

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 wall.alphacoders.com
```

Scan using IP Address
 nmap 144.217.71.114

Scan using -v option
 nmap -v wall.alphacoders.com

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

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

Perform a Fast scan
 nmap -F wall.alphacoders.com

Print Host interfaces and routes
 nmap --iflist

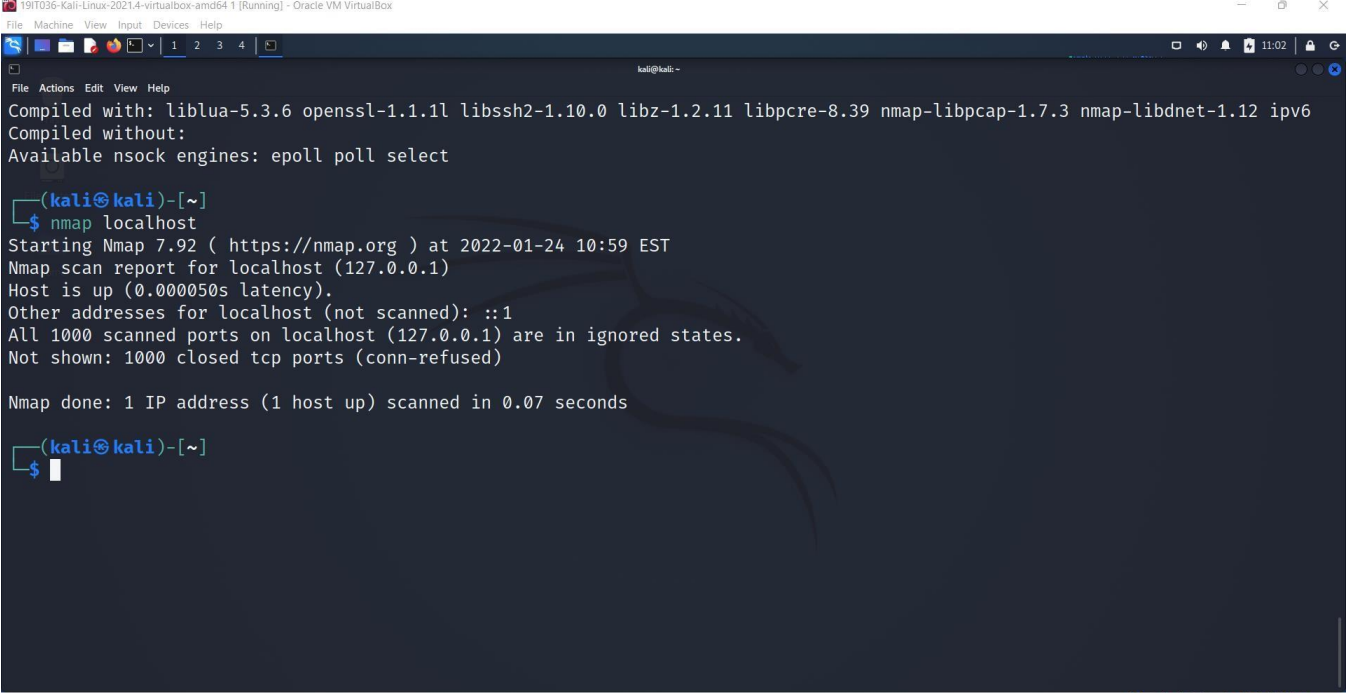
Enable OS Detection with Nmap
 sudo nmap -O wall.alphacoders.com

OUTPUT:

