**Garvin Chanderia**

**2203132**

**LY-ISA1**

**Assignment No.7**

**Aim:**  Use nmap to scan open ports, services, OS and version information of Target IP

**Theory:** Nmap is the world’s leading port security network scanner. The Nmap hosted security tool can help you determine how well your firewall and security configuration is working.

Prerequisites

* Linux operating system
* Access to a user account with sudo or root privileges
* Access to a command line/terminal window
* The apt package manager, included by default (Debian / Ubuntu)
* The yum package manager, included by default (Red Hat, CentOS)

On modern operating systems, ports are numbered addresses for network traffic. Different kinds of services use different ports by default.

For example, regular web traffic uses port 80, while the POP3 email uses port 110. One of the ways that a firewall works is by allowing or restricting traffic over a particular port.

Because the port configuration can cause a security risk, it’s critical to know which ports are open and which are blocked.

To **scan Nmap ports** on a remote system, enter the following in the terminal:

sudo nmap 192.168.0.1

Replace the IP address with the IP address of the system you’re testing. This is the basic format for **Nmap**, and it will return information about the ports on that system.

In addition to scanning by IP address, you can also use the following commands to specify a target:

To scan a host:

nmap www.hostname.com

To scan a range of IP addresses (.1 – .10):

nmap 192.168.0.1-10

To run **Nmap** on a subnet:

nmap 192.168.0.1/13

To scan targets from a text file:

nmap –iL textlist.txt

[Nmap commands](https://phoenixnap.com/kb/nmap-commands) can be used to scan a single port or a series of ports:

Scan port 80 on the target system:

nmap –p 80 192.168.0.1

Scan ports 1 through 200 on the target system:

nmap –p 1-200 192.168.0.1

Scan (Fast) the most common ports:

nmap –F 192.168.0.1

To scan all ports (1 – 65535):

nmap –p– 192.168.0.1

**Other Types of Nmap Port Scans**

Different types of scans can be performed:

To scan using TCP connect (it takes longer, but is more likely to connect):

nmap –sT 192.168.0.1

To perform the default SYN scan (it tests by performing only half of the TCP handshake):

nmap –sS 192.168.0.1

To instruct Nmap to scan UDP ports instead of TCP ports (the **–p switch** specifies ports 80, 130, and 255 in this example):

nmap –sU –p 80,130,255 192.168.0.1

Run a fast scan on the target system, but bypass host discovery. (Host discovery uses [ping](https://phoenixnap.com/glossary/what-is-ping), but many server firewalls do not respond to **ping** requests. This option forces the test without waiting for a reply that may not be coming):

