Don Bosco Institute of Technology, Mumbai 400070
Department of Information Technology

Experiment No.: 8

Date: 10/10/2022

Title: Nmap

Problem Definition: Download and install nmap. Use it with different options to scan active nodes, open ports, perform os finger printing, do a ping scan, tcp port scan, udp port scan. **Pre-requisite :** Networking commands

Theory:

Nmap - Network Mapper

Nmap is a security scanner originally written by Gordon Lyon (also known by his pseudonym Fyodor Vaskovich) used to discover hosts and services on a computer network, thus creating a "map" of the network. To accomplish its goal, Nmap sends specially crafted packets to the target host and then analyzes the responses.

The software provides a number of features for probing computer networks, including host discovery and service and operating system detection. These features are extensible by scripts that provide more advanced service detection, vulnerability detection, and other features. Nmap is also capable of adapting to network conditions including latency and congestion during a scan. Nmap is under development and refinement by its user community.

Nmap was originally a Linux-only utility, but it was ported to Microsoft Windows, Solaris, HP-UX, BSD variants (including Mac OS X), AmigaOS, and SGI IRIX. Linux is the most popular platform, followed closely by Windows.

Nmap features include:

- Host discovery – Identifying hosts on a network. For example, listing the hosts that respond to TCP and/or ICMP requests or have a particular port open.
- Port scanning – Enumerating the open ports on target hosts.
- Version detection – Interrogating network services on remote devices to determine application name and version number.
- OS detection – Determining the operating system and hardware characteristics of network devices.
- Scriptable interaction with the target – using Nmap Scripting Engine (NSE) and Lua programming language.

Nmap can provide further information on targets, including reverse DNS names, device types, and MAC addresses.

Typical uses of Nmap:

7. Auditing the security of a device or firewall by identifying the network connections which can be made to, or through it.
8. Identifying open ports on a target host in preparation for auditing.
9. Network inventory, network mapping, maintenance and asset management.
10. Auditing the security of a network by identifying new servers.
11. Generating traffic to hosts on a network.
12. Find and exploit vulnerabilities in a network.

Procedure/ Algorithm:

Commands that run on zenmap/nmap

nmap -sn 10.0.5.*

Displays the active nodes.

nmap -sn 10.0.5.237

Displays the whether specific node is active.

nmap -T5 10.0.5.237

Displays the ports of specific node.

nmap -A 10.0.5.237

Displays the operating system of specific node(OS finger printing).

Commands that run on terminal

nmap -sP 10.0.5.237

Used for ping scanning of specific node.