```

19IT036-Kali-Linux-2021.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
--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
Nmap version 7.92 ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.3.6 openssl-1.1.1l libssh2-1.10.0 libz-1.2.11 libpcap-1.7.3 nmap-libpcap-1.7.3 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select
kali@kali:~$
  
```

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

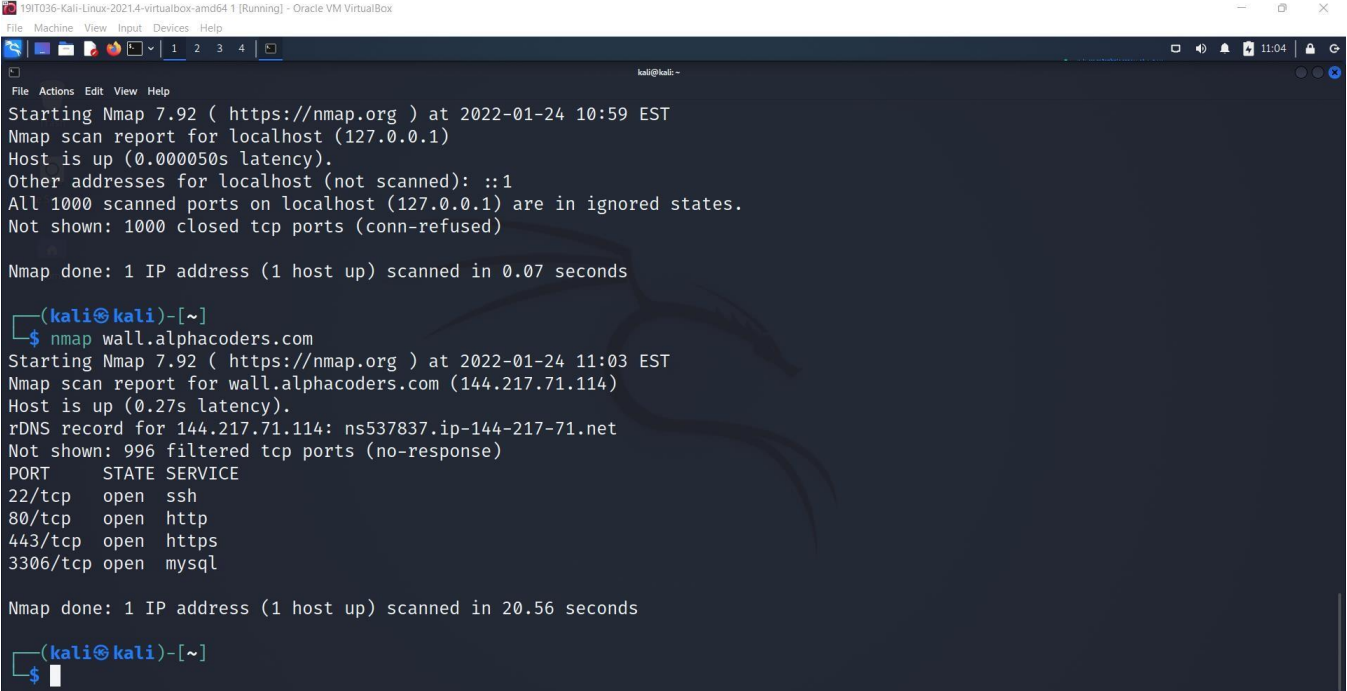


```
19IT036-Kali-Linux-2021.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali:~$ nmap localhost
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-24 10:59 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000050s latency).
Other addresses for 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 0.07 seconds

kali@kali:~$
```

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



```
19IT036-Kali-Linux-2021.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali:~$ nmap wall.alphacoders.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-24 11:03 EST
Nmap scan report for wall.alphacoders.com (144.217.71.114)
Host is up (0.27s latency).
rDNS record for 144.217.71.114: ns537837.ip-144-217-71.net
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
3306/tcp  open  mysql

Nmap done: 1 IP address (1 host up) scanned in 20.56 seconds

kali@kali:~$
```

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

```

19IT036-Kali-Linux-2021.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
rDNS record for 144.217.71.114: ns537837.ip-144-217-71.net
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
3306/tcp   open  mysql

Nmap done: 1 IP address (1 host up) scanned in 20.56 seconds

(kali@kali)-[~]
$ nmap 144.217.71.114
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-24 11:05 EST
Nmap scan report for ns537837.ip-144-217-71.net (144.217.71.114)
Host is up (0.26s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
3306/tcp   open  mysql

Nmap done: 1 IP address (1 host up) scanned in 19.30 seconds

(kali@kali)-[~]
$

```

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

```

19IT036-Kali-Linux-2021.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
Nmap done: 1 IP address (1 host up) scanned in 19.30 seconds

