**Report for Project**

1. Introduction

In this we will discuss how to scan a network and discover everything connected to it by using any open source software and we have to retrieve variety of Information about what’s connected , what services each host is operating , scan the hostname, list all the hosts in a text file and identify a host’s operating system(OS). To scan a network and its information we use Nmap as a open source software. Nmap ("Network Mapper") is a free and open source  utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. It was designed to rapidly scan large networks but works fine against single hosts.

* 1. Objective of a Project

The Objective of this task is to scan a network and discover everything connected to it like identify a host’s operating system, what services each host is operating and we also have to list all the hosts in a text file.

* 1. Description of the project

To scan a network, we use Nmap as an open source software to retrieve variety of information about what connected and identify a host operating system(OS). We use few linux command to scan a network ,Real time information of a network , Detailed information of all the IPs activated on a network , Provide the list of live hosts and operating system.

Scope of the project

Scope of the project is to scan a network and retrieve variety of information using Nmap(“Network Mapper”) as an open source software.

1. System Description
   1. Target system description

Linux is the targeted system to scan a network , identify a host operating system and retrieve variety of information.

1. Analysis Report
   1. System snapshots and full analysis report
2. Open Linux as my targeted system
3. Open the terminal and Install Nmap by using yum install nmap.
4. Use nmap -sn <Ip range> to scan a network.