nmap -p T:80 10.0.5.237

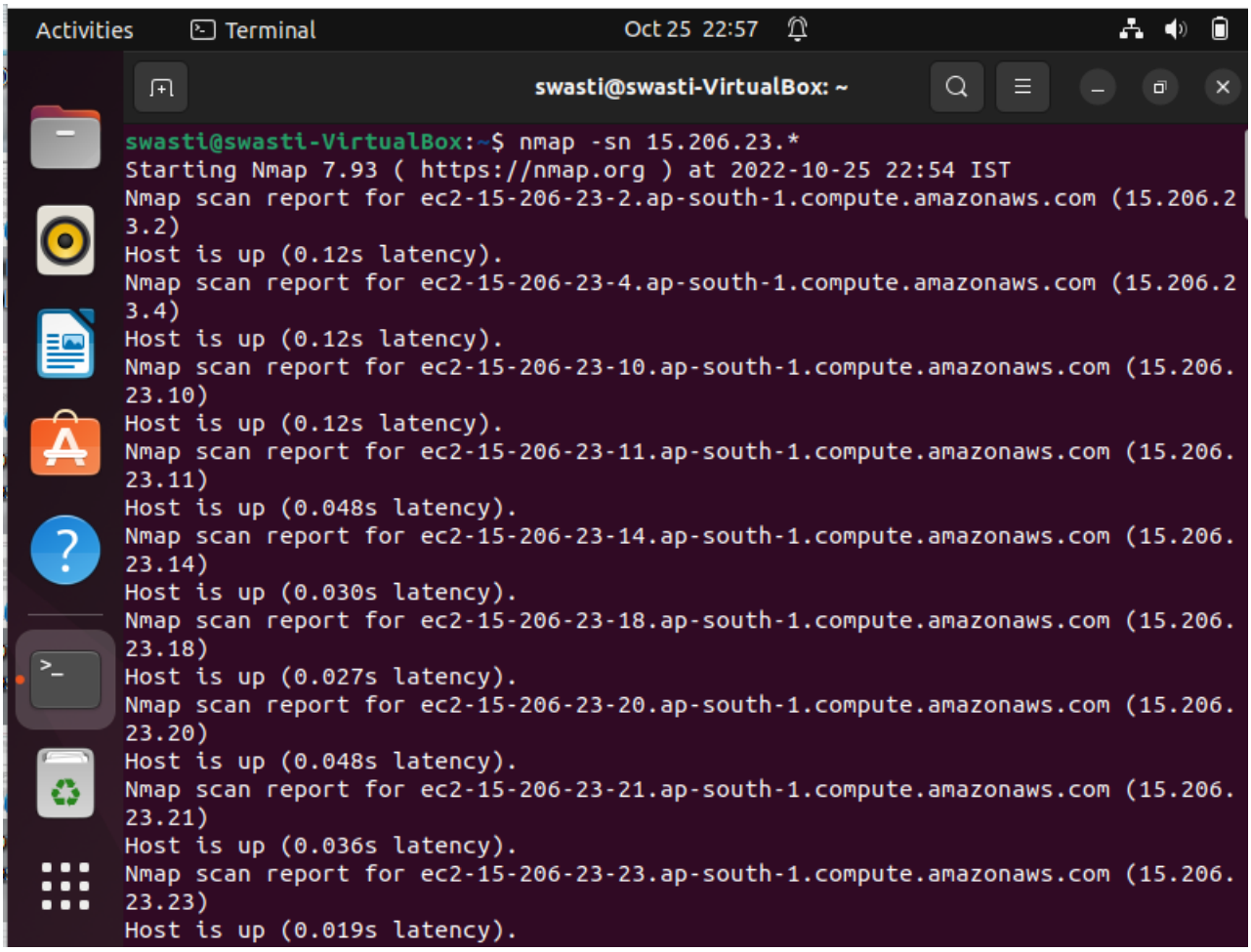
Used for tcp scanning of specific node.

nmap -p U:53 10.0.5.237

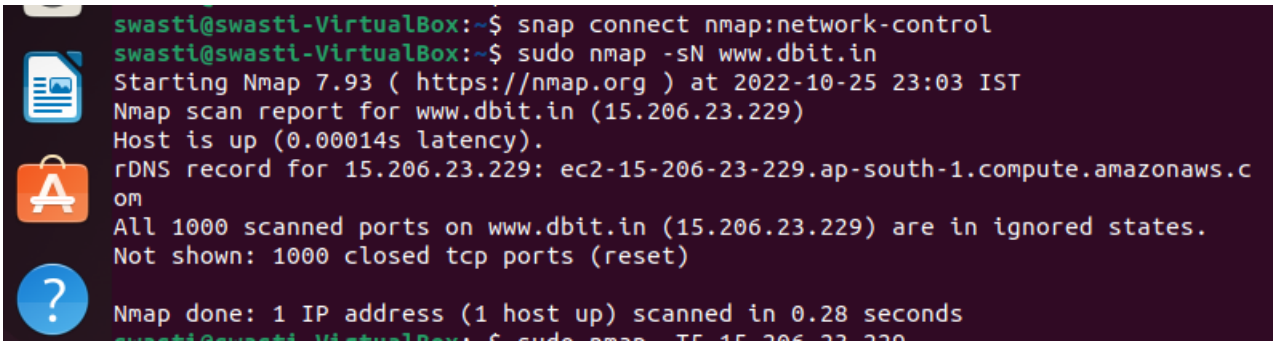
Used for udp scanning of specific node.

Results :

