PRACTICAL: 4

AIM:

Port scanning is a method for determining open ports and services available on a network or a host. It involves connecting with TCP and UDP ports on system, once you found the IP addresses of a target network or host by Footprinting technique. You have to map the network of this targeted organization. Nmap (Network Mapper) is a powerful, flexible, open source and easy to use tool for port scanning available for both Linux and Windows based operating system. Study practical approach to implement scanning and enumeration techniques using Nmap.

THEORY:

Nmap ("Network Mapper") is an open source tool for network exploration and security auditing. It was designed to rapidly scan large networks, although it works fine against single hosts. 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. While Nmap is commonly used for security audits, many systems and network administrators find it useful for routine tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

Key among that information is the "interesting ports table". That table lists the port number and protocol, service name, and state. The state is either open, filtered, closed, or unfiltered. Open means that an application on the target machine is listening for connections/packets on that port. Filtered means that a firewall, filter, or other network obstacle is blocking the port so that Nmap cannot tell whether it is open or closed. Closed ports have no application listening on them, though they could open up at any time. Ports are classified as unfiltered when they are responsive to Nmap's probes, but Nmap cannot determine whether they are open or closed. Nmap reports the state combinations open|filtered and closed|filtered when it cannot determine which of the two states describe a port. The port table may also include software version details when version detection has been requested. When an IP protocol scan is requested (-sO), Nmap provides information on supported IP protocols rather than listening ports.

CODE:

```
Find Nmap version
        nmap -v

Scan using Hostname
        nmap localhost

Scan using URL
        nmap amazon.com
```

Scan using IP Address
nmap 205.251.242.103

Scan using -v option
nmap -v amazon.com

Scan a Host to Detect Firewall
sudo nmap -sA amazon.com

Scan a Host to check its Protected by Firewall
sudo nmap -PN amazon.com

Perform a Fast scan
nmap -F amazon.com

Print Host interfaces and routes
nmap --iflist

Enable OS Detection with Nmap
sudo nmap -O amazon.com

OUTPUT:

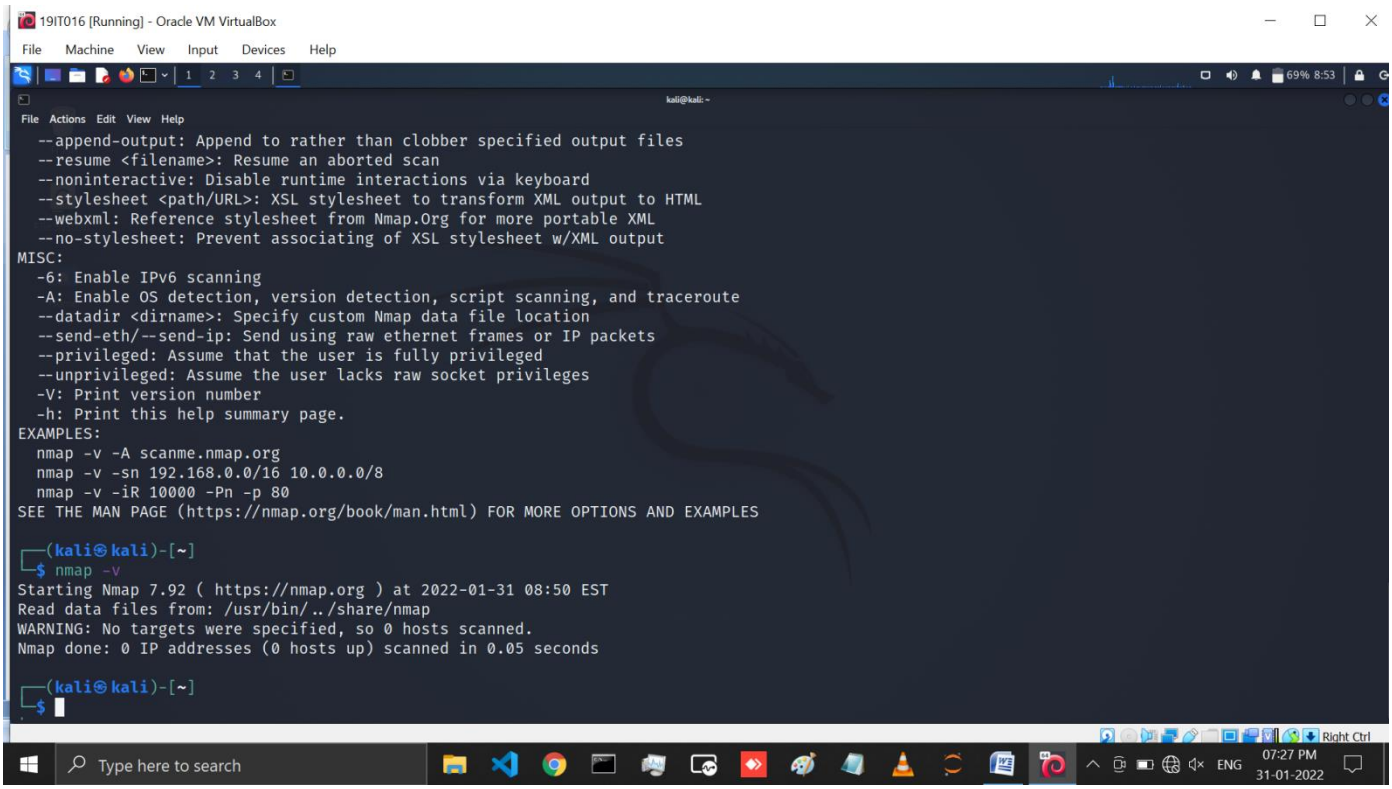


Figure 1: using nmap -v command we can see the version of nmap that we are using

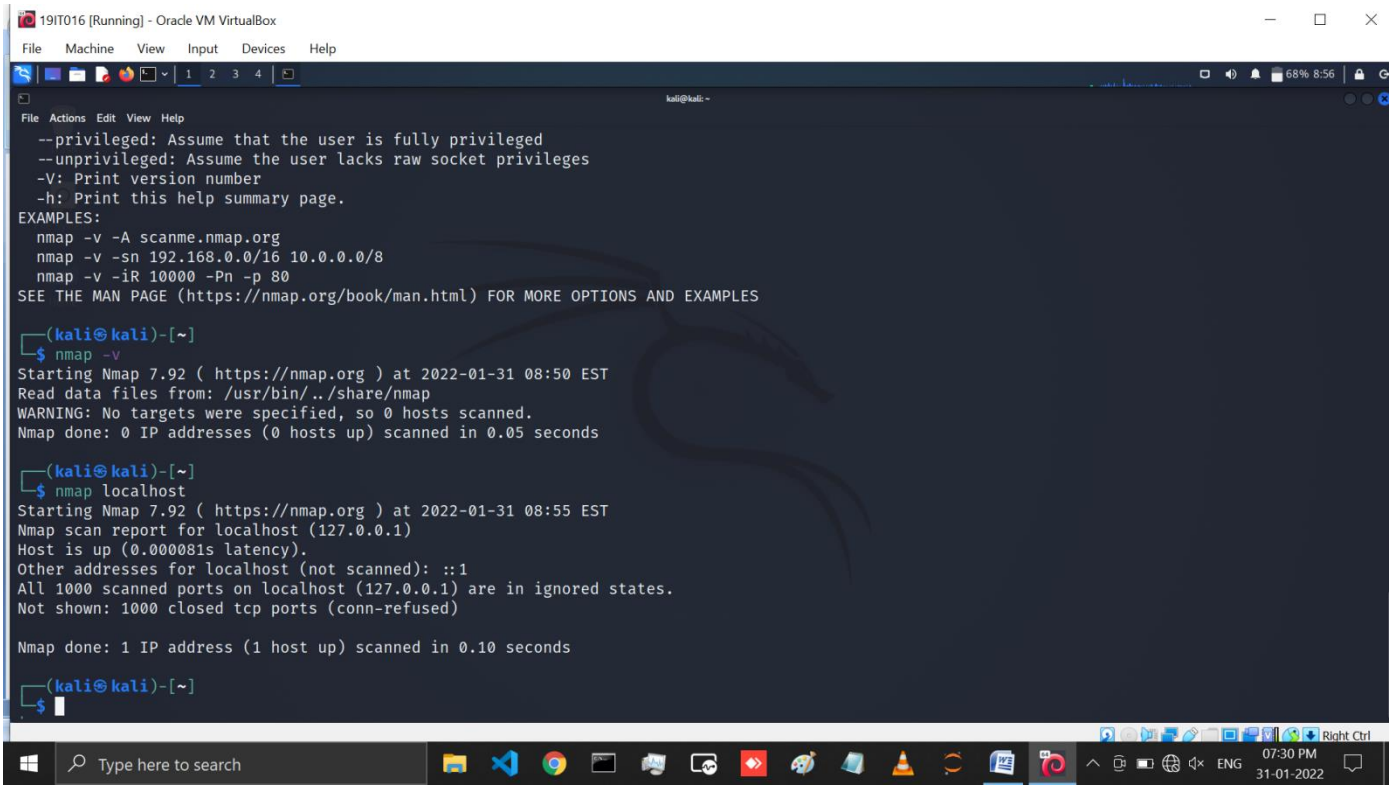


Figure 2: In this page you can see the scanning using nmap localhost command

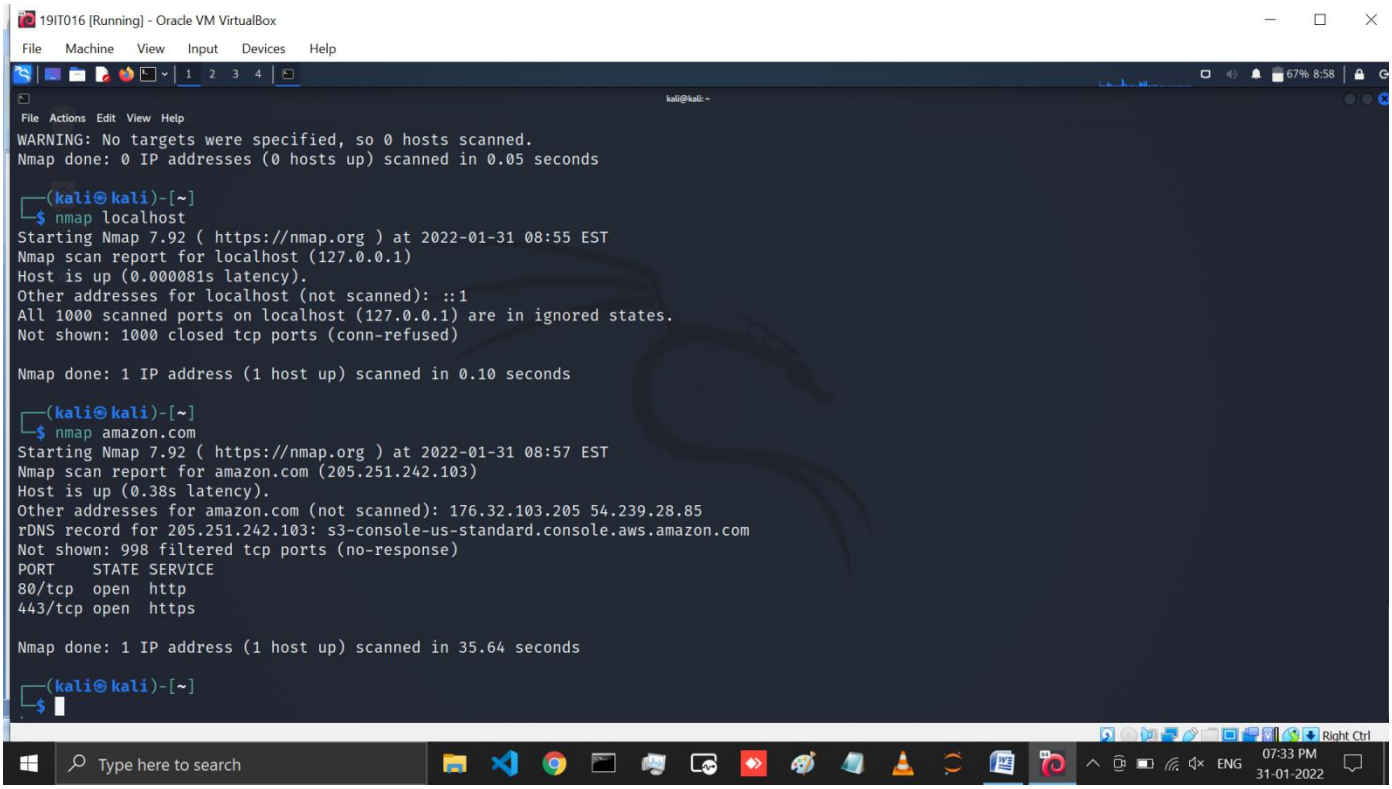


Figure 3: Here we performed scan using particular URL for this we use amazon.*com* website.here you can see the open ports, ip address and host details of that website