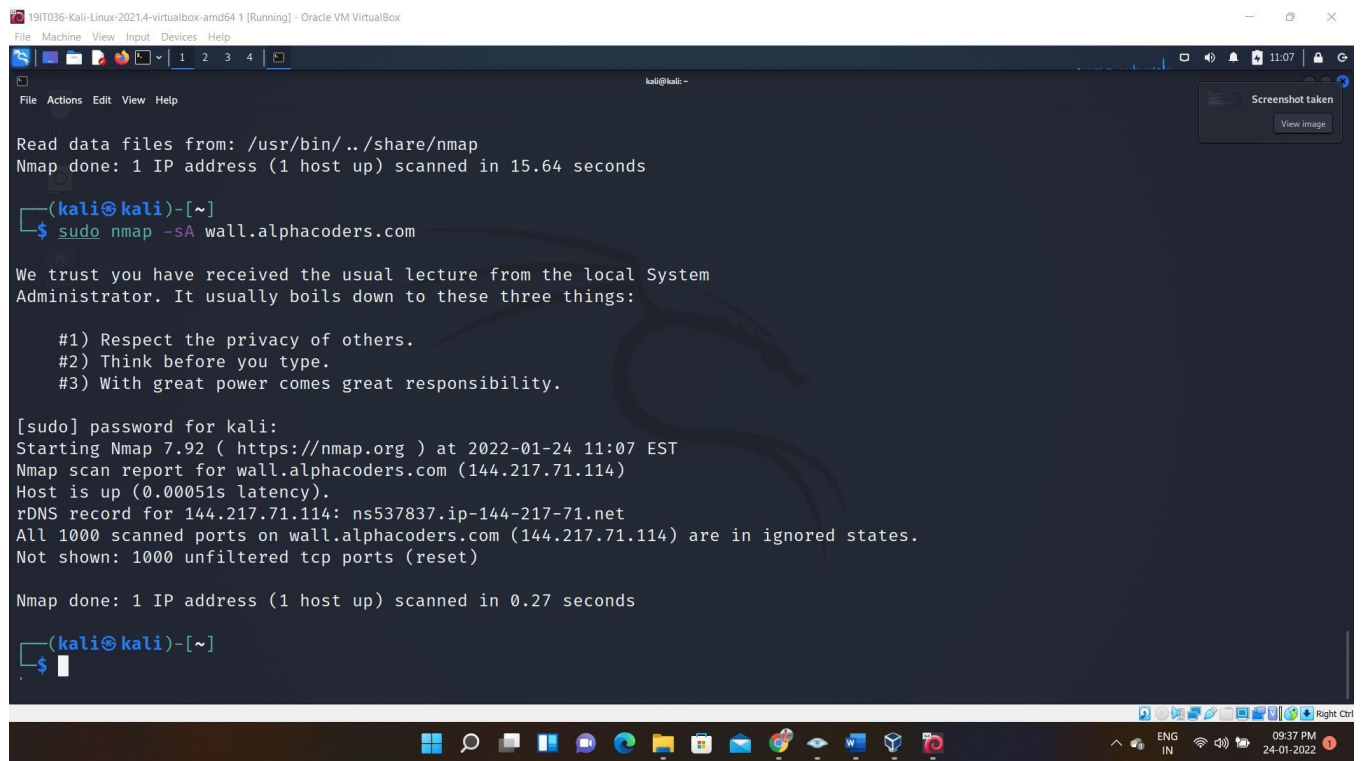
(kali@kali)-[~]
$ nmap -v wall.alphacoders.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-24 11:06 EST
Initiating Ping Scan at 11:06
Scanning wall.alphacoders.com (144.217.71.114) [2 ports]
Completed Ping Scan at 11:06, 0.27s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:06
Completed Parallel DNS resolution of 1 host. at 11:06, 0.01s elapsed
Initiating Connect Scan at 11:06
Scanning wall.alphacoders.com (144.217.71.114) [1000 ports]
Discovered open port 443/tcp on 144.217.71.114
Discovered open port 80/tcp on 144.217.71.114
Discovered open port 3306/tcp on 144.217.71.114
Discovered open port 22/tcp on 144.217.71.114
Completed Connect Scan at 11:06, 15.18s elapsed (1000 total ports)
Nmap scan report for wall.alphacoders.com (144.217.71.114)
Host is up (0.26s latency).
rDNS record for 144.217.71.114: ns537837.ip-144-217-71.net
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
3306/tcp   open  mysql

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 15.64 seconds

(kali@kali)-[~]
$

```

Figure 5: In this page we have performed scan using `nmap -v` command on *wall.alphacoders.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.



```

19IT036-Kali-Linux-2021.4-virtualbox-amd64 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali:~$ sudo nmap -sA wall.alphacoders.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.

