

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
```

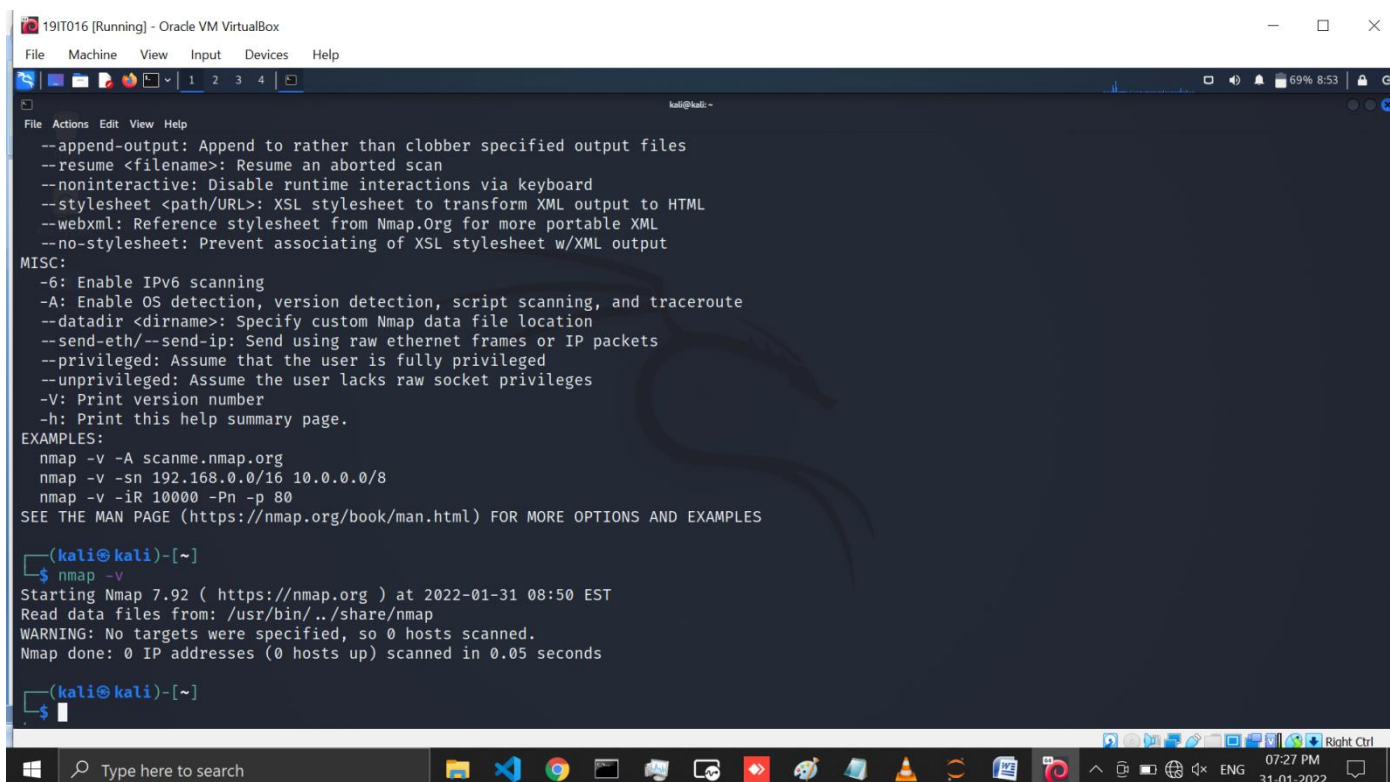
Print Host interfaces and routes