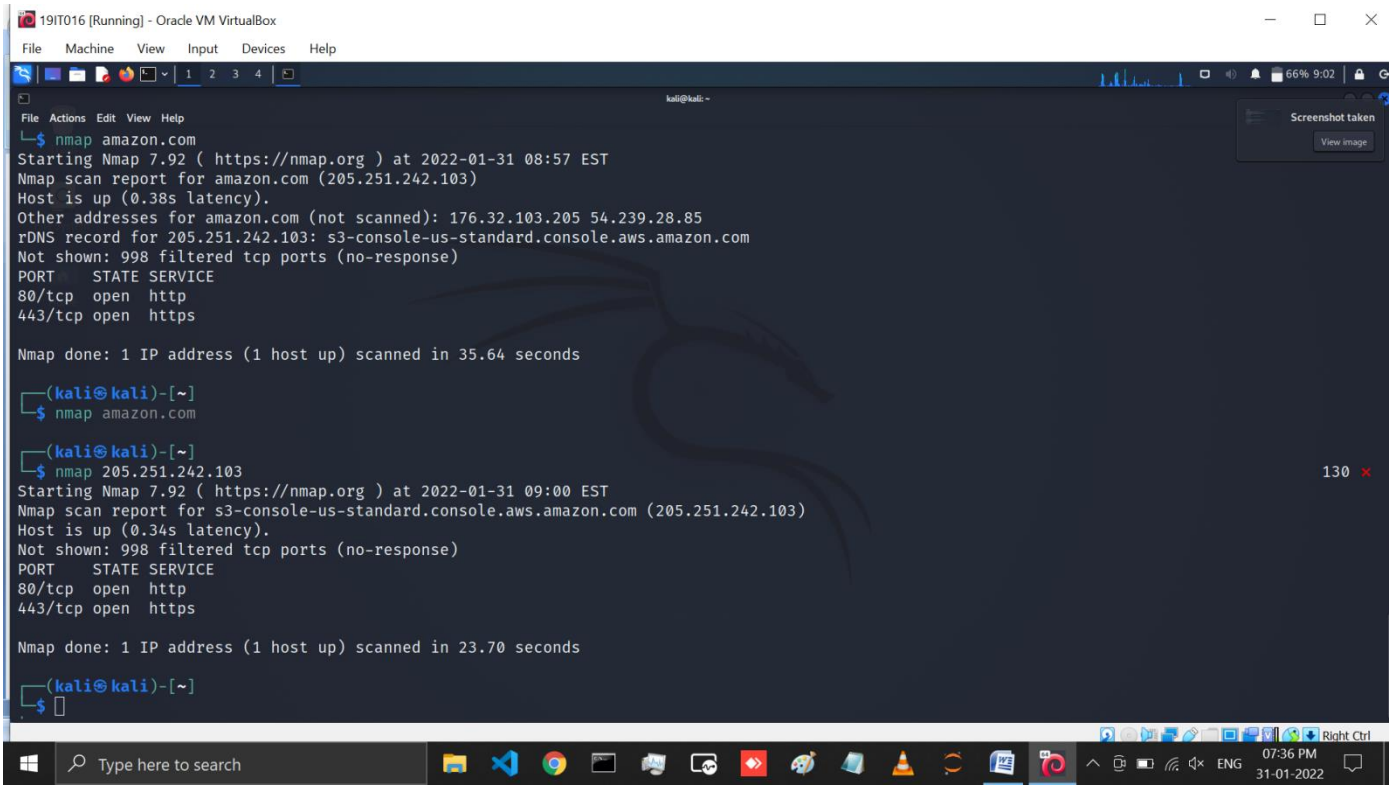


Figure 4 :: Here we performed scan using particular Ip address for this we use *amazon.com* Website. Here you can see the open ports and host details of that website

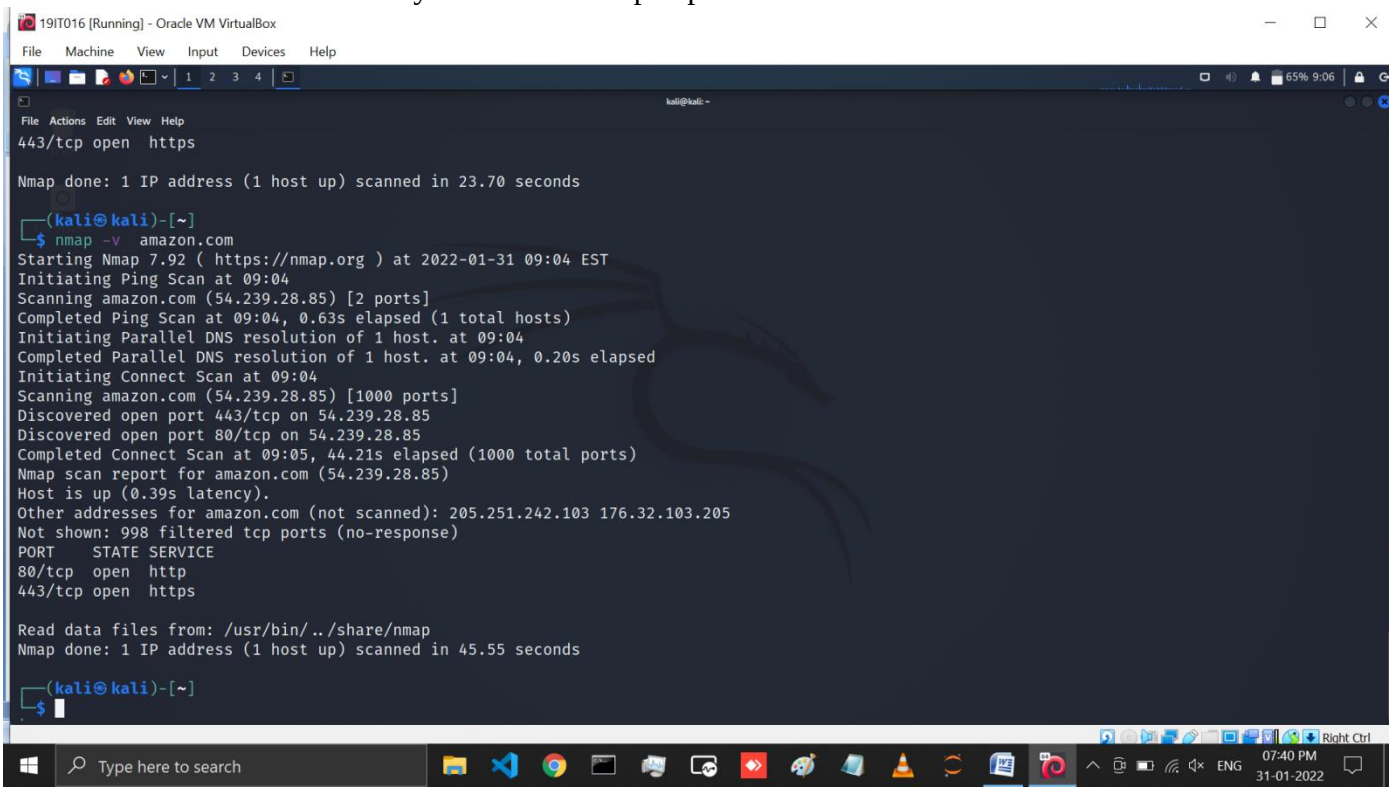


Figure 5: In this page we have performed scan using nmap -v command on *amazon.com*. Theverbose output provides additional information about the scan being performed. It is useful to monitorstep by step actions Nmap performs on a network, especially if you are an outsider scanning a client's network.