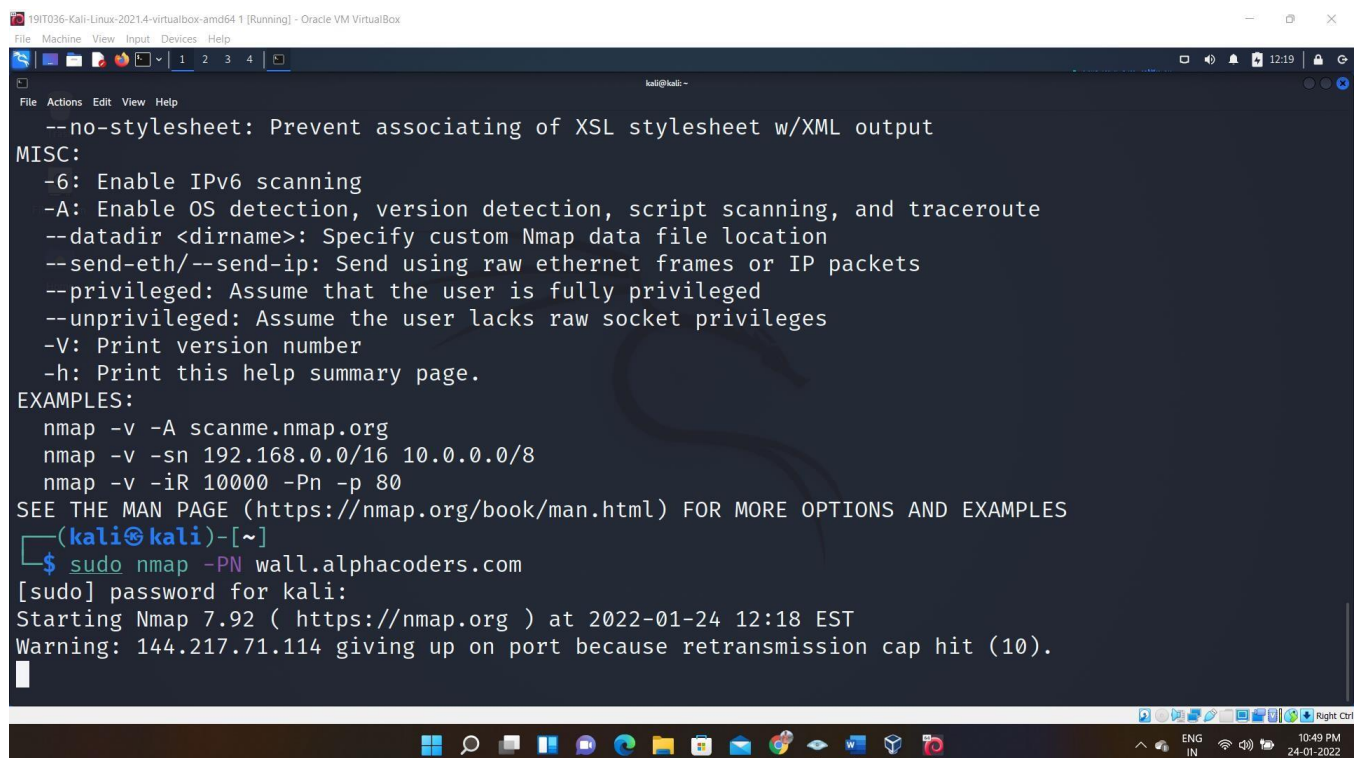
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-24 11:07 EST
Nmap scan report for wall.alphacoders.com (144.217.71.114)
Host is up (0.00051s latency).
rDNS record for 144.217.71.114: ns537837.ip-144-217-71.net
All 1000 scanned ports on wall.alphacoders.com (144.217.71.114) are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds

kali@kali:~$

```

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



```

19IT036-Kali-Linux-2021.4-virtualbox-amd64 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

--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:~$ sudo nmap -PN wall.alphacoders.com
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-24 12:18 EST
Warning: 144.217.71.114 giving up on port because retransmission cap hit (10).