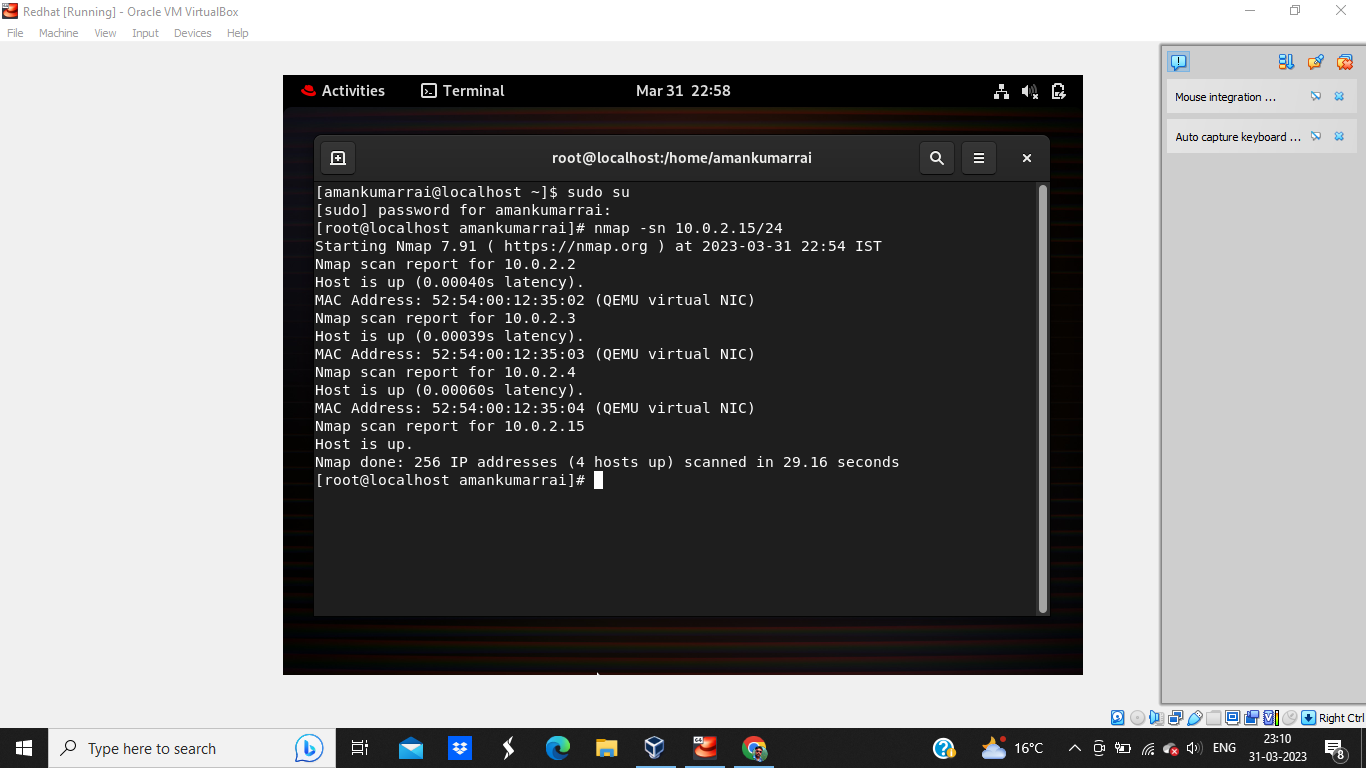


Figure 1: Scan a network.