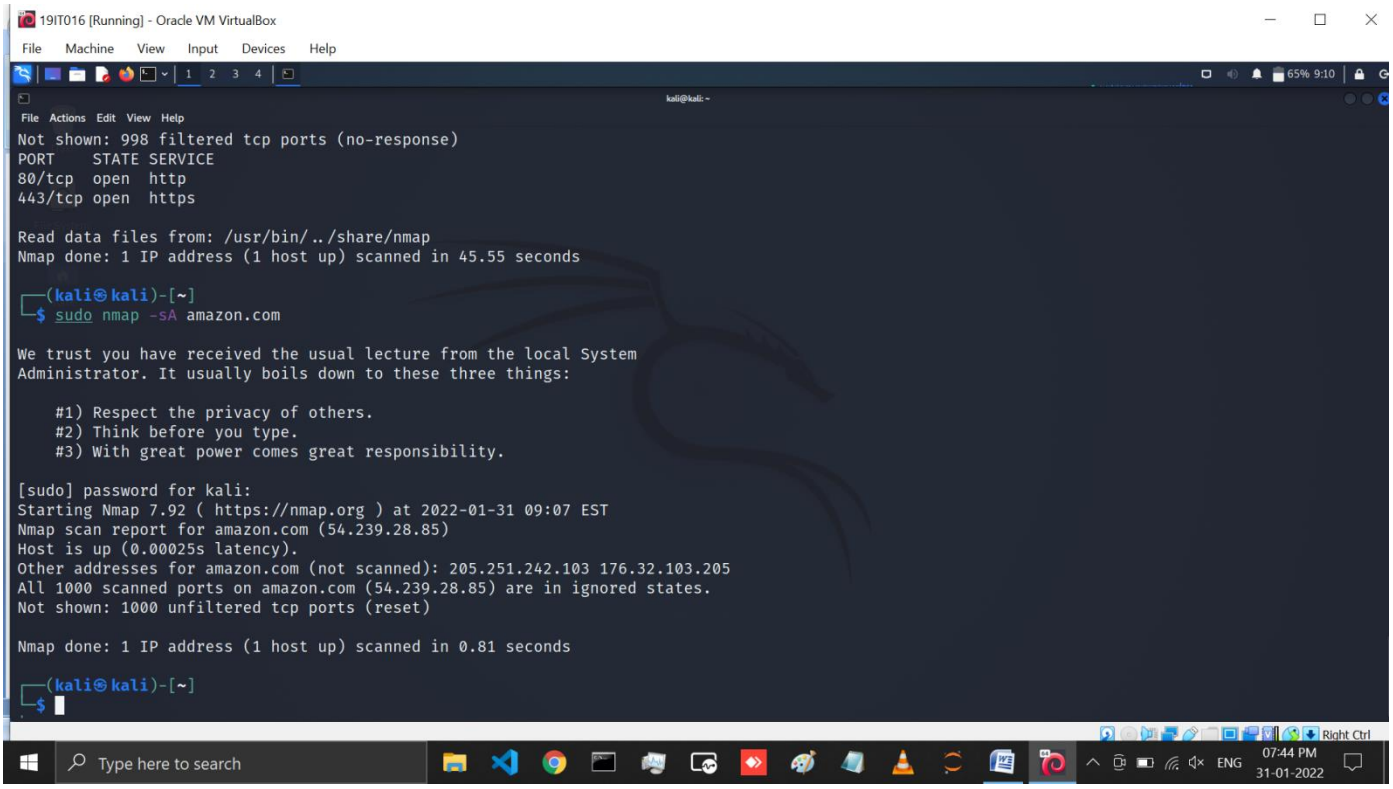


Figure 6: nmap -sA command is use for Scan a host to detect firewall

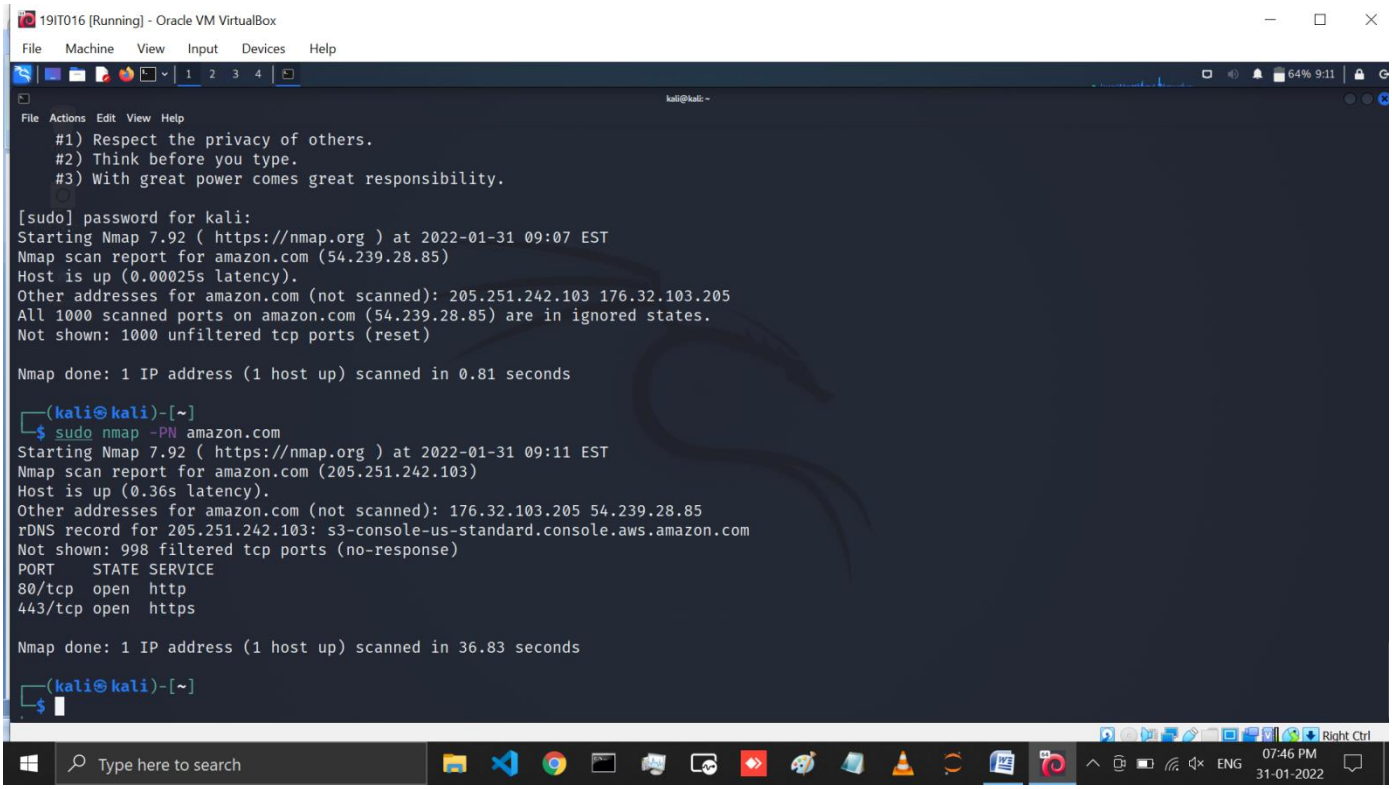


Figure 7: If we want to check our host is protected by firewall or not for that we have to use nmap -PN command