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

```

19IT036-Kali-Linux-2021.4-virtualbox-amd64.1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali:~$ nmap -F wall.alphacoders.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-24 11:24 EST
Nmap scan report for wall.alphacoders.com (144.217.71.114)
Host is up (0.32s latency).
rDNS record for 144.217.71.114: ns537837.ip-144-217-71.net
Not shown: 96 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
3306/tcp   open  mysql

Nmap done: 1 IP address (1 host up) scanned in 9.58 seconds

kali@kali:~$

```

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

```

Nmap done: 1 IP address (1 host up) scanned in 9.58 seconds

kali@kali:~$ nmap --iflist
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-24 11:25 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

```

19IT036-Kali-Linux-2021.4-virtualbox-amd64.1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali:~$ nmap -h
-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:~$ sudo nmap -PN wall.alphacoders.com
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-24 12:18 EST
Warning: 144.217.71.114 giving up on port because retransmission cap hit (10).

kali@kali:~$ sudo nmap -O wall.alphacoders.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-24 12:20 EST
Warning: 144.217.71.114 giving up on port because retransmission cap hit (10).

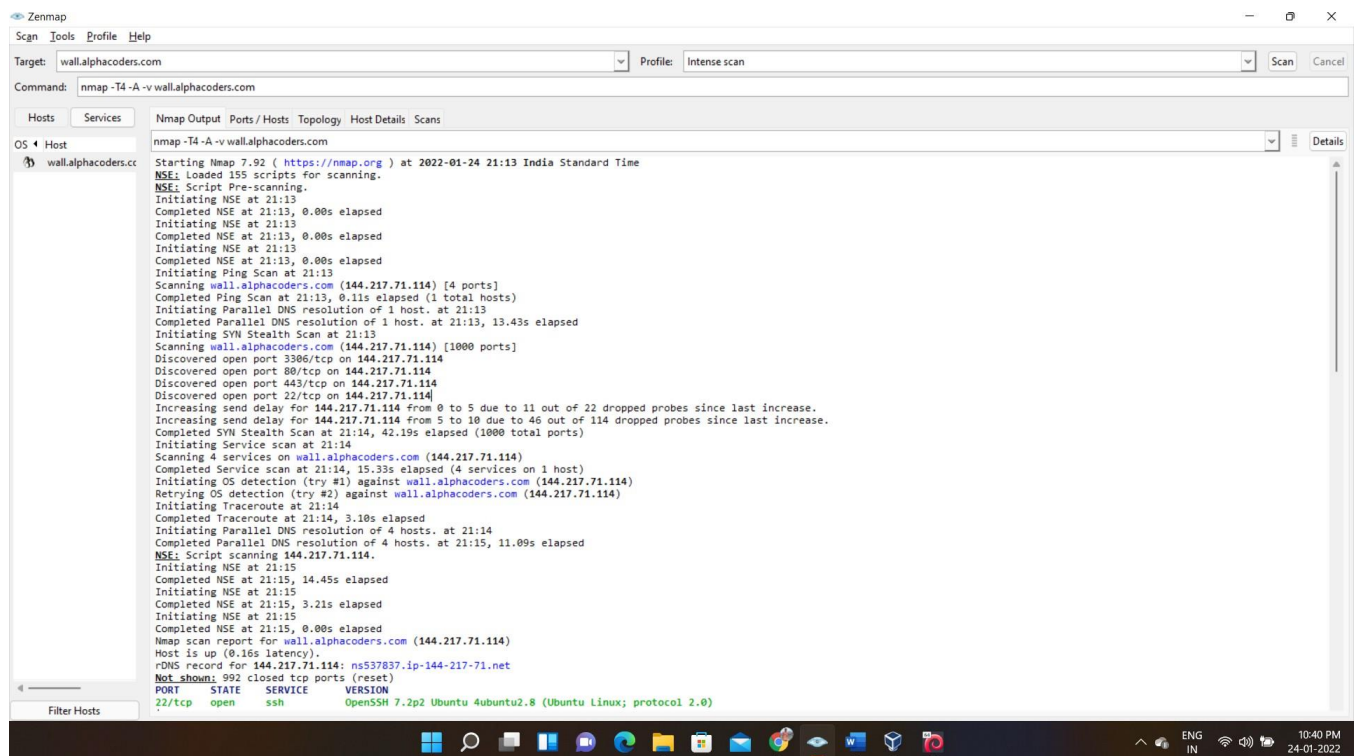
Nmap Output:
Nmap -T4 -A -v wall.alphacoders.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-24 21:13 India Standard Time
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 21:13
Completed NSE at 21:13, 0.00s elapsed
Initiating NSE at 21:13
Completed NSE at 21:13, 0.00s elapsed
Initiating NSE at 21:13
Completed NSE at 21:13, 0.00s elapsed
Initiating NSE at 21:13
Completed NSE at 21:13, 0.00s elapsed
Initiating Ping Scan at 21:13
Scanning wall.alphacoders.com (144.217.71.114) [4 ports]
Completed Ping Scan at 21:13, 0.11s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:13
Completed Parallel DNS resolution of 1 host. at 21:13, 13.43s elapsed
Initiating SYN Stealth Scan at 21:13
Scanning wall.alphacoders.com (144.217.71.114) [1000 ports]