```
nmap --iflist
```

Enable OS Detection with Nmap

```
sudo nmap -O amazon.com
```

OUTPUT:

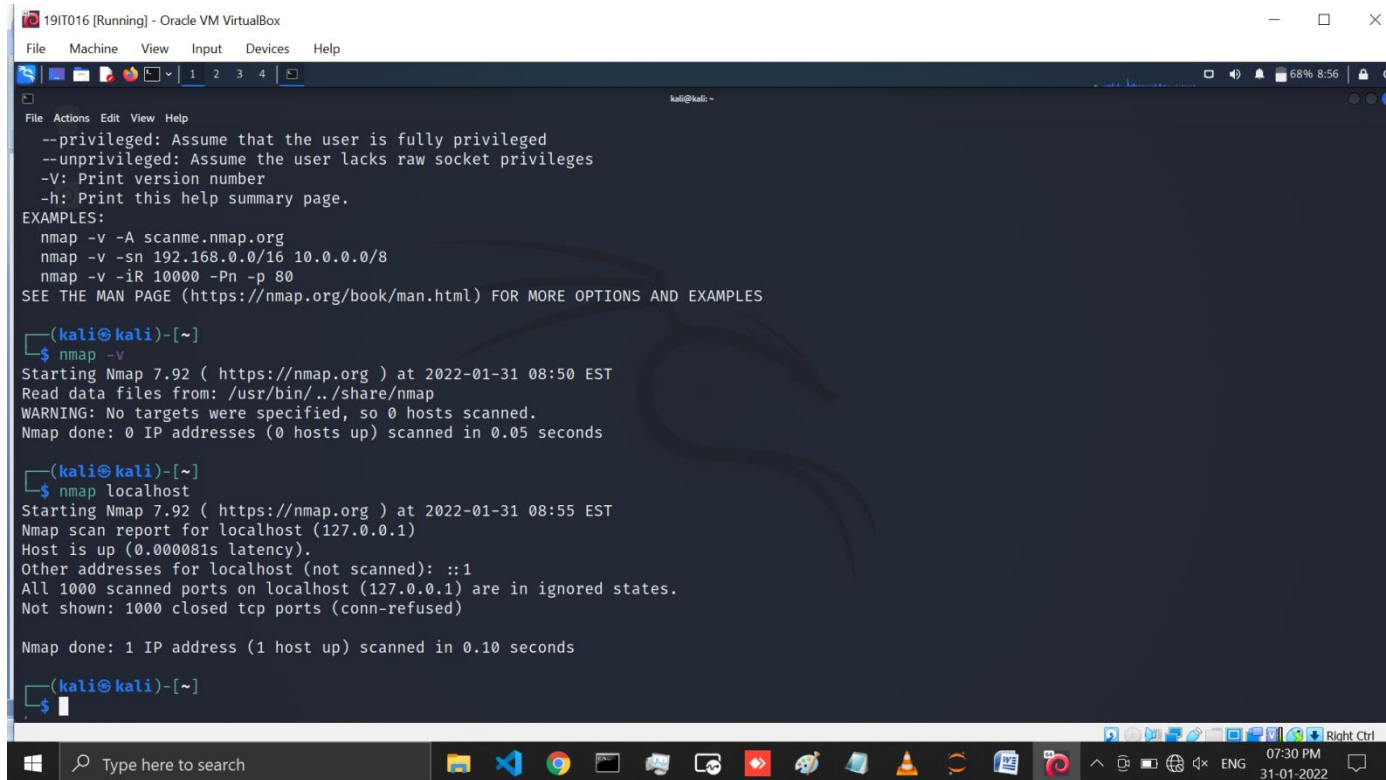


```
19IT016 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali:~$ nmap -v
--append-output: Append to rather than clobber specified output files
--resume <filename>: Resume an aborted scan
--noninteractive: Disable runtime interactions via keyboard
--stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
--webxml: Reference stylesheet from Nmap.Org for more portable XML
--no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
  -6: Enable IPv6 scanning
  -A: Enable OS detection, version detection, script scanning, and traceroute
  --datadir <dirname>: Specify custom Nmap data file location
  --send-eth/--send-ip: Send using raw ethernet frames or IP packets
  --privileged: Assume that the user is fully privileged
  --unprivileged: Assume the user lacks raw socket privileges
  -V: Print version number
  -h: Print this help summary page.
EXAMPLES:
  nmap -v -A scanme.nmap.org
  nmap -v -sn 192.168.0.0/16 10.0.0.0/8
  nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES

(kali@kali)-[~]
$ nmap -v
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-31 08:50 EST
Read data files from: /usr/bin/../share/nmap
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.05 seconds

(kali@kali)-[~]
$
```

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



```
19IT016 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali:~$ nmap -v
--privileged: Assume that the user is fully privileged
--unprivileged: Assume the user lacks raw socket privileges
-V: Print version number
-h: Print this help summary page.
EXAMPLES:
nmap -v -A scanme.nmap.org
nmap -v -sn 192.168.0.0/16 10.0.0.0/8
nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES

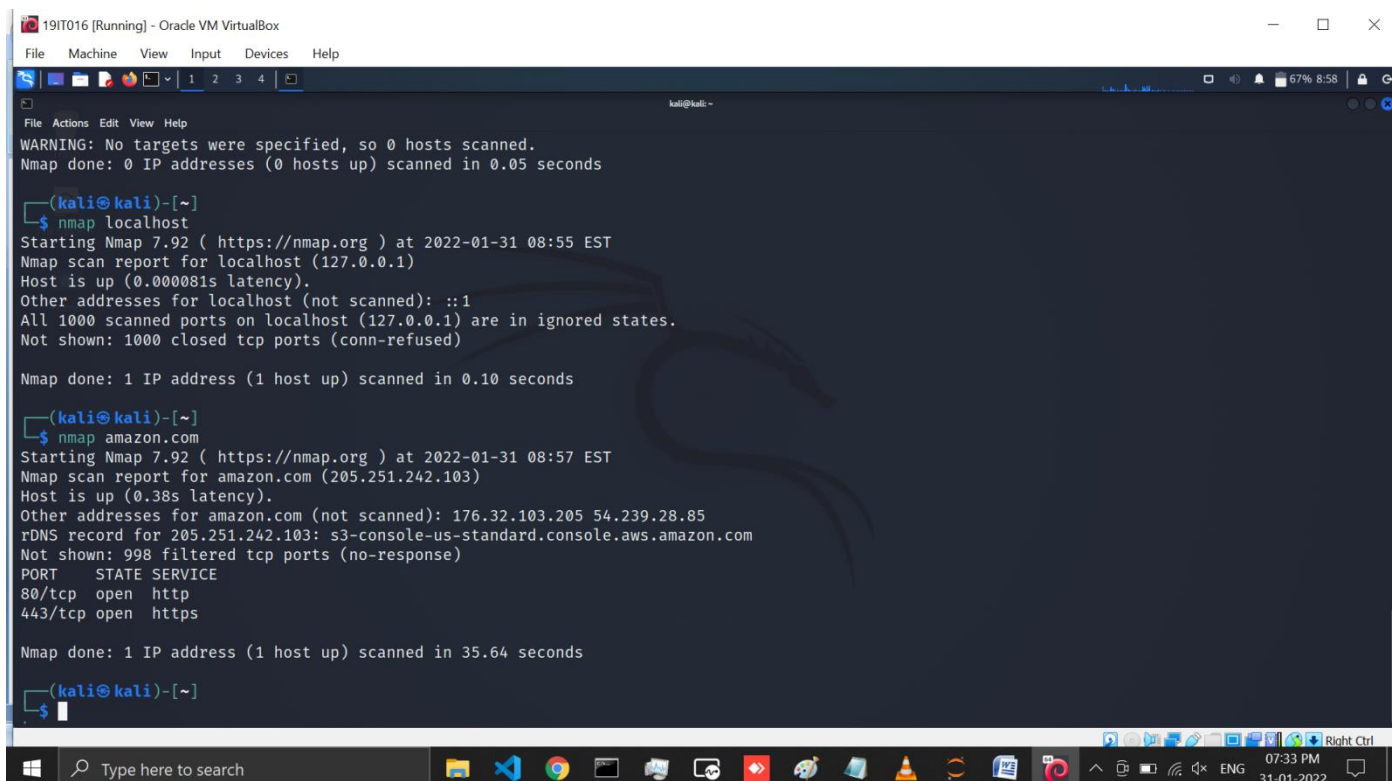
(kali@kali)-[~]
$ nmap -v
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-31 08:50 EST
Read data files from: /usr/bin/../share/nmap
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.05 seconds