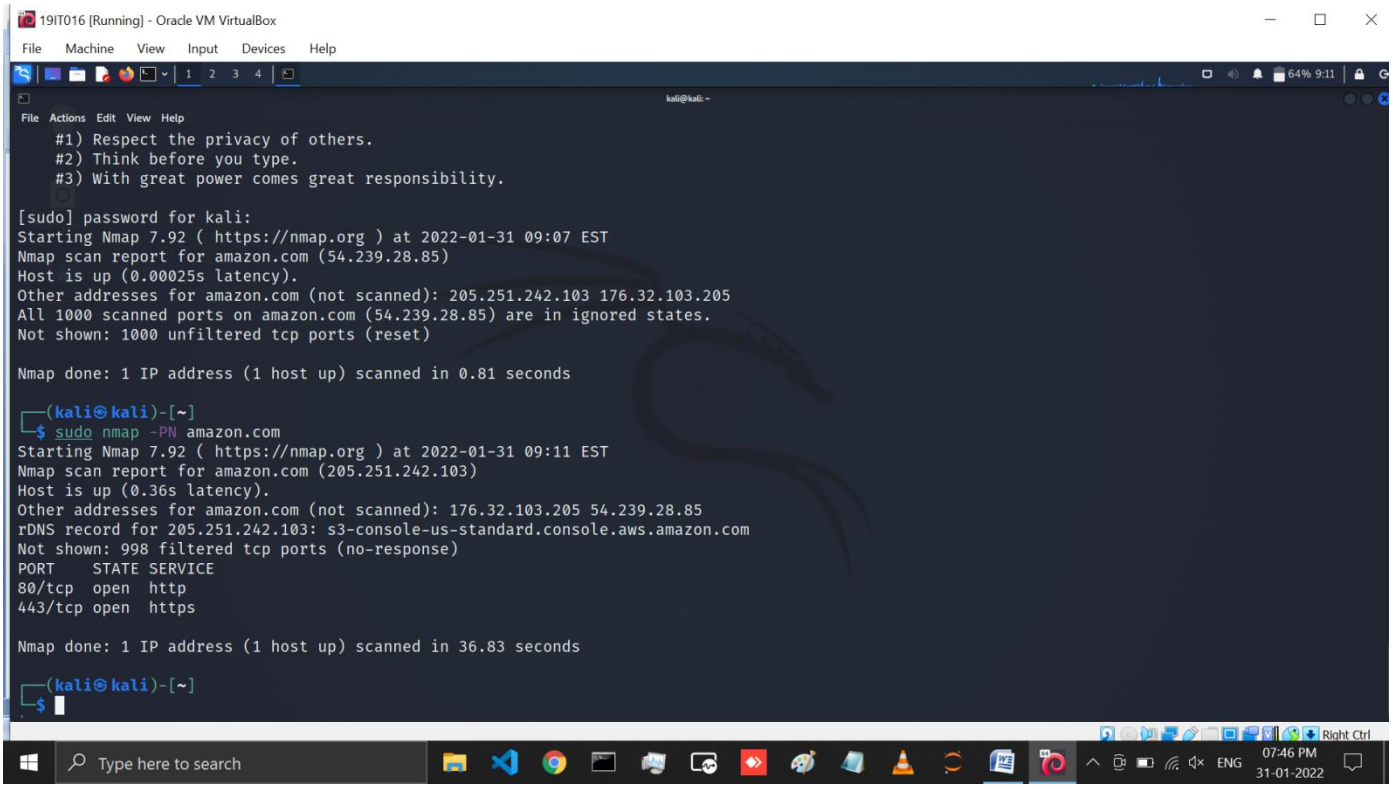


Figure 8: In this page you can see the nmap -F command which is use to perform fast scanning