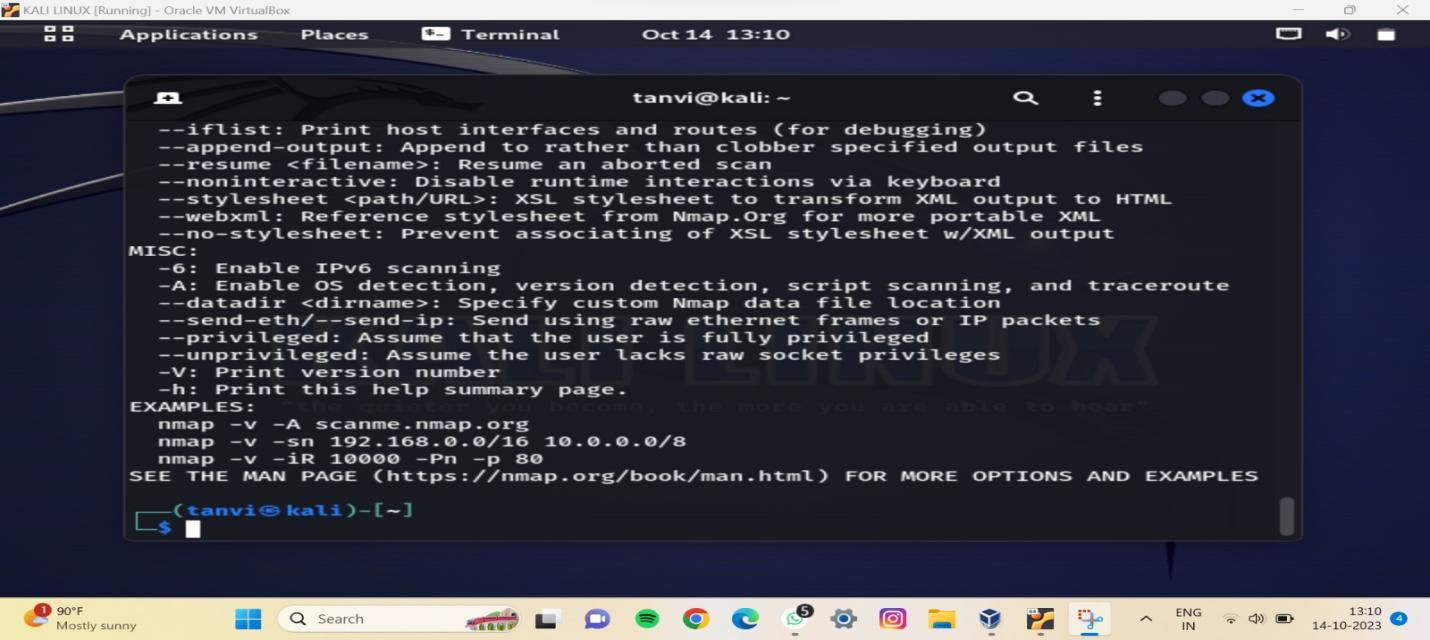
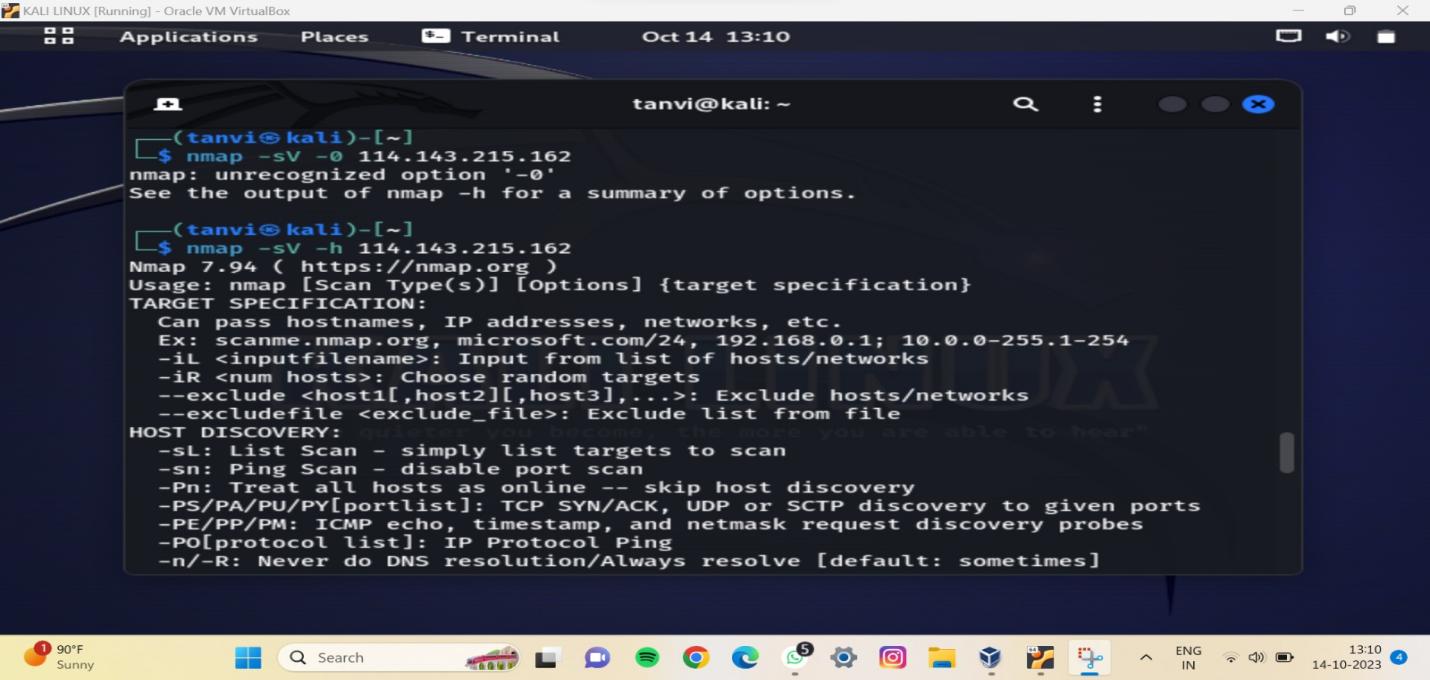
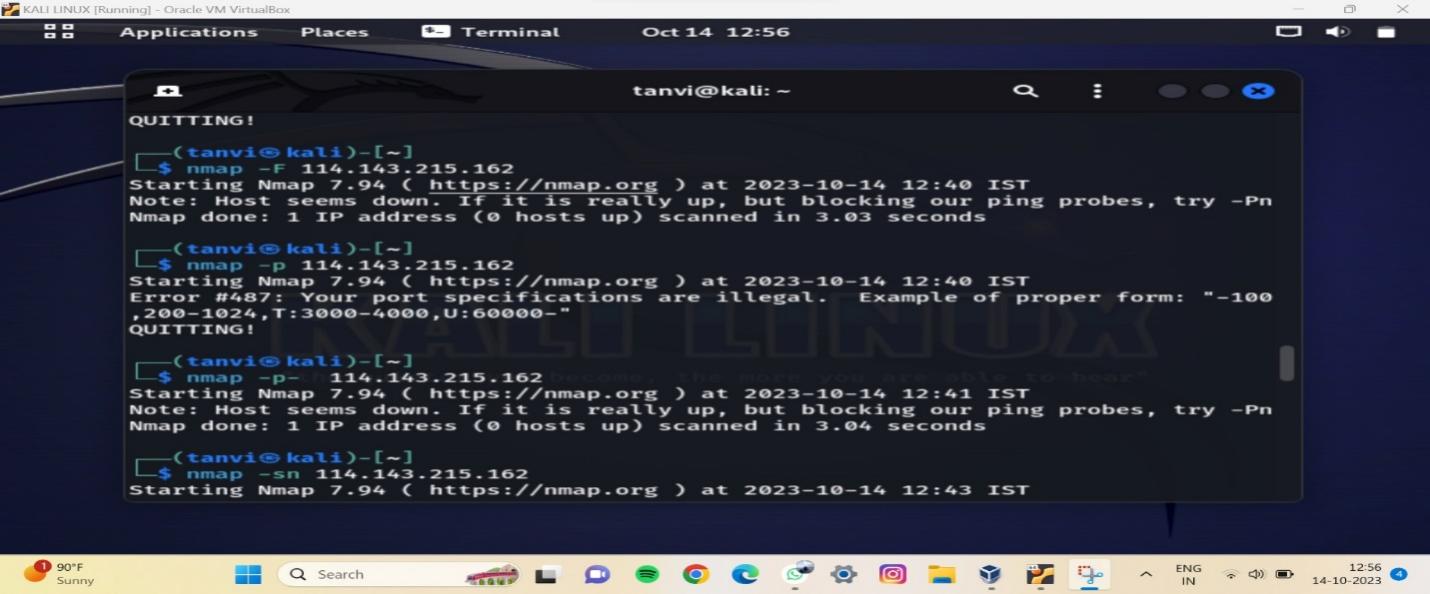
