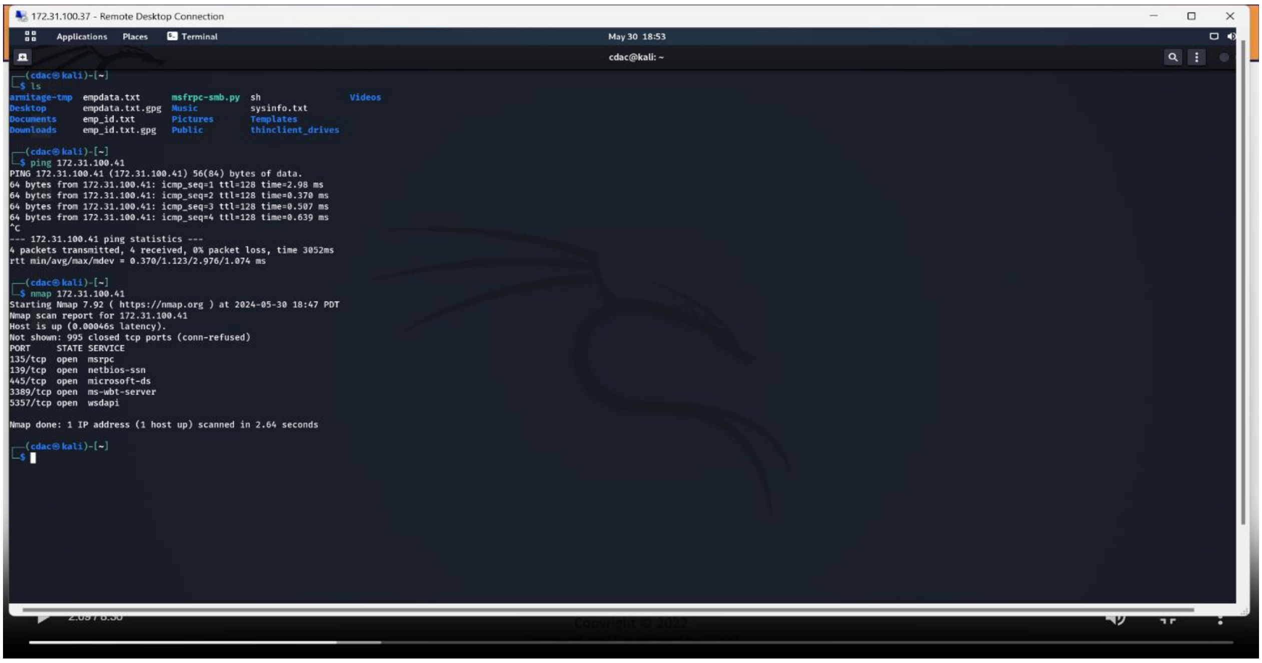
Name -Dinesh Pradhan

Topic – Nmap Assignment

1.Scanning port

$ nmap <target ip>

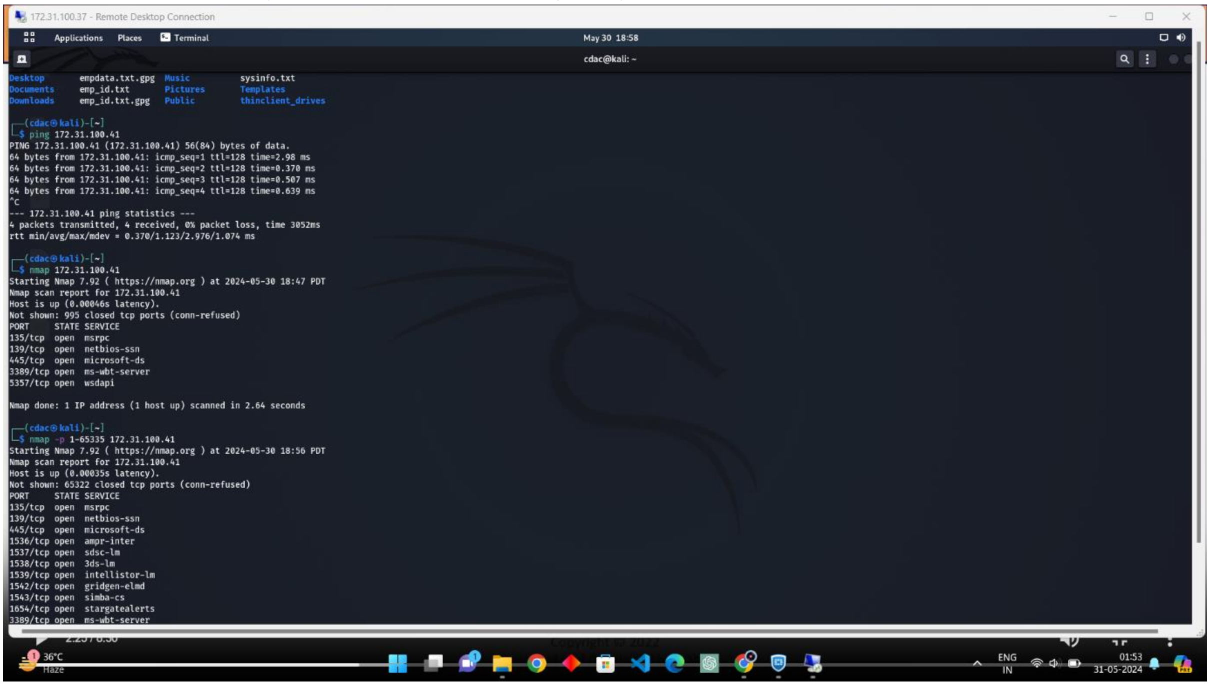


```
┌──(cdac㉿kali)-[~]
└─$ ls
armitage-tmp  empdata.txt      msfrpc-smb.py  sh                Videos
Desktop       empdata.txt.gpg  Music          sysinfo.txt
Documents     emp_id.txt       Pictures       Templates
Downloads     emp_id.txt.gpg   Public         thinclient_drives

┌──(cdac㉿kali)-[~]
└─$ ping 172.31.100.41
PING 172.31.100.41 (172.31.100.41) 56(84) bytes of data.
64 bytes from 172.31.100.41: icmp_seq=1 ttl=128 time=2.98 ms
64 bytes from 172.31.100.41: icmp_seq=2 ttl=128 time=0.370 ms
64 bytes from 172.31.100.41: icmp_seq=3 ttl=128 time=0.507 ms
64 bytes from 172.31.100.41: icmp_seq=4 ttl=128 time=0.639 ms
^C
--- 172.31.100.41 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3052ms
rtt min/avg/max/mdev = 0.370/1.123/2.976/1.074 ms

┌──(cdac㉿kali)-[~]
└─$ nmap 172.31.100.41
Starting Nmap 7.92 ( https://nmap.org ) at 2024-05-30 18:47 PDT
Nmap scan report for 172.31.100.41
Host is up (0.00046s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
5357/tcp open  wsdapi

Nmap done: 1 IP address (1 host up) scanned in 2.64 seconds

┌──(cdac㉿kali)-[~]
└─$ 
```

2.Scanning range of port

$ nmap -p 1-65535 <target ip>

- This command scan all the port from 1 to 65535 for a targeted ip or host .