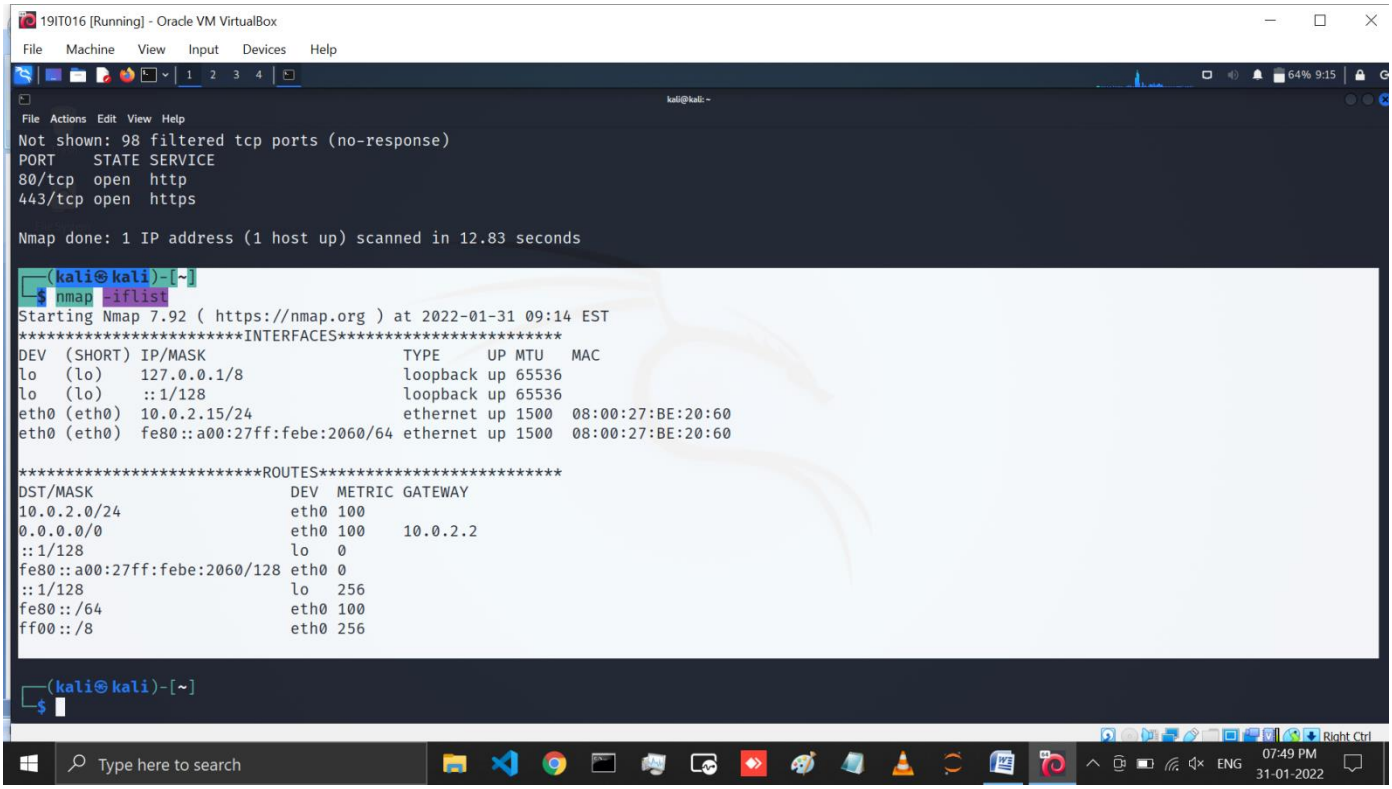


Figure 9: Here nmap --iflist command is use to print host interfaces and routes

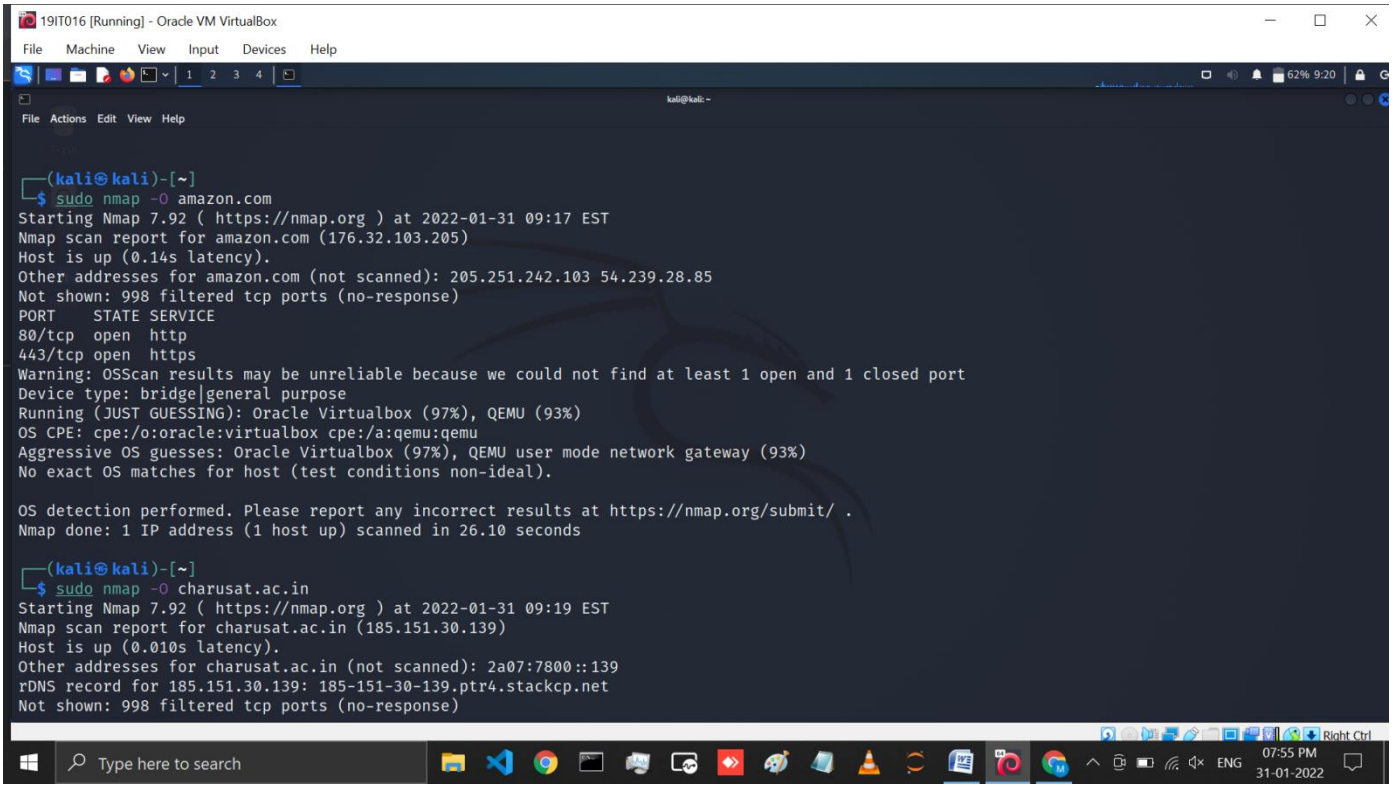
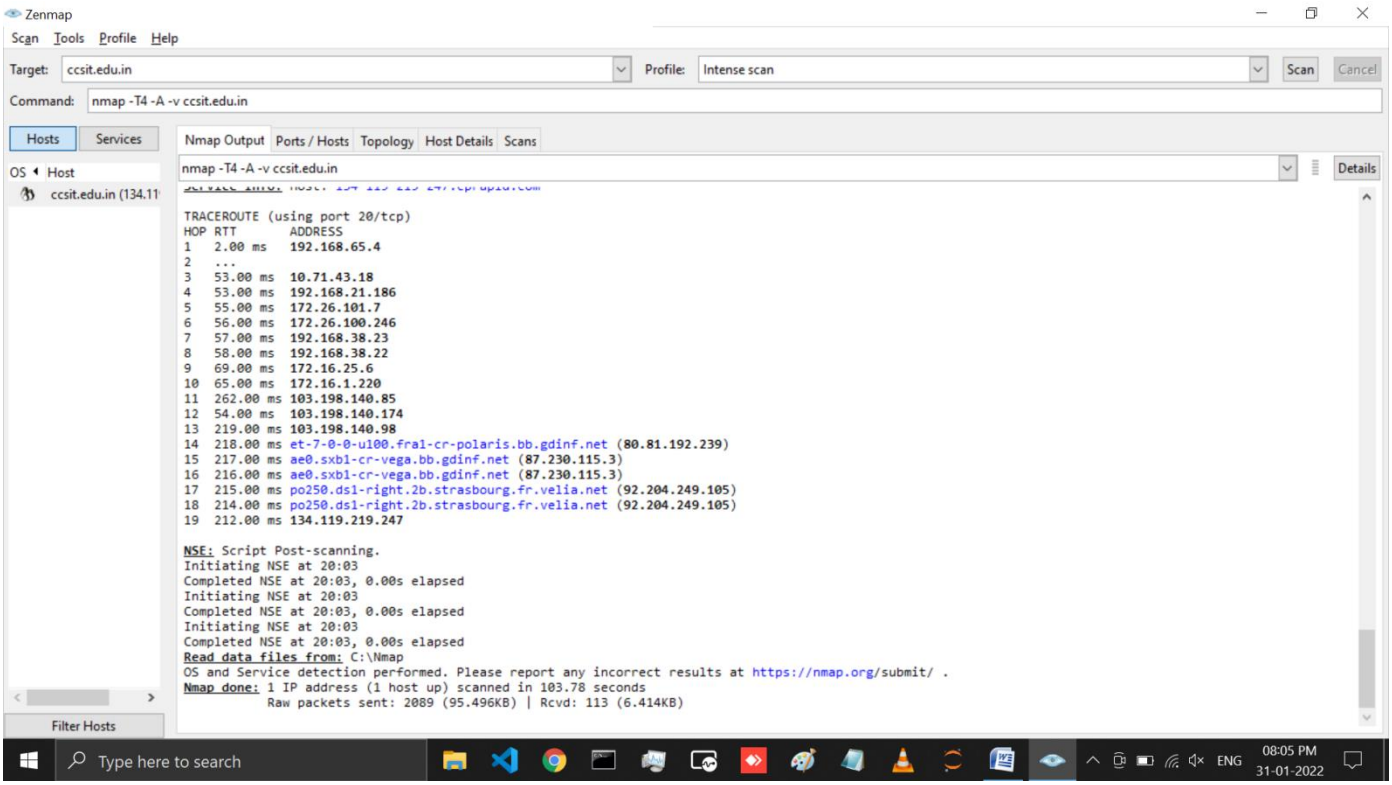