(kali@kali)-[~]
$ nmap localhost
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-31 08:55 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000081s latency).
Other addresses for localhost (not scanned): ::1
All 1000 scanned ports on localhost (127.0.0.1) are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds

(kali@kali)-[~]
$
```

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



```
19IT016 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali:~$ nmap localhost
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.05 seconds

(kali@kali)-[~]
$ nmap localhost
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-31 08:55 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000081s latency).
Other addresses for localhost (not scanned): ::1
All 1000 scanned ports on localhost (127.0.0.1) are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

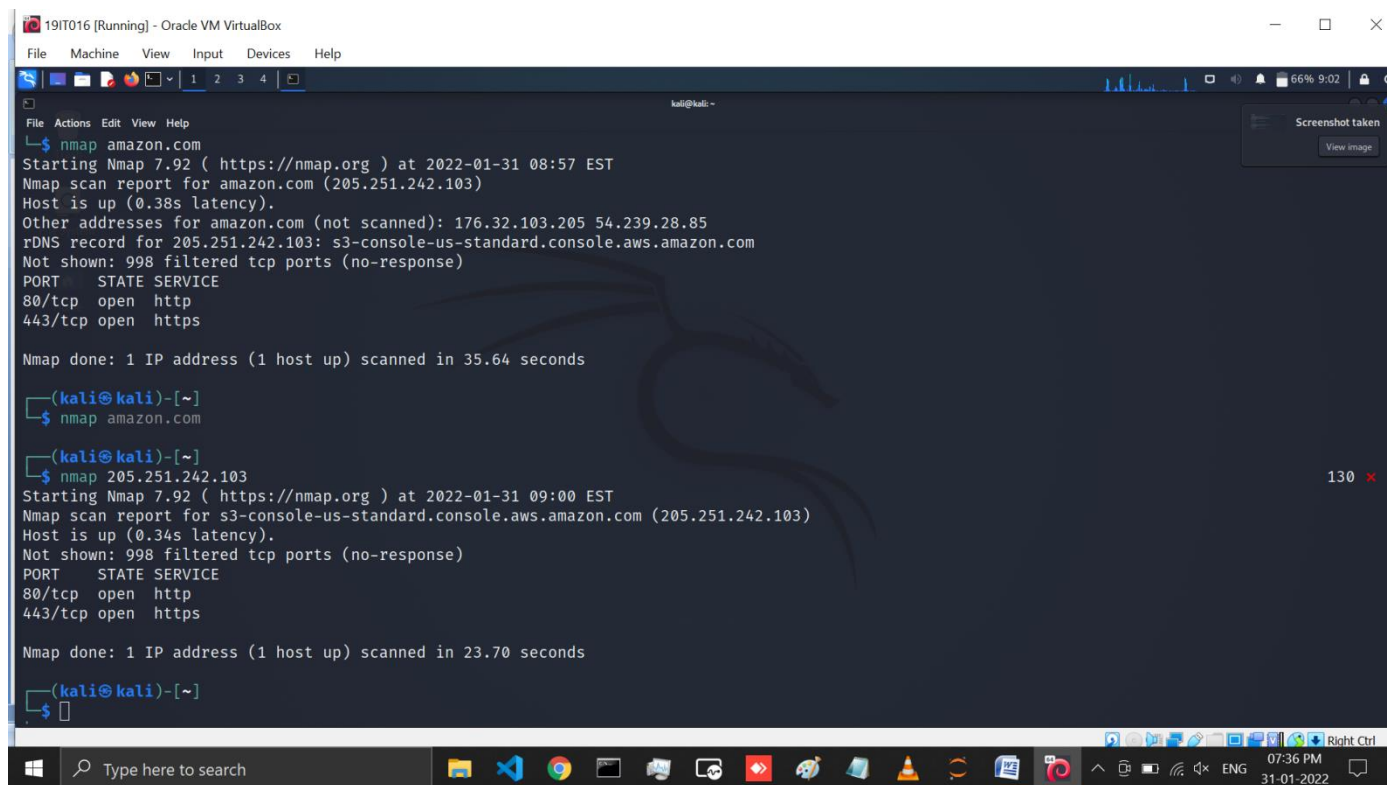
Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds