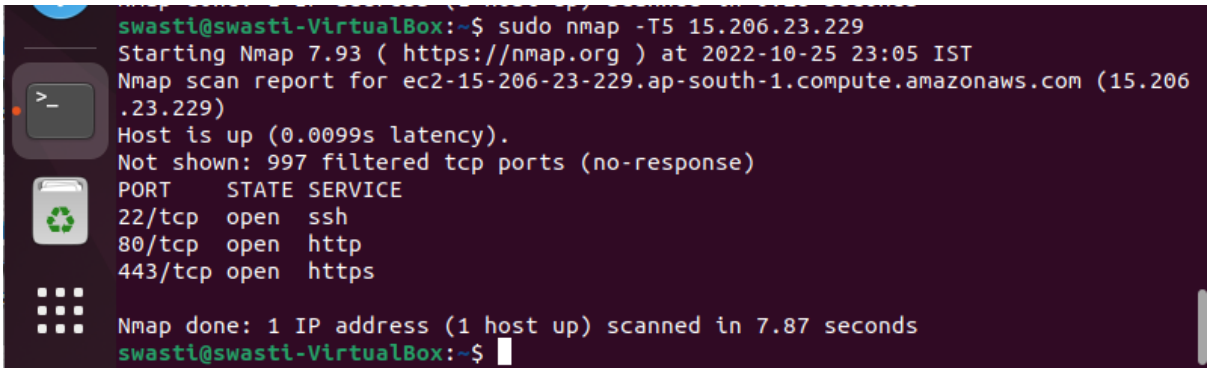
Shows the active nodes:

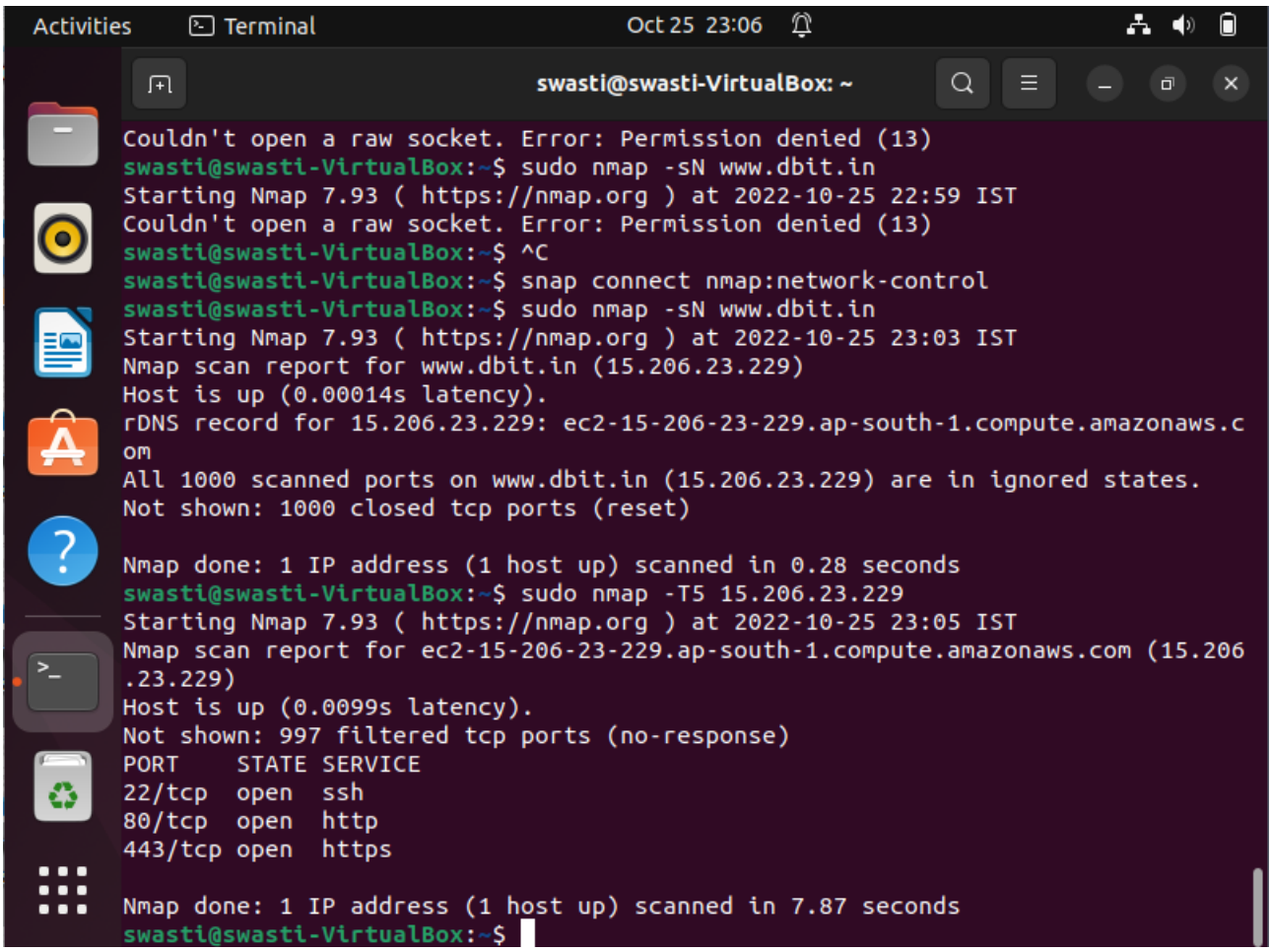


Shows specific port is active :