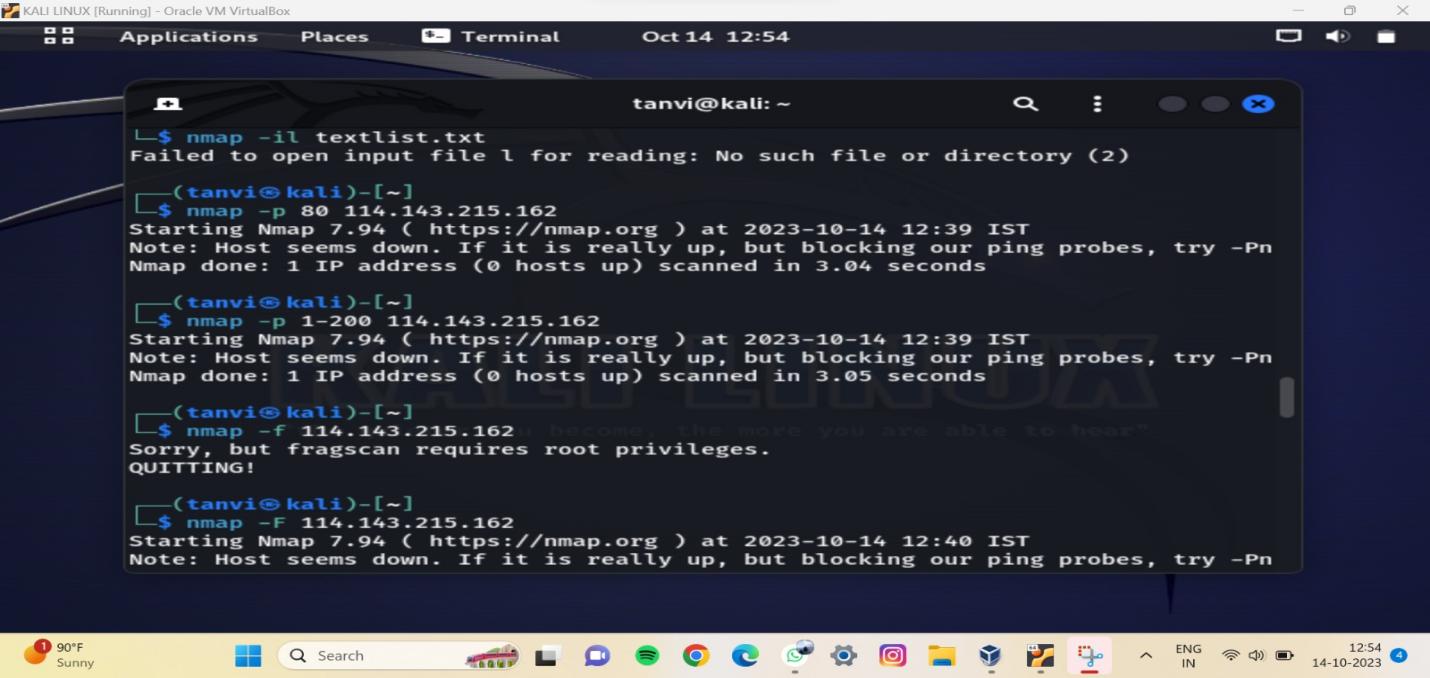
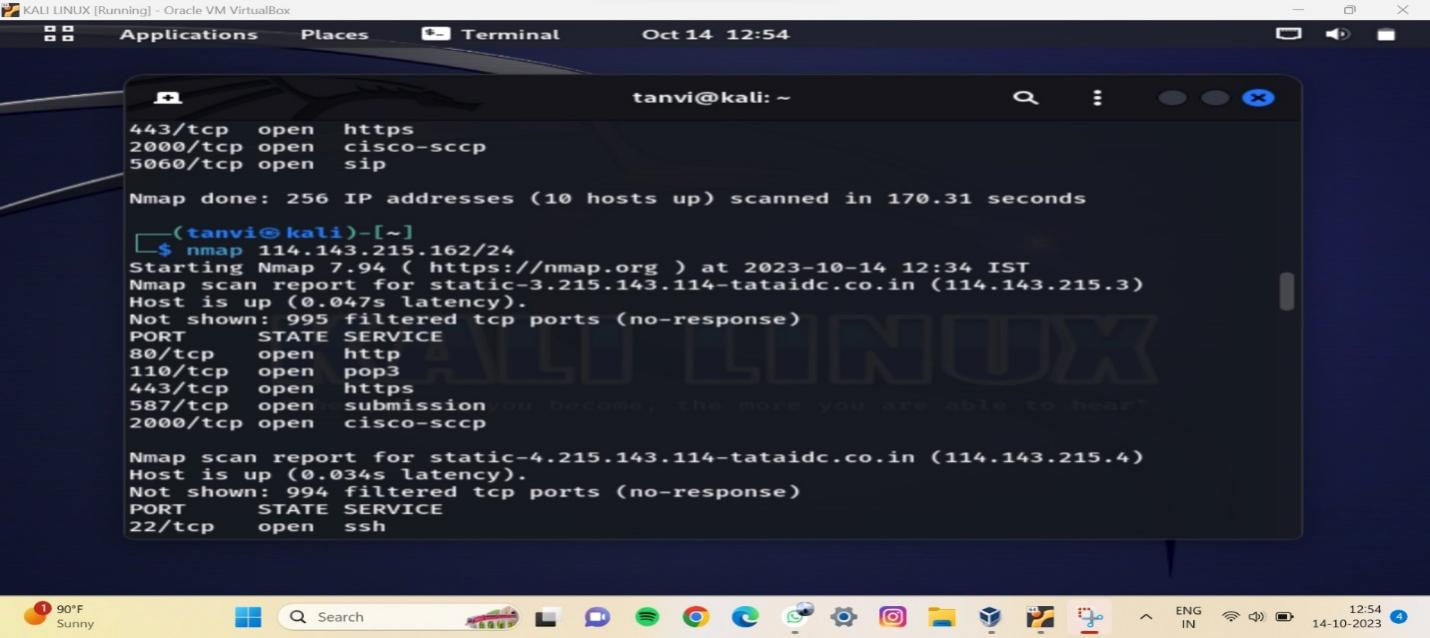
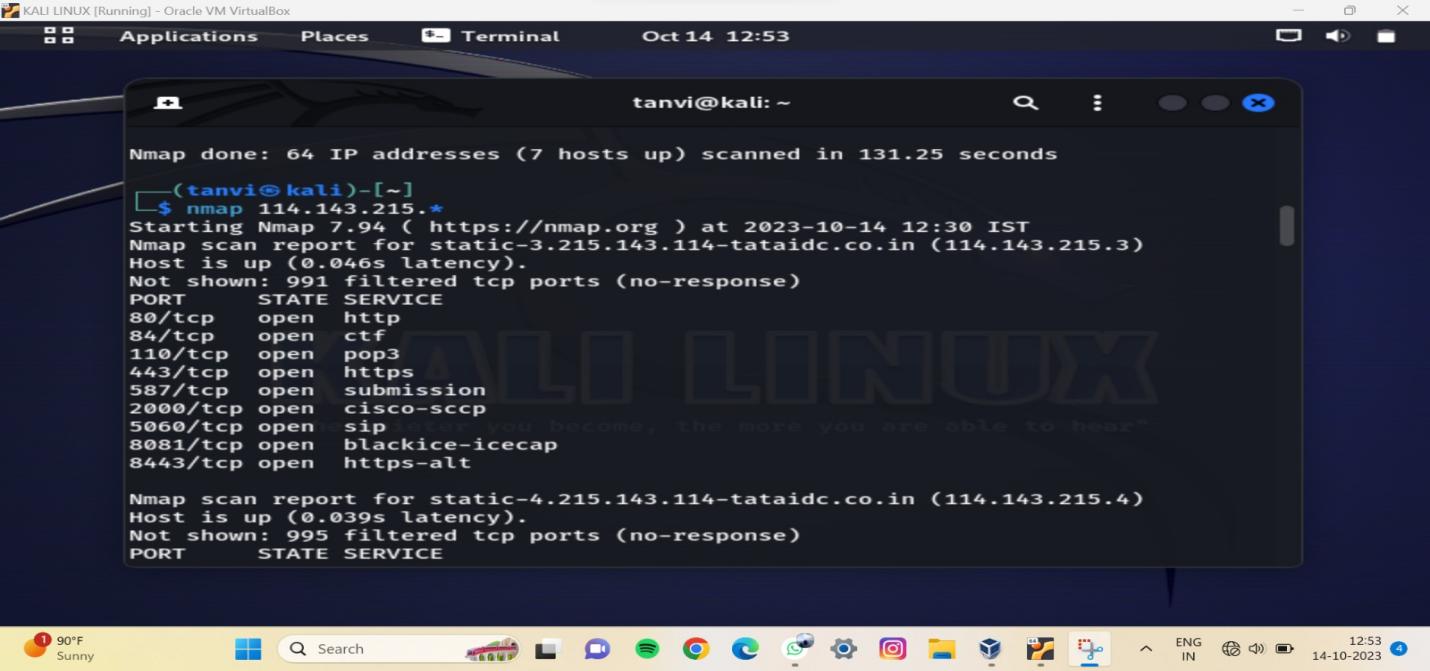
