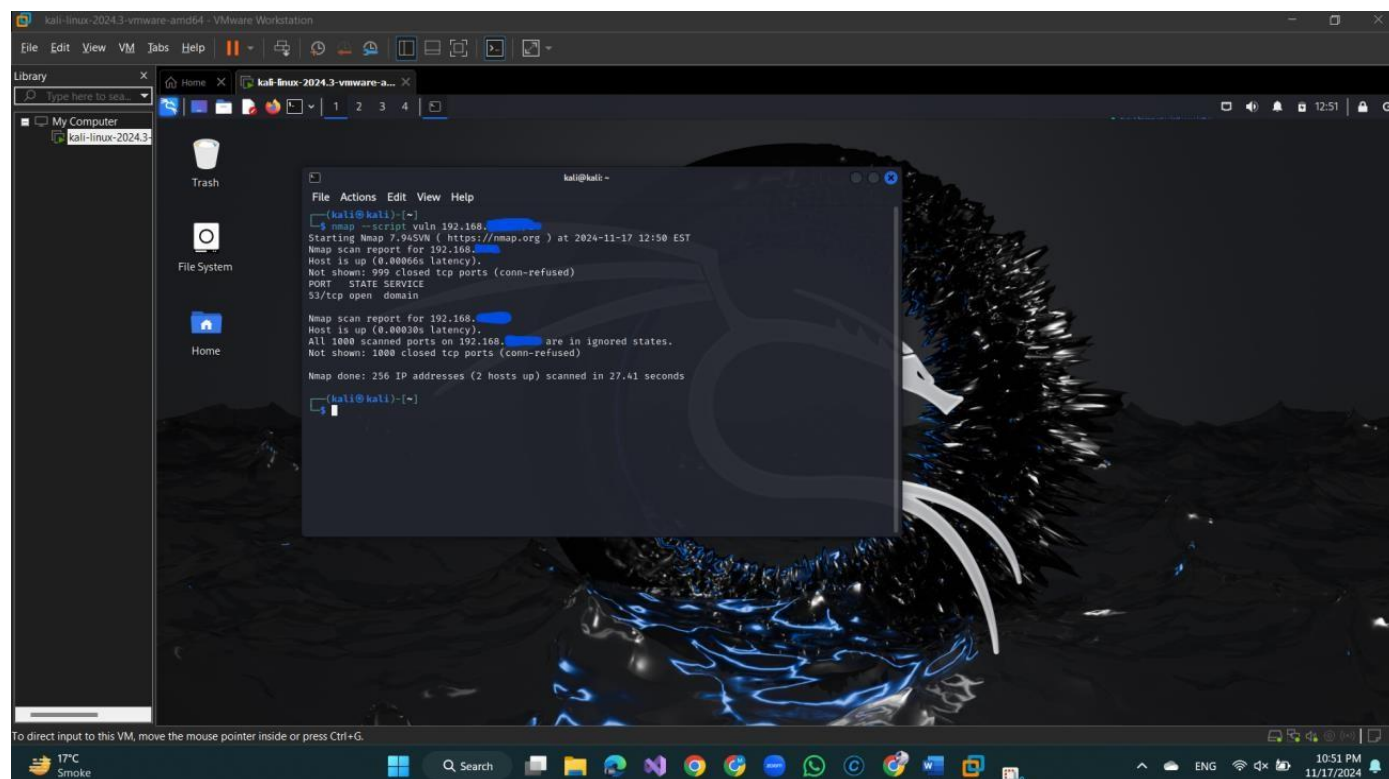


This step allowed me to identify the specific versions of the services, which could be crucial for identifying vulnerabilities.

Vulnerability Scanning with Nmap Scripts:

4. Vulnerability Scan

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

A screenshot of a Kali Linux virtual machine running in VMware Workstation. The desktop background is a dark, abstract image with blue and white patterns. A terminal window is open in the center, displaying the output of the Nmap `vuln` script. The terminal shows the command `nmap --script vuln 192.168.1.100` and its output, which includes the Nmap version (7.94SVN), the target IP (192.168.1.100), and the results of the scan. The scan shows that the host is up, all 1000 scanned ports are in ignored states, and there are 256 IP addresses (2 hosts up) scanned in 27.41 seconds. The terminal output is as follows:

```
kali@kali:~$ nmap --script vuln 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 (0.00000s 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 (0.00020s latency).
All 1000 scanned ports on 192.168.1.100 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

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

This script identifies known vulnerabilities in the services running on the target.