1. Use nmap -sV <host IP> to retrieve more information like services, Version , State and port.

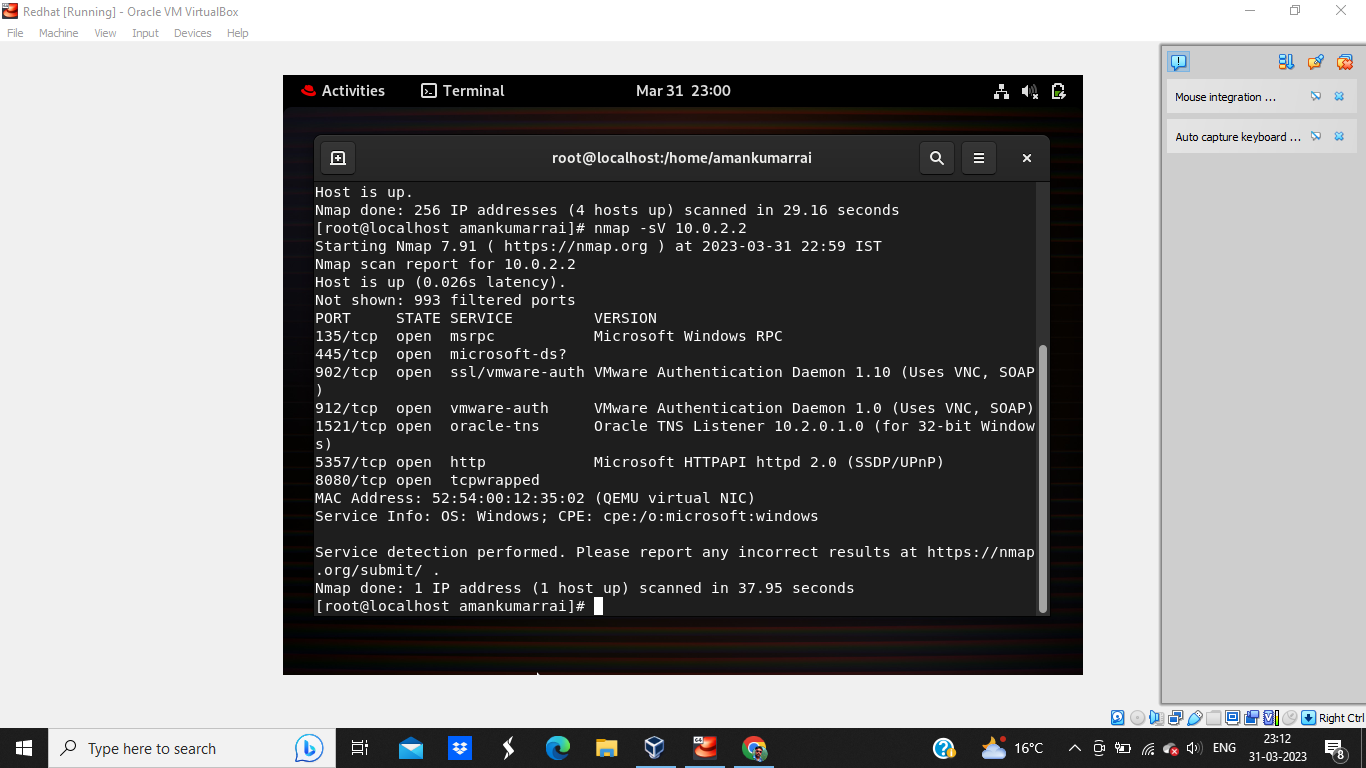


Figure 2: Information of host 10.0.2.2

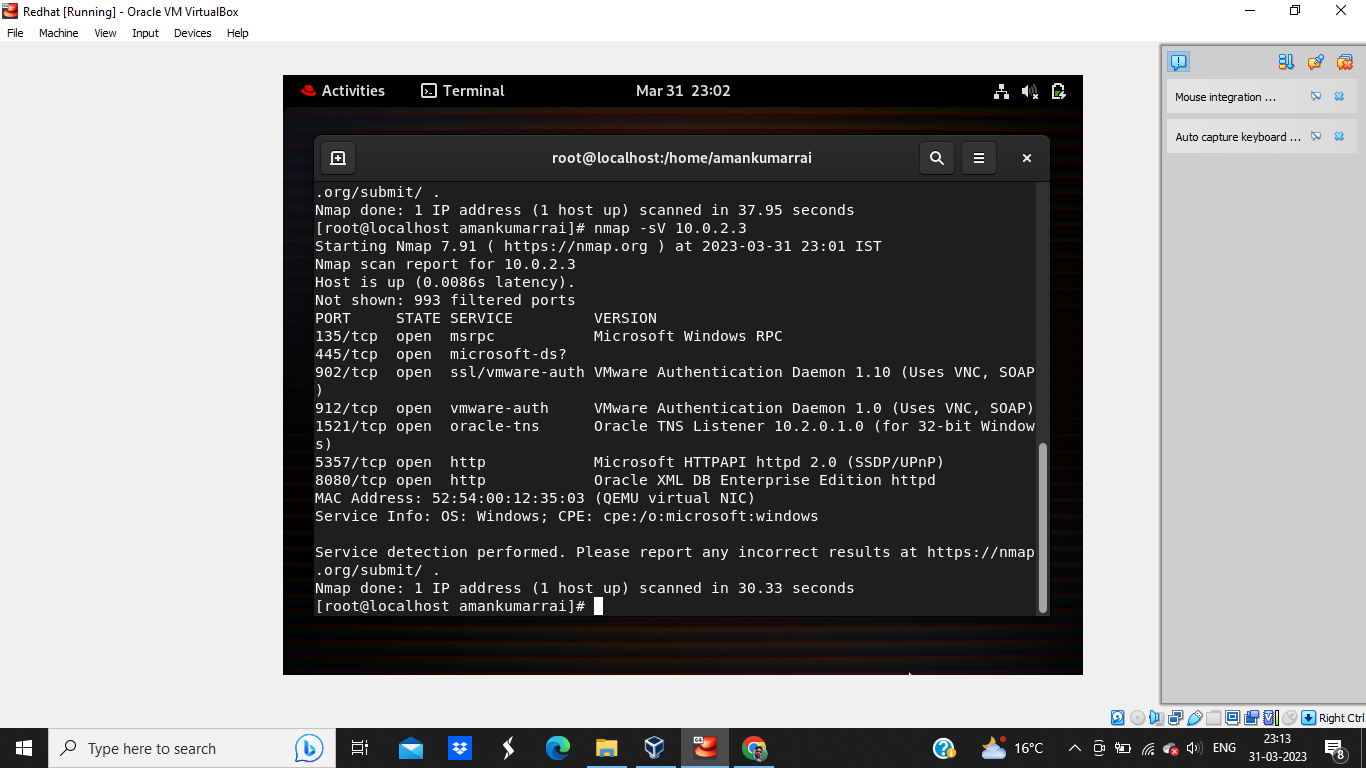


Figure 3: Information of host 10.0.2.3

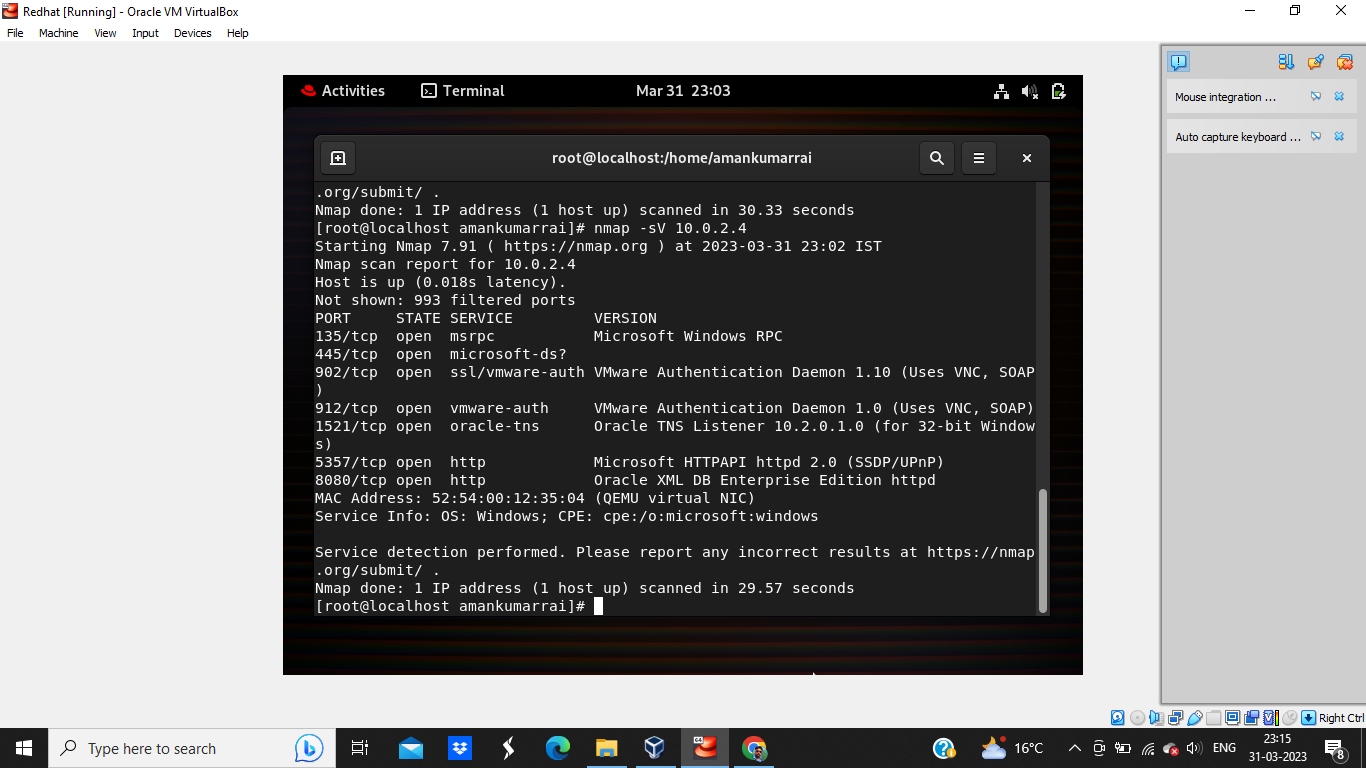


Figure 4: Information of host 10.0.2.4

Text

Description automatically generated