(kali@kali)-[~]
$ nmap amazon.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-31 08:57 EST
Nmap scan report for amazon.com (205.251.242.103)
Host is up (0.38s latency).
Other addresses for amazon.com (not scanned): 176.32.103.205 54.239.28.85
rDNS record for 205.251.242.103: s3-console-us-standard.console.aws.amazon.com
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 35.64 seconds

(kali@kali)-[~]
$
```

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



```

19IT016 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali: ~
$ nmap amazon.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-31 08:57 EST
Nmap scan report for amazon.com (205.251.242.103)
Host is up (0.38s latency).
Other addresses for amazon.com (not scanned): 176.32.103.205 54.239.28.85
rDNS record for 205.251.242.103: s3-console-us-standard.console.aws.amazon.com
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 35.64 seconds

(kali@kali)-[~]
$ nmap amazon.com

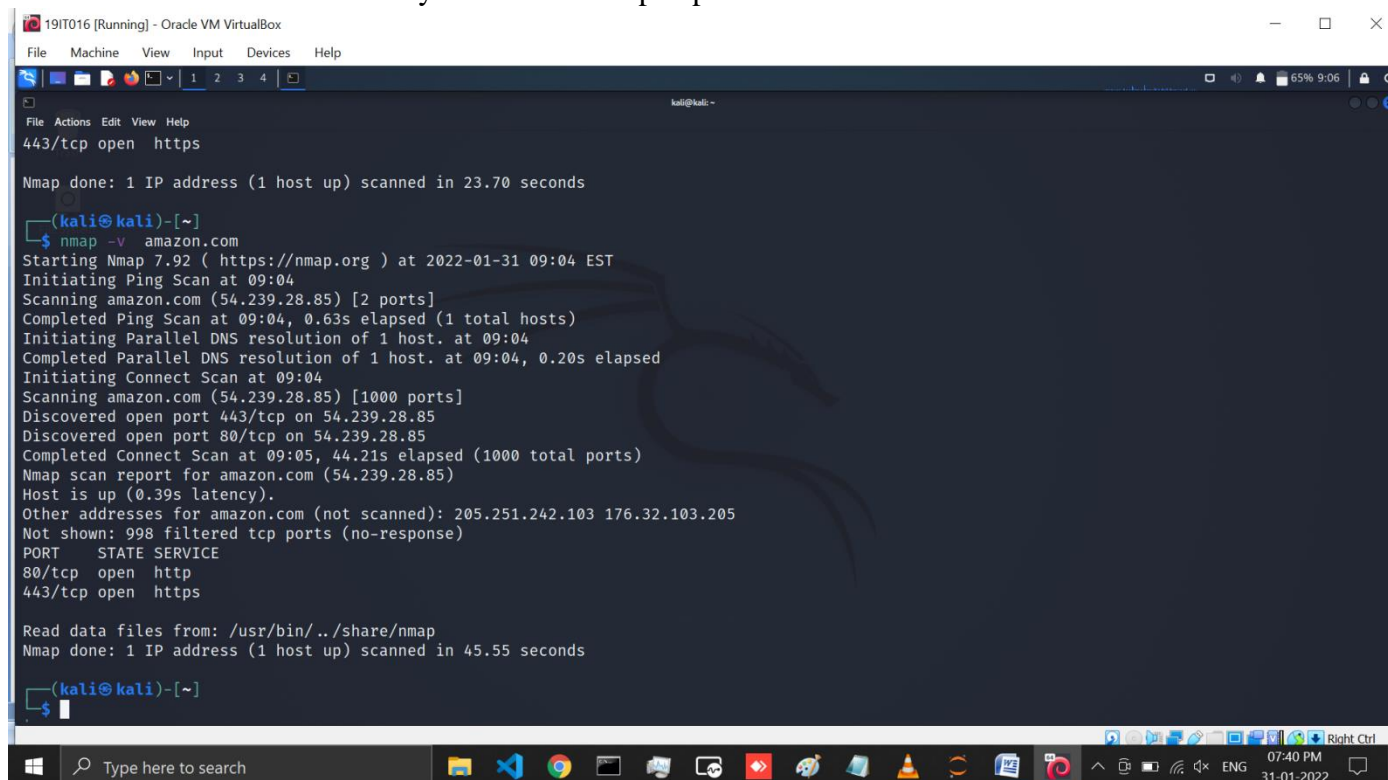
(kali@kali)-[~]
$ nmap 205.251.242.103
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-31 09:00 EST
Nmap scan report for s3-console-us-standard.console.aws.amazon.com (205.251.242.103)
Host is up (0.34s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 23.70 seconds

(kali@kali)-[~]
$

```

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



```

19IT016 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali: ~
443/tcp open https