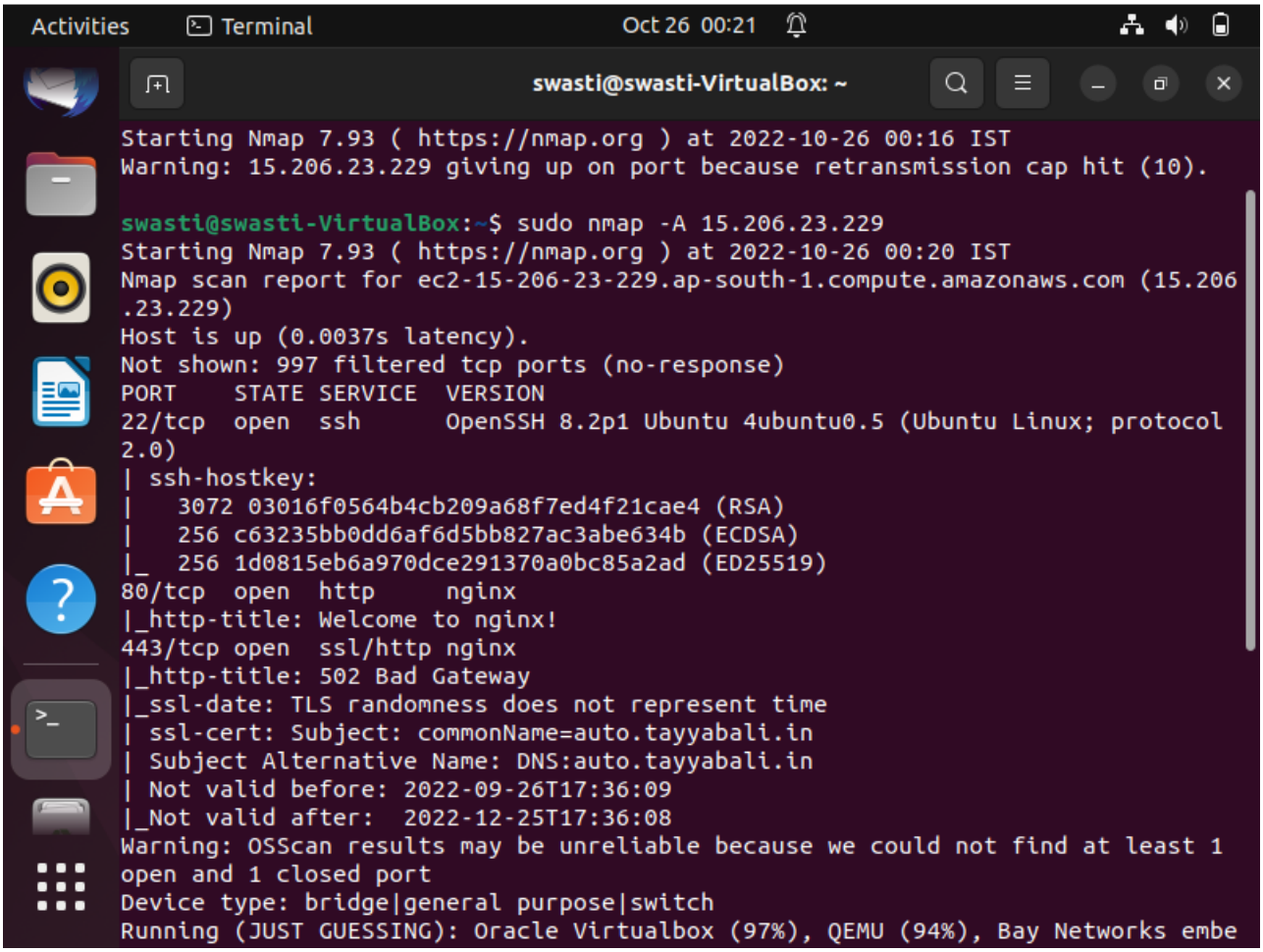


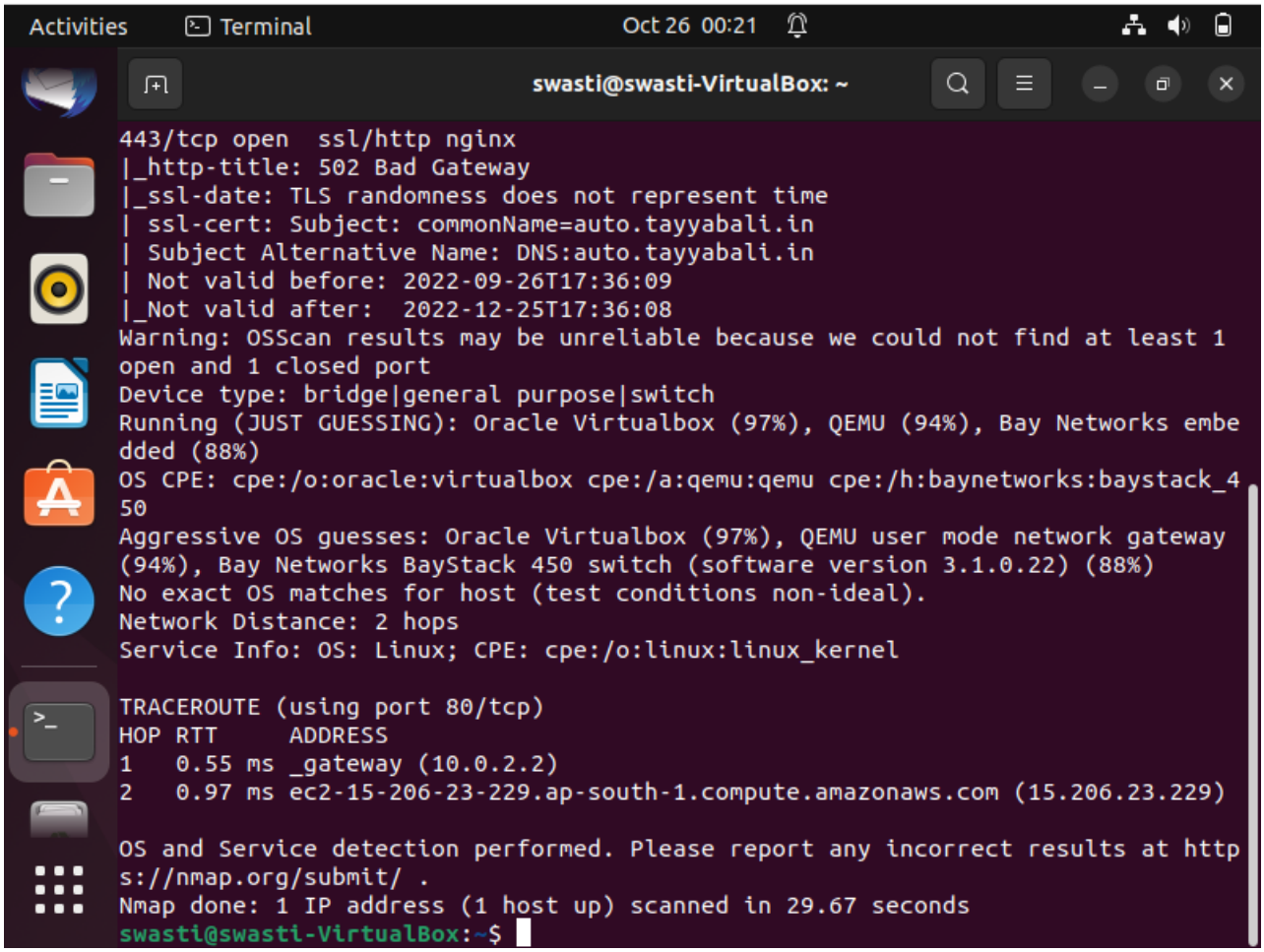
Display the port of specific node :


swasti@swasti-VirtualBox:~$ sudo nmap -T5 15.206.23.229
Starting Nmap 7.93 (https://nmap.org) at 2022-10-25 23:05 IST
Nmap scan report for ec2-15-206-23-229.ap-south-1.compute.amazonaws.com (15.206.23.229)
Host is up (0.0099s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
443/tcp open https
Nmap done: 1 IP address (1 host up) scanned in 7.87 seconds
swasti@swasti-VirtualBox:~$