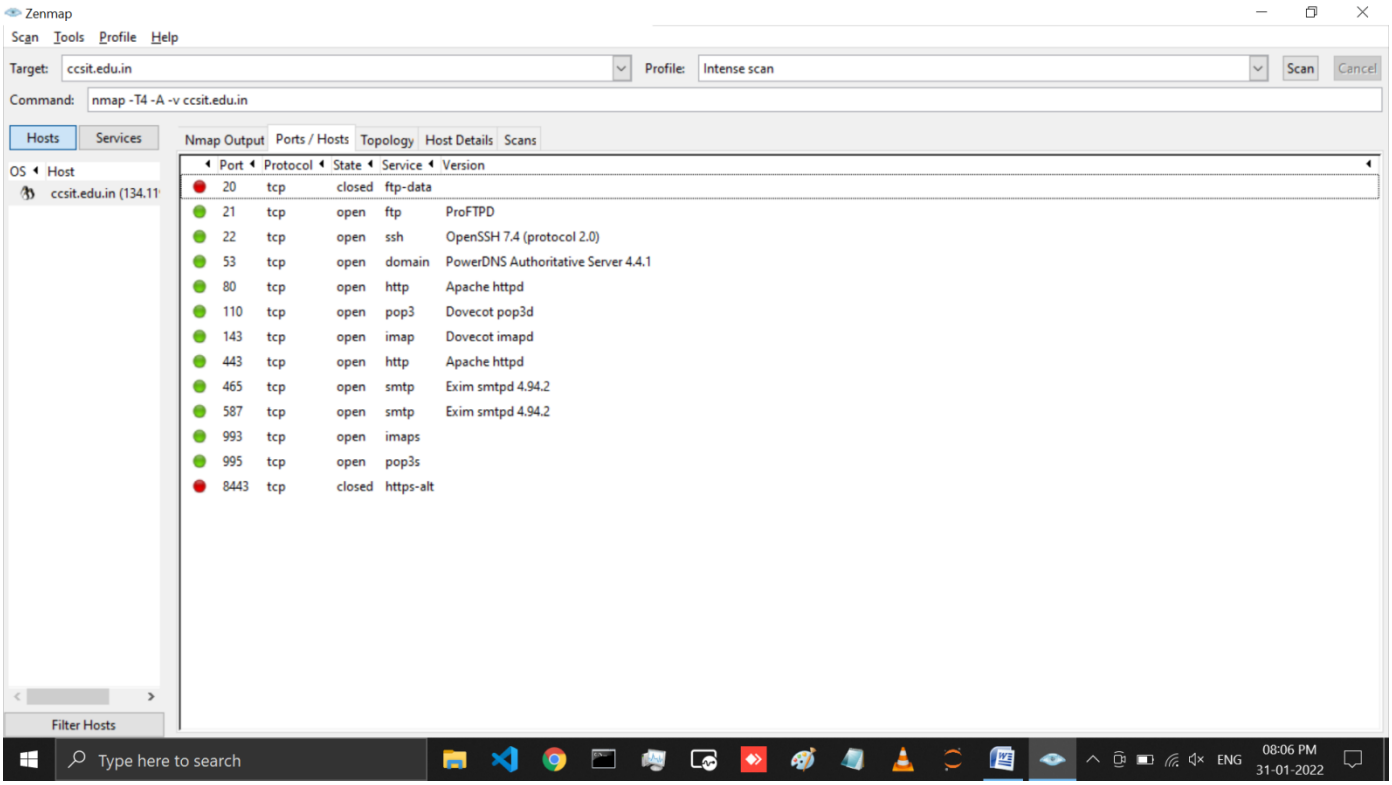
Figure 10: OS scanning is one of the most powerful features of Nmap. When using this type of scan, Nmap sends TCP and UDP packets to a particular port, and then analyze its response. It compares this response to a database of 2600 operating systems, and return information on the OS (and version) of a host. To run an OS scan, use the nmap -o command