Nmap done: 1 IP address (1 host up) scanned in 23.70 seconds

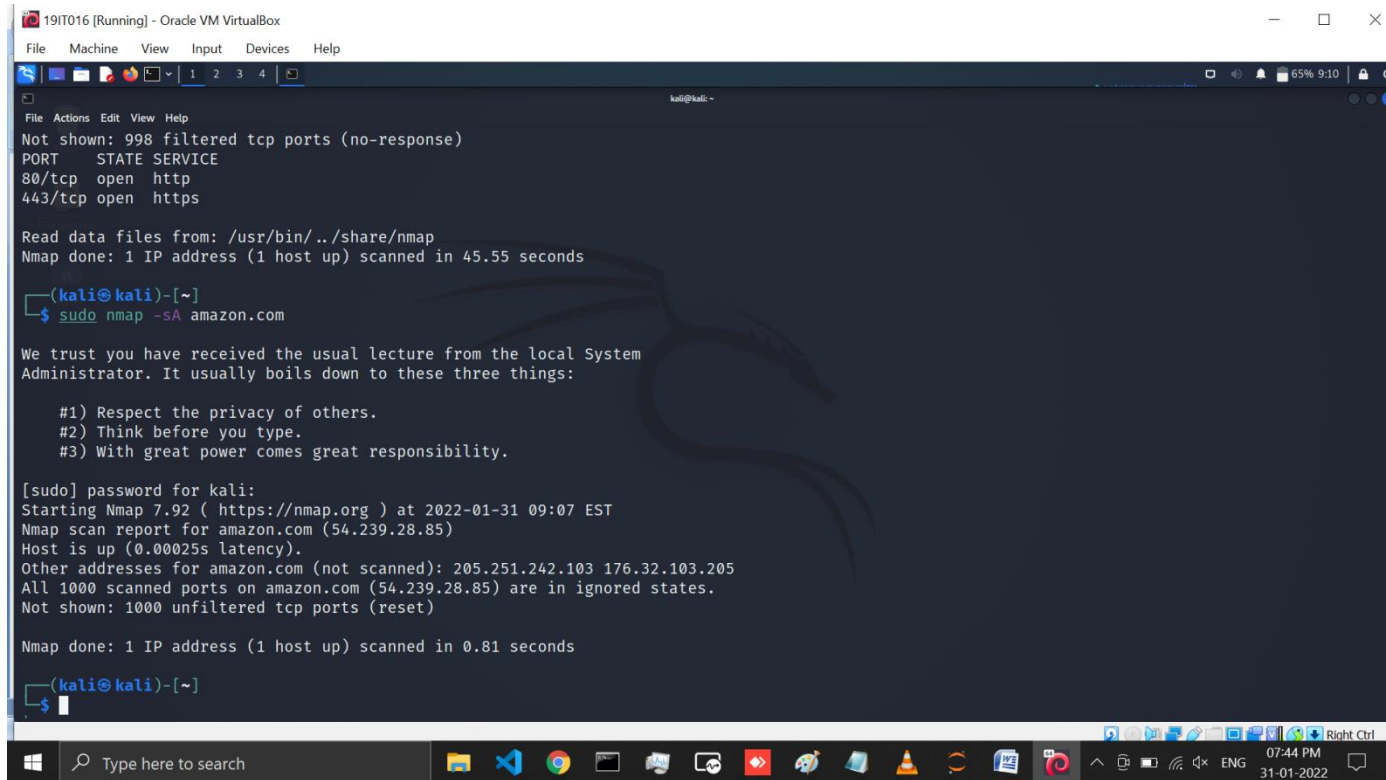
(kali@kali)-[~]
$ nmap -v amazon.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-31 09:04 EST
Initiating Ping Scan at 09:04
Scanning amazon.com (54.239.28.85) [2 ports]
Completed Ping Scan at 09:04, 0.63s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 09:04
Completed Parallel DNS resolution of 1 host. at 09:04, 0.20s elapsed
Initiating Connect Scan at 09:04
Scanning amazon.com (54.239.28.85) [1000 ports]
Discovered open port 443/tcp on 54.239.28.85
Discovered open port 80/tcp on 54.239.28.85
Completed Connect Scan at 09:05, 44.21s elapsed (1000 total ports)
Nmap scan report for amazon.com (54.239.28.85)
Host is up (0.39s latency).
Other addresses for amazon.com (not scanned): 205.251.242.103 176.32.103.205
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 45.55 seconds

(kali@kali)-[~]
$

```

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



```

19IT016 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali: ~
File Actions Edit View Help
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 45.55 seconds

(kali@kali)-[~]
$ sudo nmap -sA amazon.com

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

#1) Respect the privacy of others.
#2) Think before you type.
#3) With great power comes great responsibility.