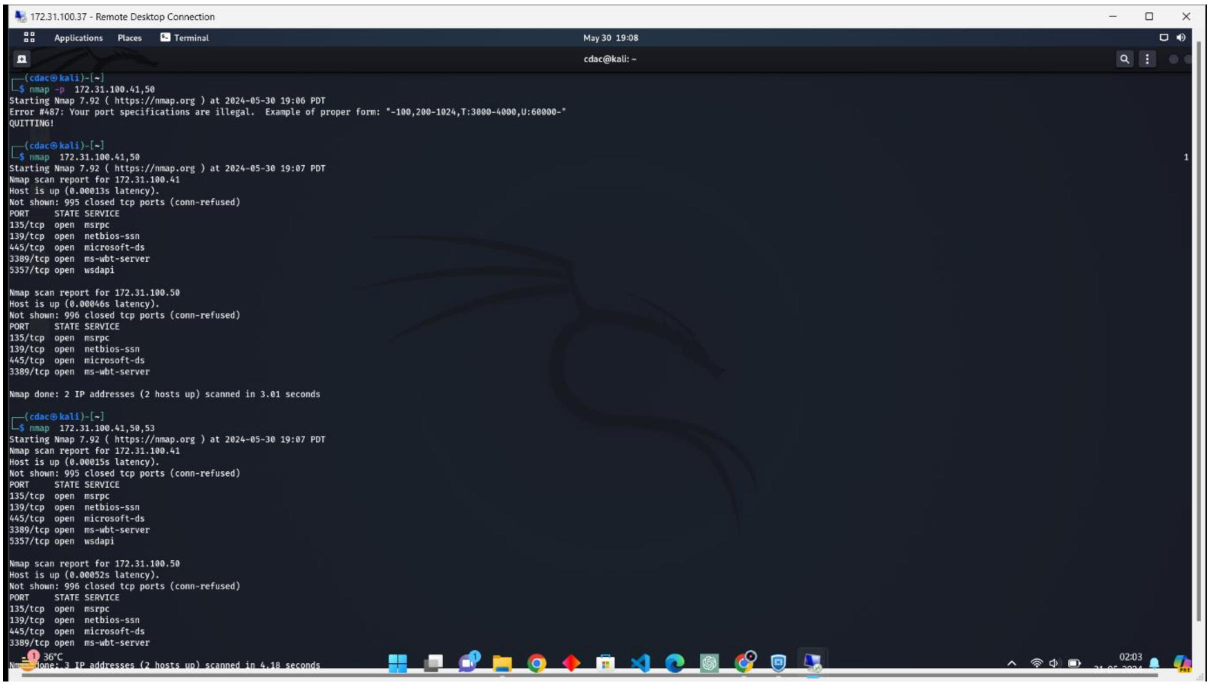


```
Desktop       empdata.txt.gpg  Music          sysinfo.txt
Documents     emp_id.txt       Pictures       Templates
Downloads     emp_id.txt.gpg   Public         thinclient_drives

┌──(cdac㉿kali)-[~]
└─$ ping 172.31.100.41
PING 172.31.100.41 (172.31.100.41) 56(84) bytes of data.
64 bytes from 172.31.100.41: icmp_seq=1 ttl=128 time=2.98 ms
64 bytes from 172.31.100.41: icmp_seq=2 ttl=128 time=0.370 ms
64 bytes from 172.31.100.41: icmp_seq=3 ttl=128 time=0.507 ms
64 bytes from 172.31.100.41: icmp_seq=4 ttl=128 time=0.639 ms
^C
--- 172.31.100.41 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3052ms
rtt min/avg/max/mdev = 0.370/1.123/2.976/1.074 ms

┌──(cdac㉿kali)-[~]
└─$ nmap 172.31.100.41
Starting Nmap 7.92 ( https://nmap.org ) at 2024-05-30 18:47 PDT
Nmap scan report for 172.31.100.41
Host is up (0.00046s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
5357/tcp open  wsdapi

Nmap done: 1 IP address (1 host up) scanned in 2.64 seconds

┌──(cdac㉿kali)-[~]
└─$ nmap -p 1-65335 172.31.100.41
Starting Nmap 7.92 ( https://nmap.org ) at 2024-05-30 18:56 PDT
Nmap scan report for 172.31.100.41
Host is up (0.00035s latency).
Not shown: 65322 closed tcp ports (conn-refused)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1536/tcp open  ampr-inter
1537/tcp open  sdsc-lm
1538/tcp open  3ds-lm
1539/tcp open  intellistor-lm
1542/tcp open  gridgen-elmd
1543/tcp open  simba-cs
1654/tcp open  stargatealerts
3389/tcp open  ms-wbt-server
```

3.Scanning multiple ip addresses

$ nmap -p 1-65535 <target ip>,<target ip>

- We can scan multiple ip addresses in the command separated by commas .