Discovered open port 3306/tcp on 144.217.71.114
Discovered open port 80/tcp on 144.217.71.114
Discovered open port 443/tcp on 144.217.71.114
Discovered open port 22/tcp on 144.217.71.114
Increasing send delay for 144.217.71.114 from 0 to 5 due to 11 out of 22 dropped probes since last increase.
Increasing send delay for 144.217.71.114 from 5 to 10 due to 46 out of 114 dropped probes since last increase.
Completed SYN Stealth Scan at 21:14, 42.19s elapsed (1000 total ports)
Initiating Service scan at 21:14
Scanning 4 services on wall.alphacoders.com (144.217.71.114)
Completed Service scan at 21:14, 15.33s elapsed (4 services on 1 host)
Initiating OS detection (try #1) against wall.alphacoders.com (144.217.71.114)
Retrying OS detection (try #2) against wall.alphacoders.com (144.217.71.114)
Initiating Traceroute at 21:14
Completed Traceroute at 21:14, 3.10s elapsed
Initiating Parallel DNS resolution of 4 hosts. at 21:14
Completed Parallel DNS resolution of 4 hosts. at 21:15, 11.09s elapsed
NSE: Script scanning 144.217.71.114.
Initiating NSE at 21:15
Completed NSE at 21:15, 14.45s elapsed