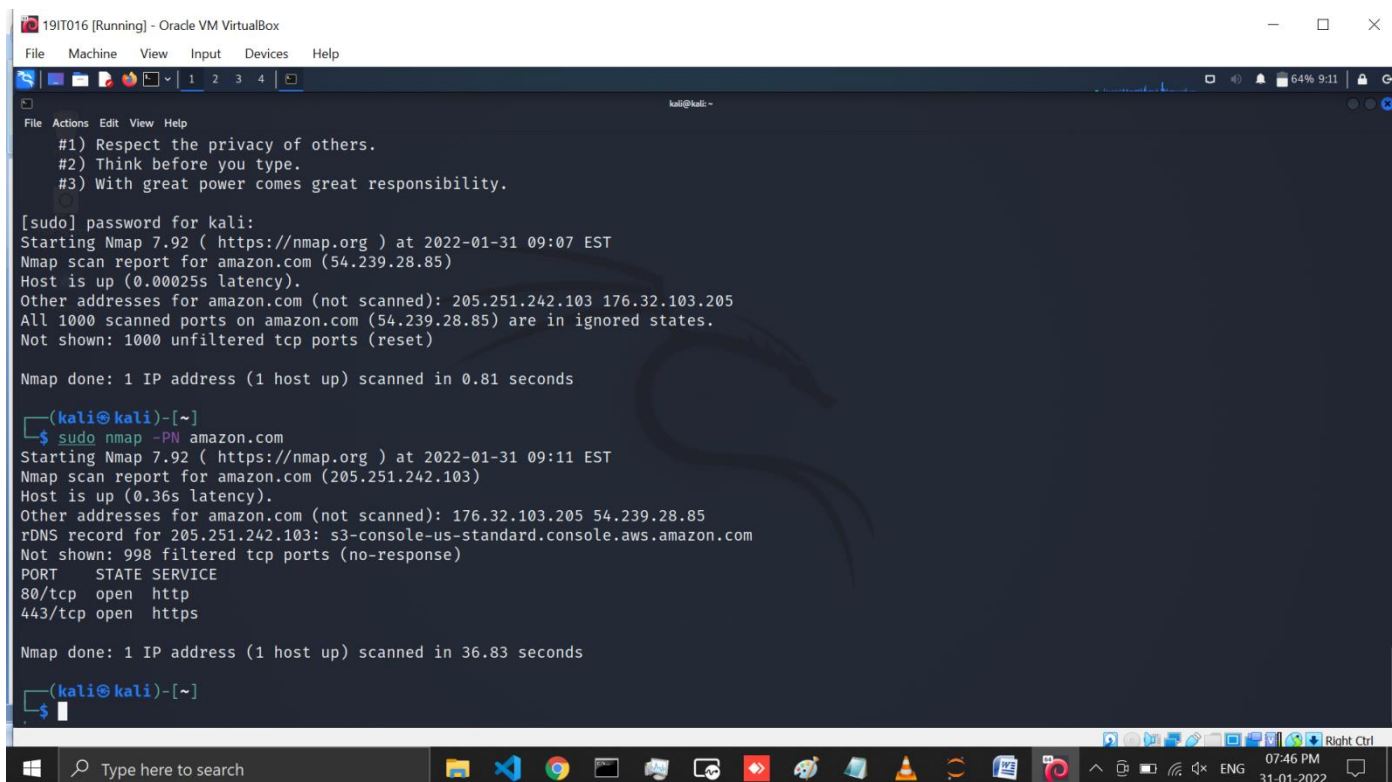
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-31 09:07 EST
Nmap scan report for amazon.com (54.239.28.85)
Host is up (0.00025s latency).
Other addresses for amazon.com (not scanned): 205.251.242.103 176.32.103.205
All 1000 scanned ports on amazon.com (54.239.28.85) are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.81 seconds

(kali@kali)-[~]
$

```

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



```

19IT016 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali: ~
File Actions Edit View Help
#1) Respect the privacy of others.
#2) Think before you type.
#3) With great power comes great responsibility.

[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-31 09:07 EST
Nmap scan report for amazon.com (54.239.28.85)
Host is up (0.00025s latency).
Other addresses for amazon.com (not scanned): 205.251.242.103 176.32.103.205
All 1000 scanned ports on amazon.com (54.239.28.85) are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.81 seconds

(kali@kali)-[~]
$ sudo nmap -PN amazon.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-31 09:11 EST
Nmap scan report for amazon.com (205.251.242.103)
Host is up (0.36s latency).
Other addresses for amazon.com (not scanned): 176.32.103.205 54.239.28.85
rDNS record for 205.251.242.103: s3-console-us-standard.console.aws.amazon.com
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 36.83 seconds

(kali@kali)-[~]
$

```

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

```

19IT016 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

#1) Respect the privacy of others.
#2) Think before you type.
#3) With great power comes great responsibility.

[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-31 09:07 EST
Nmap scan report for amazon.com (54.239.28.85)
Host is up (0.00025s latency).
Other addresses for amazon.com (not scanned): 205.251.242.103 176.32.103.205
All 1000 scanned ports on amazon.com (54.239.28.85) are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.81 seconds

(kali@kali)-[~]
$ sudo nmap -PN amazon.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-31 09:11 EST
Nmap scan report for amazon.com (205.251.242.103)
Host is up (0.36s latency).
Other addresses for amazon.com (not scanned): 176.32.103.205 54.239.28.85
rDNS record for 205.251.242.103: s3-console-us-standard.console.aws.amazon.com
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 36.83 seconds

(kali@kali)-[~]
$

```

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

```

19IT016 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Not shown: 98 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 12.83 seconds

(kali@kali)-[~]
$ nmap --iflist
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-31 09:14 EST
*****INTERFACES*****
DEV (SHORT) IP/MASK      TYPE      UP MTU  MAC
lo (lo)      127.0.0.1/8            loopback  up 65536
lo (lo)      ::1/128               loopback  up 65536
eth0 (eth0)  10.0.2.15/24          ethernet  up 1500  08:00:27:BE:20:60
eth0 (eth0)  fe80::a00:27ff:febe:2060/64 ethernet  up 1500  08:00:27:BE:20:60