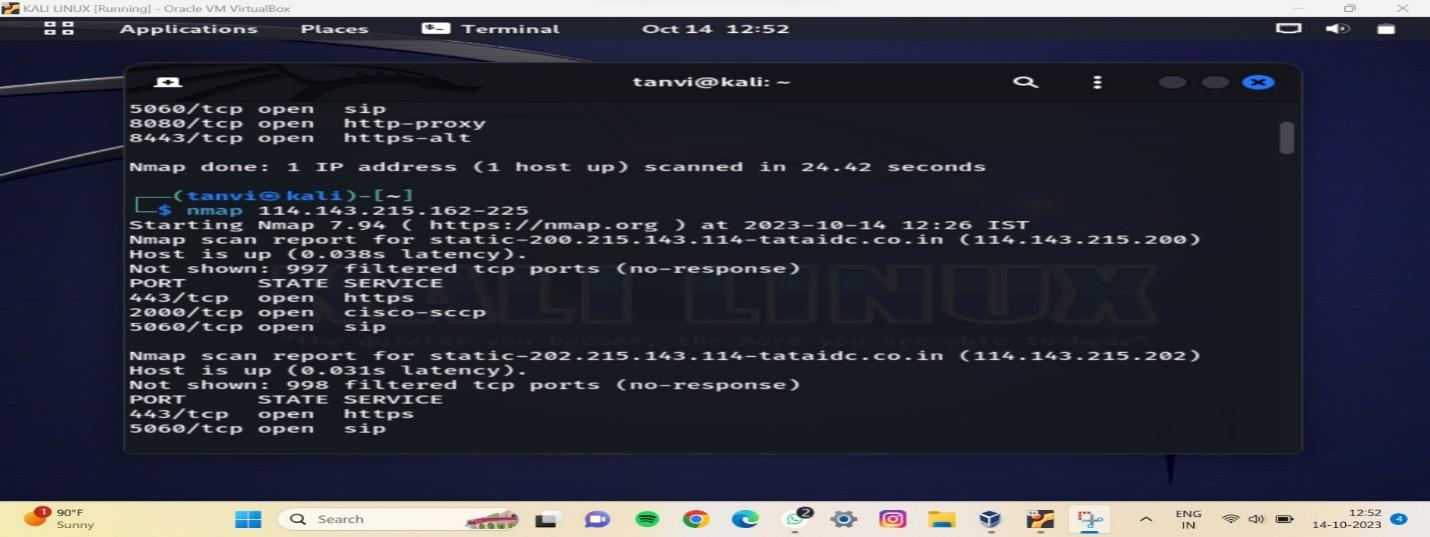
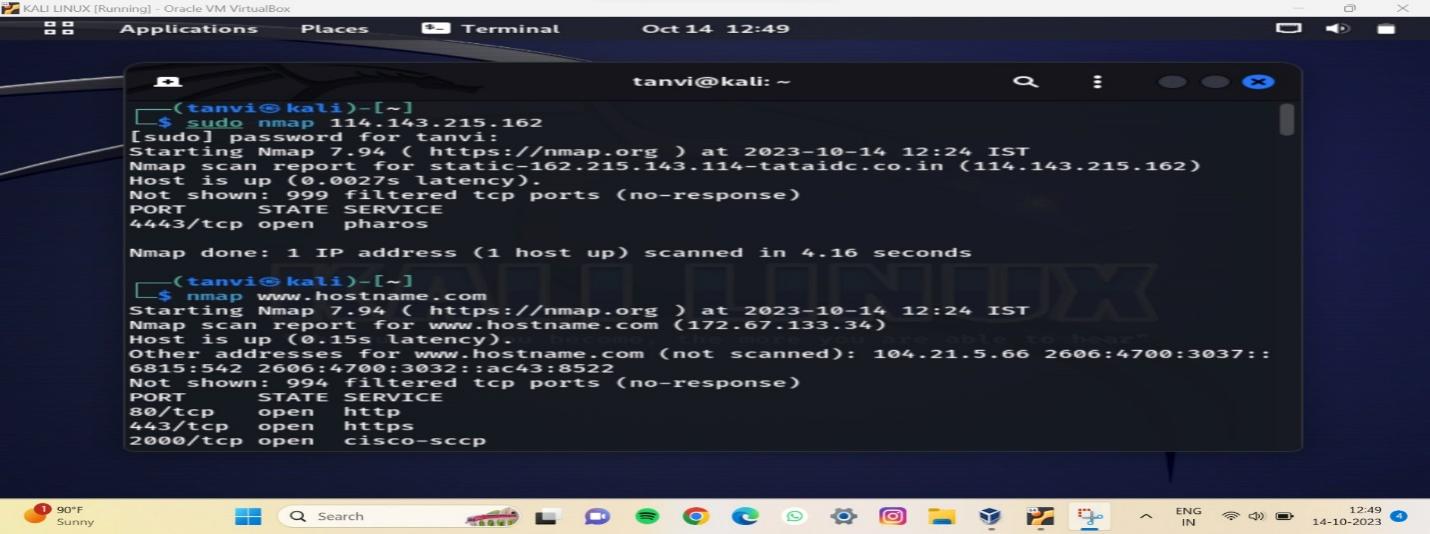
nmap –Pn –F 192.168.0.1

The **nmap** utility can be used to detect the operating system of a particular target:

nmap –A 192.168.0.1

It can also be used to probe for the services that might be using different ports:

nmap –sV 192.168.0.1

**Output:** 

**Komal Pal**

**2203021**

**LY-ISA1**