<u>Obtaining all necessary information of target host using Zenmap.</u>

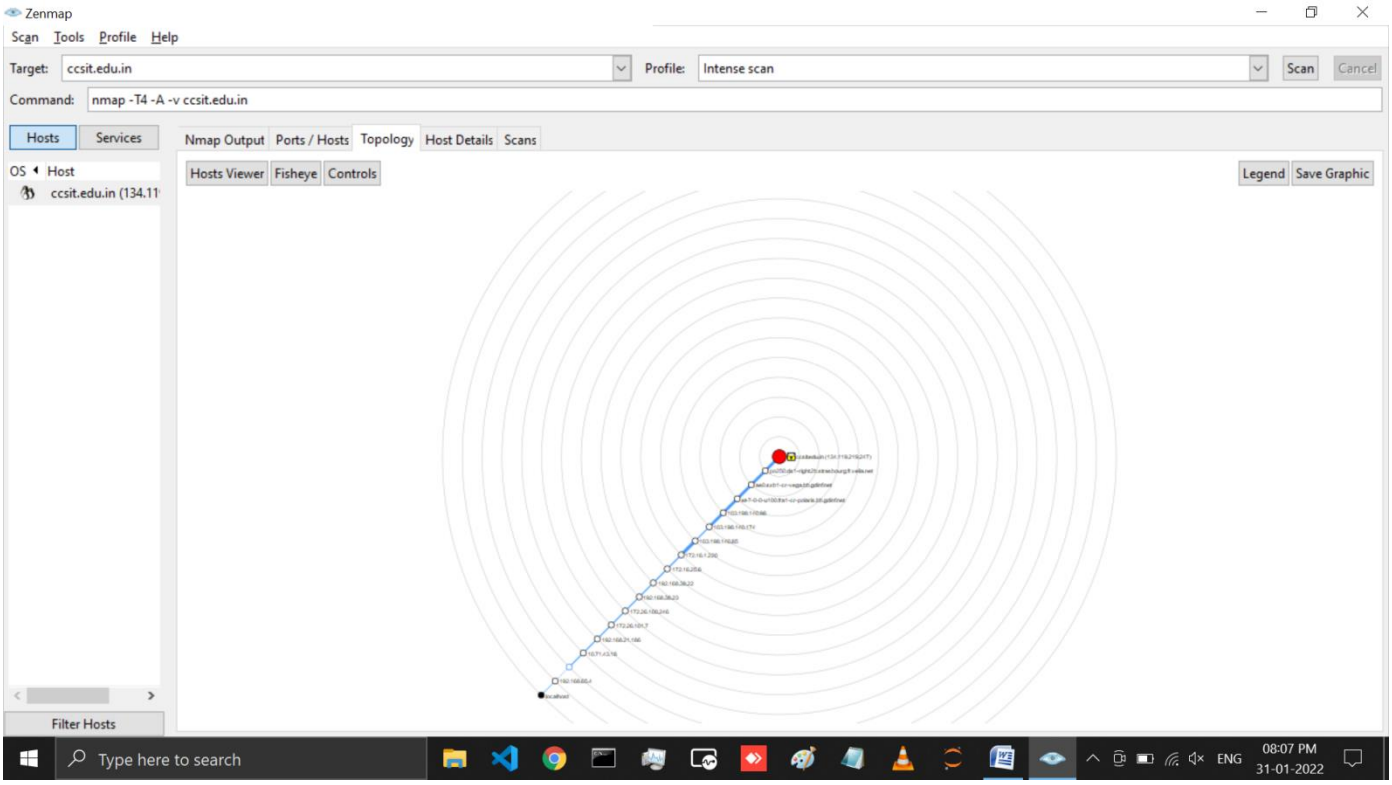
- Performing aggressive scans in target host



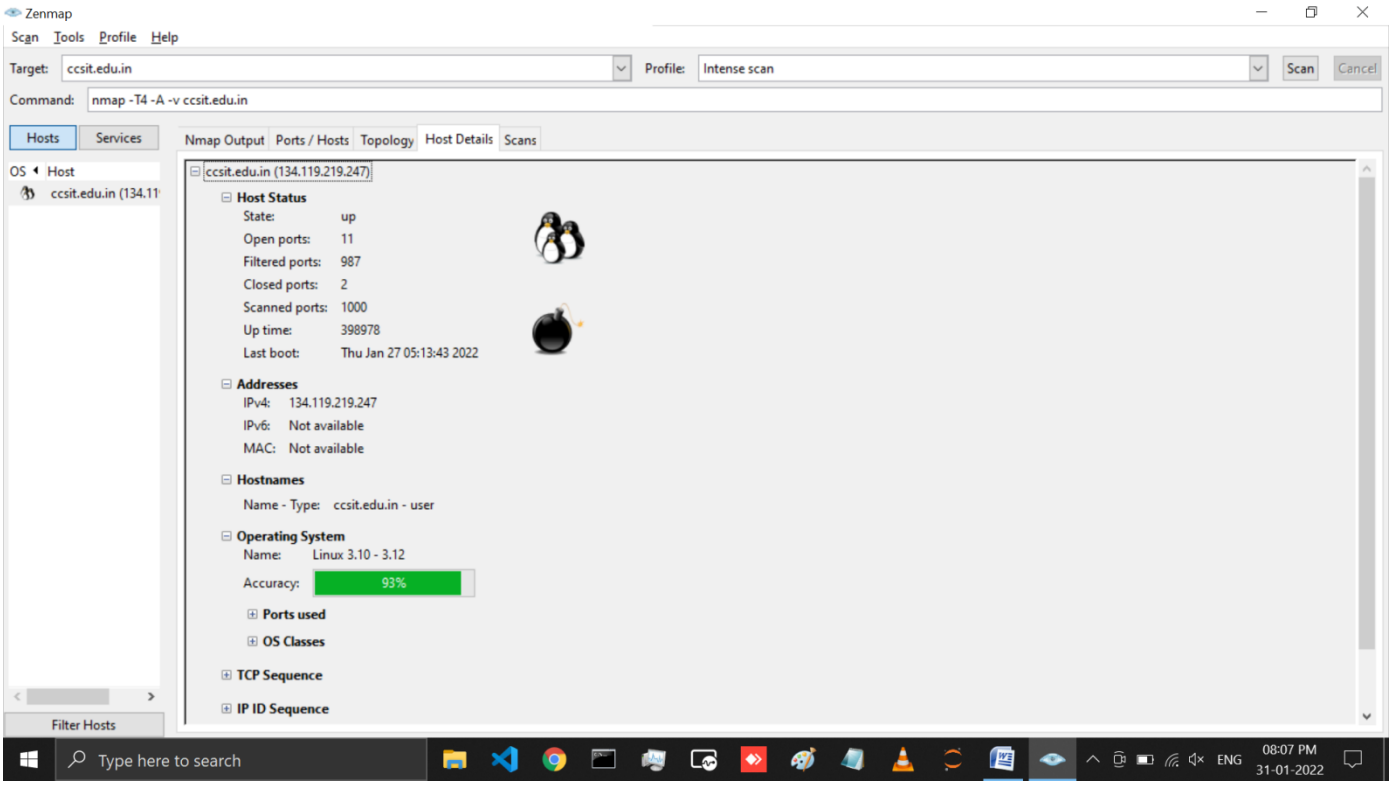
- In Ports/Hosts option we can see the open port of target host.



- In Topology option we can see the number of system IP required to reach target host.



- In Host Details option we can see the target host operating system.



LATEST APPLICATIONS:

- Auditing the security of a device or firewall by identifying the network connections which can be made to, or through it.
- Identifying open ports on a target host in preparation for auditing.
- Network inventory, network mapping, and maintenance and asset management.
- Auditing the security of a network by identifying new servers.
- Generating traffic to hosts on a network, response analysis and response time measurement.
- Finding and exploiting vulnerabilities in a network.
- DNS queries and subdomain search.

LEARNING OUTCOME:

In this Practical we have learned all about Nmap tool. And also learned how Nmap allows you to scan your network and discover not only everything connected to it, but also a wide variety of information about what's connected, what services each host is operating, and so on. It allows a large number of scanning techniques, such as UDP, TCP and In this Practical we have also performed some nmap command and also saw the results obtained From it.

REFERENCES:

1. https://youtu.be/fp1042XK4A8
2. Nmap Theory: https://wiki.onap.org/display/DW/Nmap
3. Nmap latest Applications: https://www.cyberciti.biz/security/nmap-command-examples-tutorials/