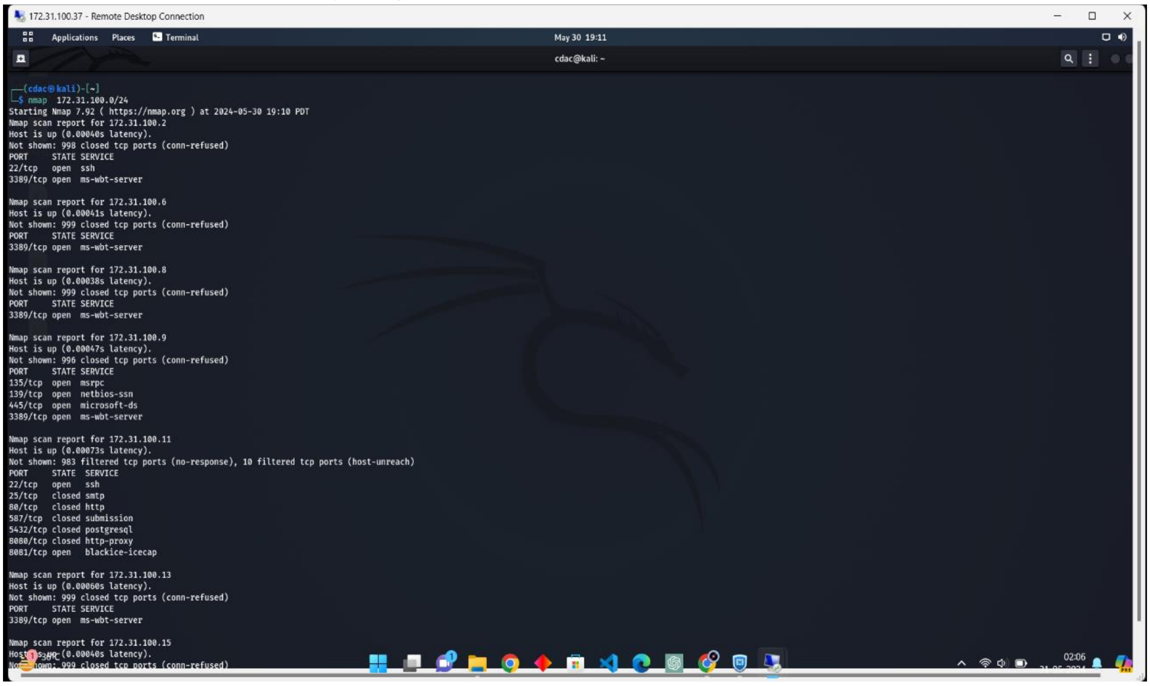
```
┌──(cdac㉿kali)-[~]
└─$ nmap -p  172.31.100.41,50
Starting Nmap 7.92 ( https://nmap.org ) at 2024-05-30 19:06 PDT
Error #487: Your port specifications are illegal.  Example of proper form: "-100,200-1024,T:3000-4000,U:60000-"
QUITTING!

┌──(cdac㉿kali)-[~]
└─$ nmap  172.31.100.41,50
Starting Nmap 7.92 ( https://nmap.org ) at 2024-05-30 19:07 PDT
Nmap scan report for 172.31.100.41
Host is up (0.00013s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
5357/tcp open  wsdapi

Nmap scan report for 172.31.100.50
Host is up (0.00046s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server

Nmap done: 2 IP addresses (2 hosts up) scanned in 3.01 seconds

┌──(cdac㉿kali)-[~]
└─$ nmap  172.31.100.41,50,53
Starting Nmap 7.92 ( https://nmap.org ) at 2024-05-30 19:07 PDT
Nmap scan report for 172.31.100.41
Host is up (0.00015s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
5357/tcp open  wsdapi

Nmap scan report for 172.31.100.50
Host is up (0.00052s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server

Nmap done: 3 IP addresses (2 hosts up) scanned in 4.18 seconds
```

- In this image ip addresses 172.31.100.50 and 172.31.100.53 are being scanned by single command .