Initiating NSE at 21:15
Completed NSE at 21:15, 3.21s elapsed
Initiating NSE at 21:15
Completed NSE at 21:15, 0.00s elapsed
Nmap scan report for wall.alphacoders.com (144.217.71.114)
Host is up (0.16s latency).
rDNS record for 144.217.71.114: ns537837.ip-144-217-71.net
PORT      STATE SERVICE
22/tcp    open  ssh
OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)

```

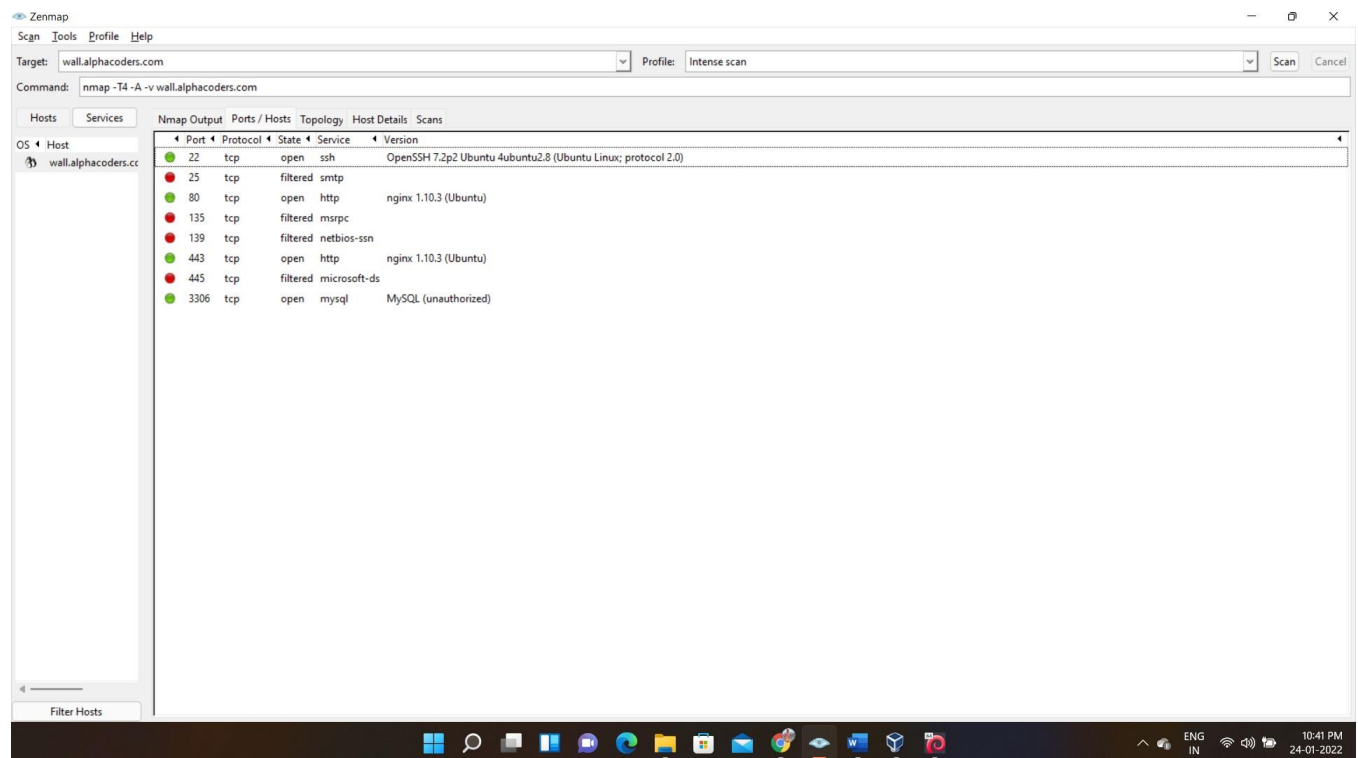
Figure 10: OS scanning is one of the most powerful features of Nmap. When using this type of scan, Nmap sends TCP and UDP packets to a particular port, and then analyze its response. It compares this response to a database of 2600 operating systems, and return information on the OS (and version) of a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

Obtaining all necessary information of target host using Zenmap.

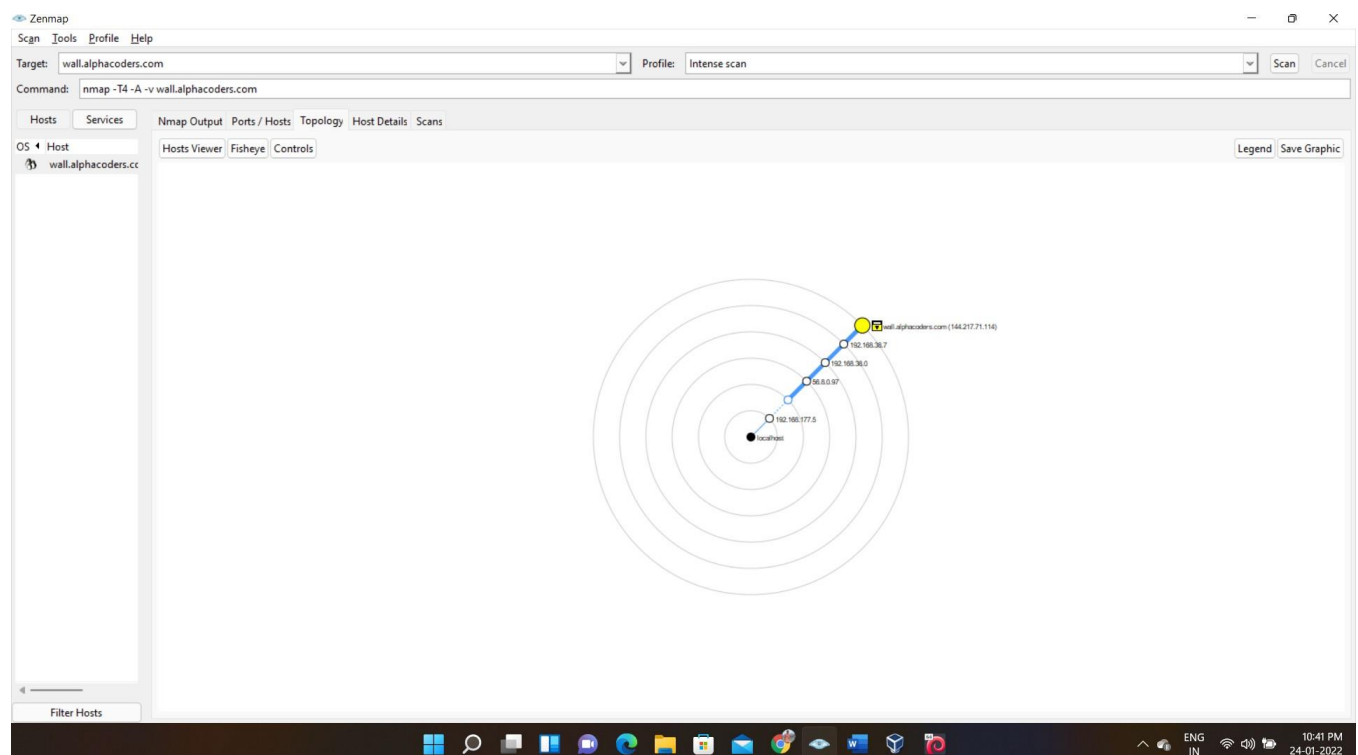
- Performing aggressive scans in target host



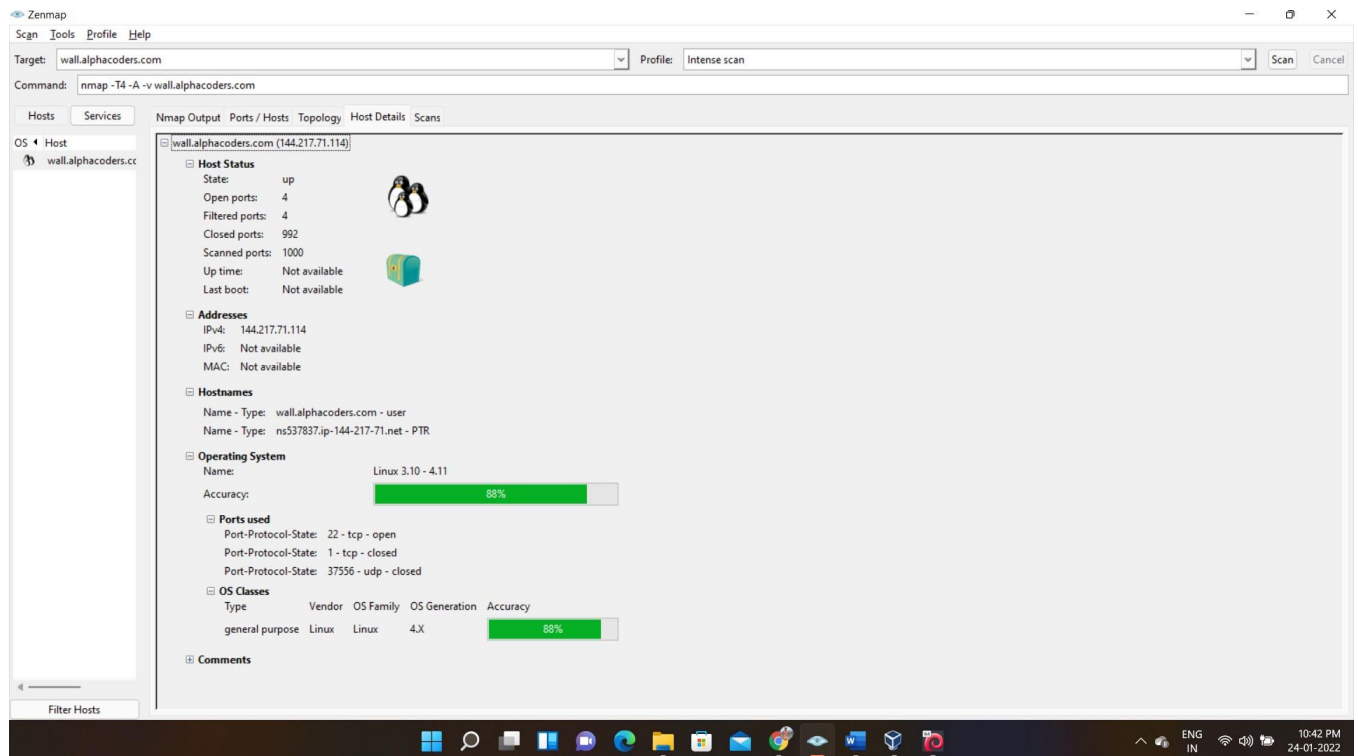
- In Ports/Hosts option we can see the open port of target host.



- 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/>