Figure 5: Information of host 10.0.2.15

1. Use nmap -A <IP address> to retrieve more information.

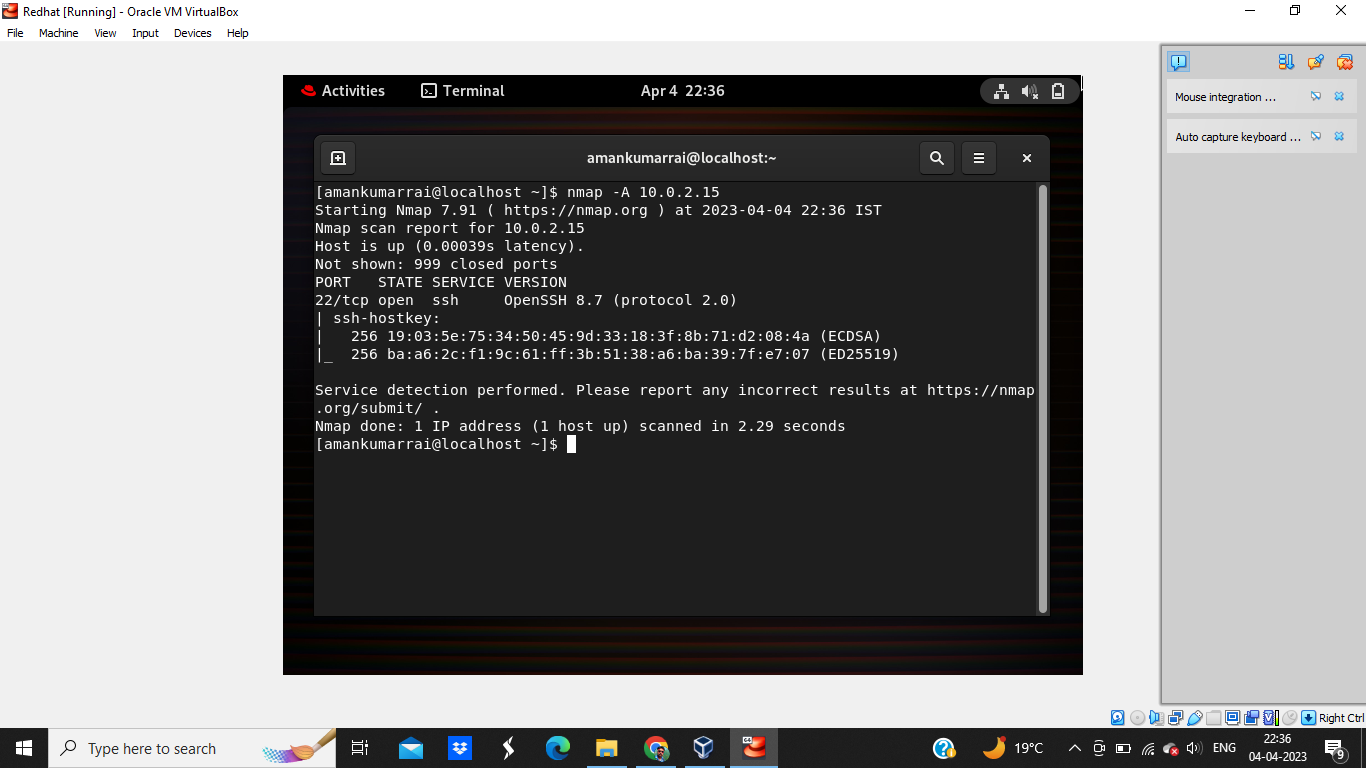


Figure 6: To retrieve more information

1. Use nmap -O <Ip address > to identify a host operating system(OS).

A screenshot of a computer

Description automatically generated

Figure 7: Identify host operating System.

1. Use nmap -sn <Ip address> -oN file.txt to list all the host in a text file.

Graphical user interface, text

Description automatically generated

Figure 8: List hosts in a text file.

1. Reference/Bibliography

<https://www.geeksforgeeks.org/nmap-command-in-linux-with-examples/>

<https://nmap.org/book/port-scanning-options.html>

GitHub Link: https://github.com/Amankumarai/ca3repo