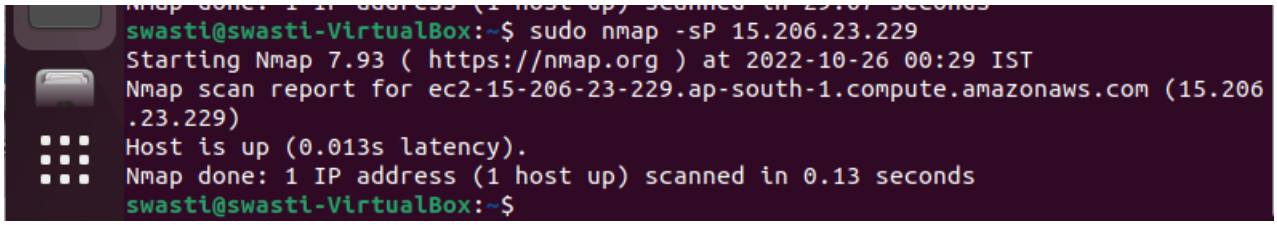

Activities
Terminal
Oct 25 23:06
swasti@swasti-VirtualBox: ~
Couldn't open a raw socket. Error: Permission denied (13)
swasti@swasti-VirtualBox:~$ sudo nmap -sN www.dbit.in
Starting Nmap 7.93 (https://nmap.org) at 2022-10-25 22:59 IST
Couldn't open a raw socket. Error: Permission denied (13)
swasti@swasti-VirtualBox:~$ ^C
swasti@swasti-VirtualBox:~$ snap connect nmap:network-control
swasti@swasti-VirtualBox:~$ sudo nmap -sN www.dbit.in
Starting Nmap 7.93 (https://nmap.org) at 2022-10-25 23:03 IST
Nmap scan report for www.dbit.in (15.206.23.229)
Host is up (0.00014s latency).
rDNS record for 15.206.23.229: ec2-15-206-23-229.ap-south-1.compute.amazonaws.com
All 1000 scanned ports on www.dbit.in (15.206.23.229) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
swasti@swasti-VirtualBox:~$ sudo nmap -T5 15.206.23.229
Starting Nmap 7.93 (https://nmap.org) at 2022-10-25 23:05 IST
Nmap scan report for ec2-15-206-23-229.ap-south-1.compute.amazonaws.com (15.206.23.229)
Host is up (0.0099s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
443/tcp open https
Nmap done: 1 IP address (1 host up) scanned in 7.87 seconds
swasti@swasti-VirtualBox:~$

Displays the operating system of specific node(OS finger printing):

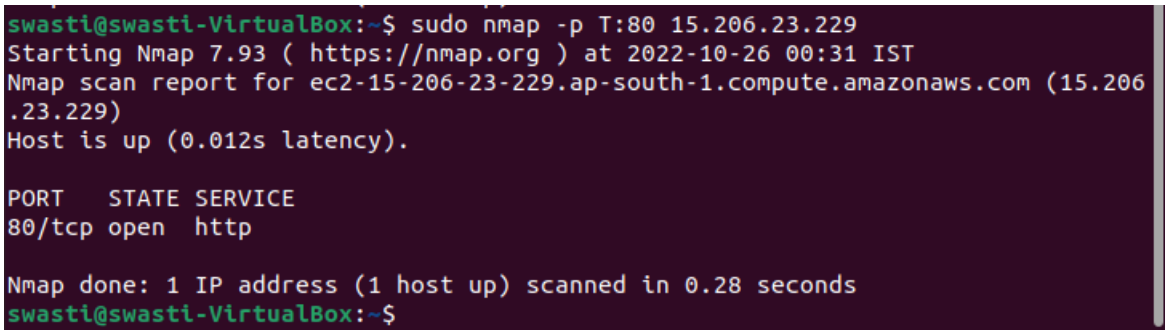




Ping scanning:



Tcp scanning:



Udp scanning:

```
UDP Scan Timing: About 6.00% done; ETC: 16:28 (0:00:31 remaining)
Stats: 0:00:03 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 9.50% done; ETC: 16:28 (0:00:29 remaining)
Nmap scan report for a23-213-57-109.deploy.static.akamaitechnologies.com (23.213.57.109)
Host is up (0.0047s latency).
All 1000 scanned ports on a23-213-57-109.deploy.static.akamaitechnologies.com (23.213.57.109) are open|filtered
```

References :

1.http://www.cyberciti.biz/networking/nmap-command-examples-tutorials/

2.http://en.wikipedia.org/wiki/Nmap