*****ROUTES*****
DST/MASK      DEV  METRIC GATEWAY
10.0.2.0/24   eth0 100
0.0.0.0/0     eth0 100    10.0.2.2
::1/128       lo    0
fe80::a00:27ff:febe:2060/128 eth0 0
::1/128       lo    256
fe80::/64     eth0 100
ff00::/8      eth0 256

(kali@kali)-[~]
$

```

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

```

(kali@kali)-[~]
$ sudo nmap -o amazon.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-31 09:17 EST
Nmap scan report for amazon.com (176.32.103.205)
Host is up (0.14s latency).
Other addresses for amazon.com (not scanned): 205.251.242.103 54.239.28.85
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge|general purpose
Running (JUST GUESSING): Oracle Virtualbox (97%), QEMU (93%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (97%), QEMU user mode network gateway (93%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.10 seconds

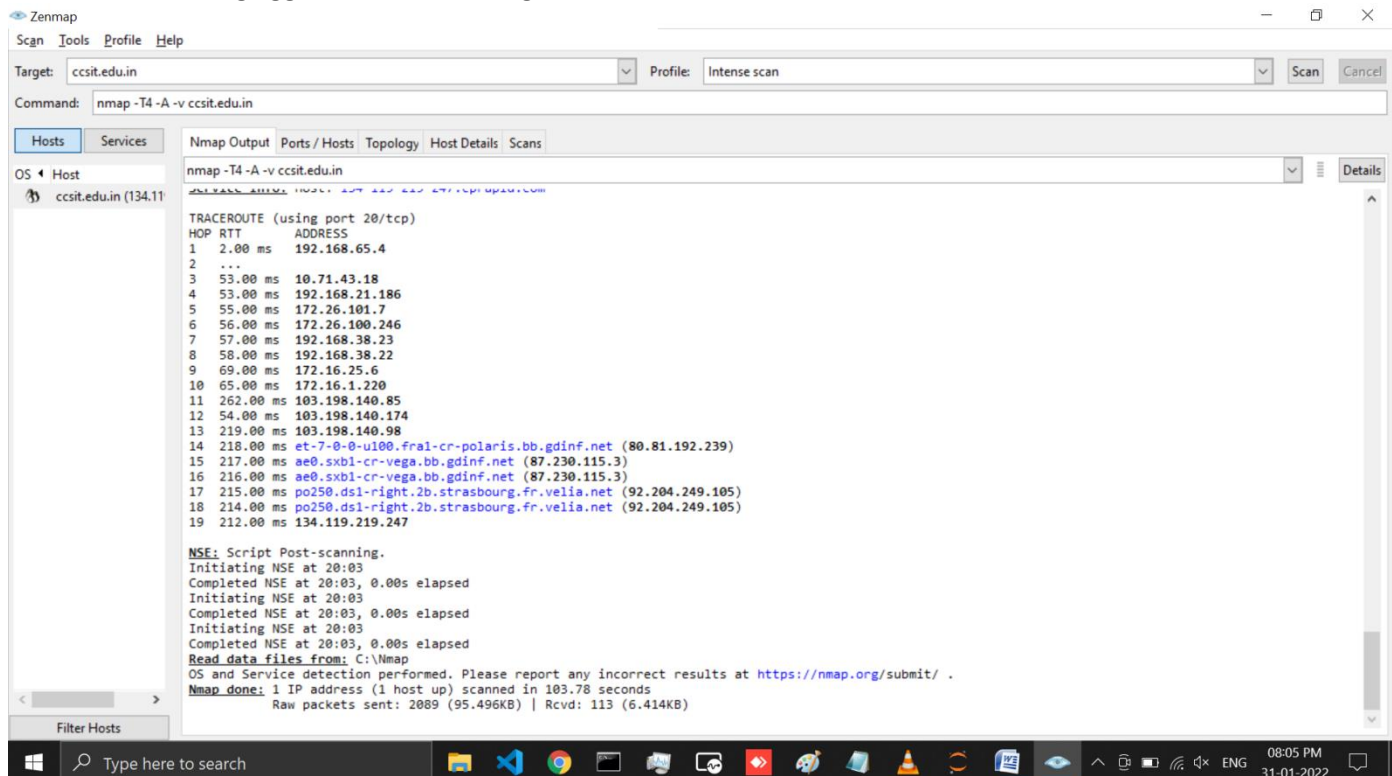
(kali@kali)-[~]
$ sudo nmap -o charusat.ac.in
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-31 09:19 EST
Nmap scan report for charusat.ac.in (185.151.30.139)
Host is up (0.010s latency).
Other addresses for charusat.ac.in (not scanned): 2a07:7800::139
rDNS record for 185.151.30.139: 185-151-30-139.ptr4.stackcp.net
Not shown: 998 filtered tcp ports (no-response)

```

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

Obtaining all necessary information of target host using Zenmap.

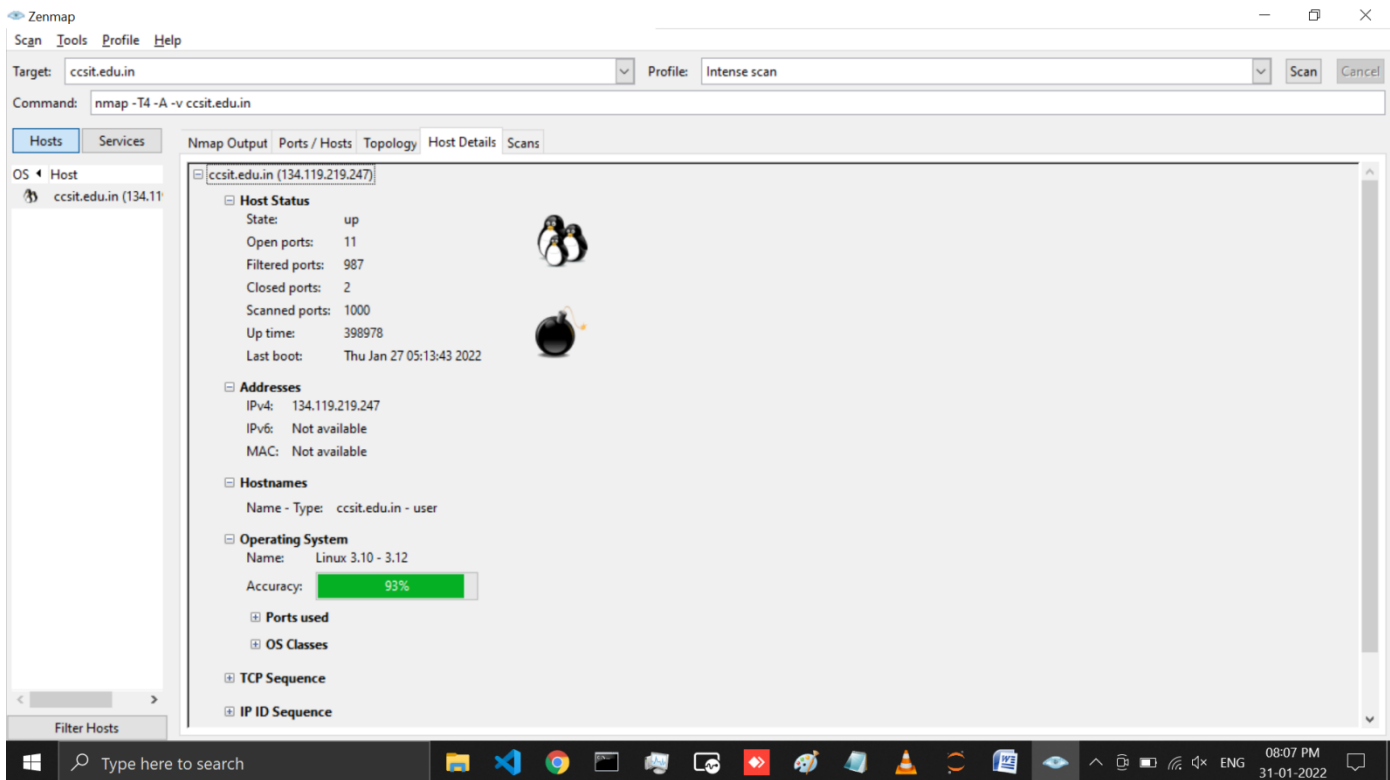
- Performing aggressive scans in target host



-
- The screenshot shows the Zenmap application window. At the top, the 'Target' field is set to 'ccsit.edu.in' and the 'Profile' is 'Intense scan'. The 'Command' field contains 'nmap -T4 -A -v ccsit.edu.in'. Below this, the 'Hosts' tab is selected in the left sidebar, showing a list of hosts with 'ccsit.edu.in (134.111.111.111)' highlighted. The main window displays the 'Nmap Output' tab, which contains a table of scan results. The table has columns for Port, Protocol, State, Service, and Version. The results show several open ports with their corresponding services and versions.
- | Port | Protocol | State | Service | Version |
|------|----------|--------|-----------|-------------------------------------|
| 20 | tcp | closed | ftp-data | |
| 21 | tcp | open | ftp | ProFTPD |
| 22 | tcp | open | ssh | OpenSSH 7.4 (protocol 2.0) |
| 53 | tcp | open | domain | PowerDNS Authoritative Server 4.4.1 |
| 80 | tcp | open | http | Apache httpd |
| 110 | tcp | open | pop3 | Dovecot pop3d |
| 143 | tcp | open | imap | Dovecot imapd |
| 443 | tcp | open | http | Apache httpd |
| 465 | tcp | open | smtp | Exim smtpd 4.94.2 |
| 587 | tcp | open | smtp | Exim smtpd 4.94.2 |
| 993 | tcp | open | imaps | |
| 995 | tcp | open | pop3s | |
| 8443 | tcp | closed | https-alt | |

-
- The screenshot shows the Zenmap application window. At the top, the 'Target' field is set to 'ccsit.edu.in' and the 'Profile' is 'Intense scan'. The 'Command' field contains 'nmap -T4 -A -v ccsit.edu.in'. The 'Hosts' tab is selected in the left sidebar, showing a list of discovered hosts. The main window displays a radar chart with concentric circles representing the scan progress. A red dot at the center indicates the target host. The bottom status bar shows the system clock as 08:07 PM on 31-01-2022.

- 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/>