4.Scanning multiple ip ranges

$ nmap   172.31.100.0/24

- This above will scan all the ip ranges from 172.31.100.0 to 172.31.100.255

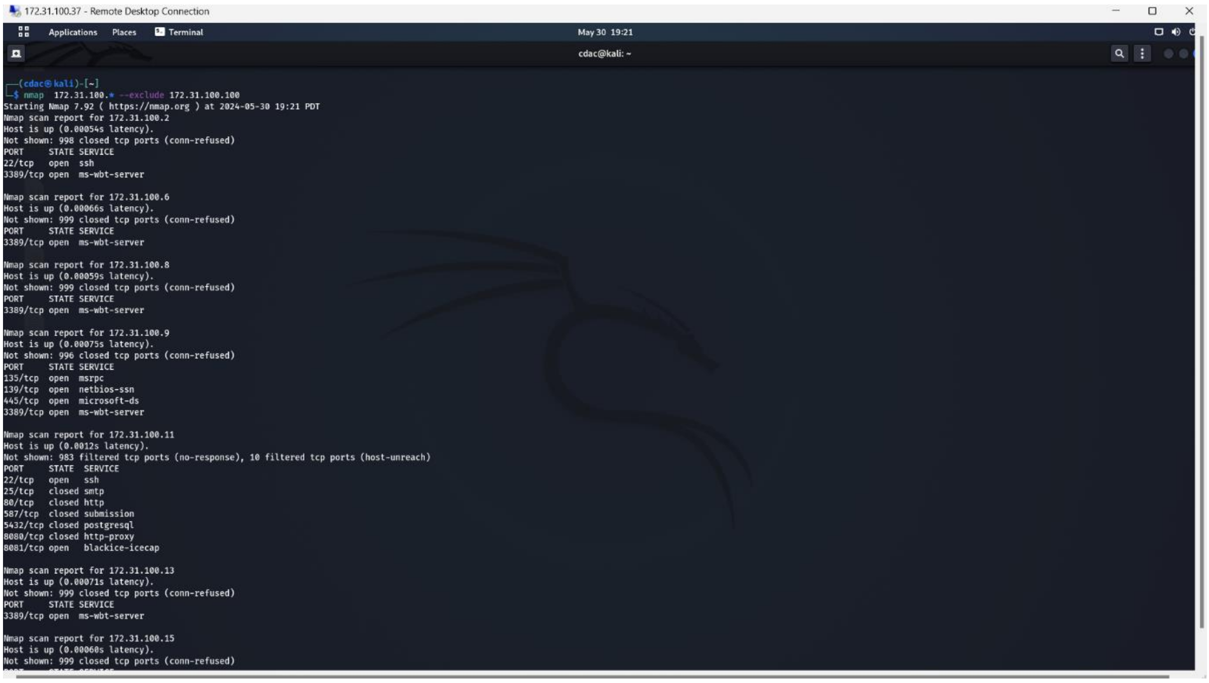


```
┌──(cdac㉿kali)-[~]
└─$ nmap  172.31.100.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2024-05-30 19:10 PDT
Nmap scan report for 172.31.100.2
Host is up (0.00040s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT     STATE SERVICE
22/tcp   open  ssh
3389/tcp open  ms-wbt-server

Nmap scan report for 172.31.100.6
Host is up (0.00041s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT     STATE SERVICE
3389/tcp open  ms-wbt-server

Nmap scan report for 172.31.100.8
Host is up (0.00038s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT     STATE SERVICE
3389/tcp open  ms-wbt-server

Nmap scan report for 172.31.100.9
Host is up (0.00047s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server

Nmap scan report for 172.31.100.11
Host is up (0.00073s latency).
Not shown: 983 filtered tcp ports (no-response), 10 filtered tcp ports (host-unreach)
PORT     STATE  SERVICE
22/tcp   open   ssh
25/tcp   closed smtp
80/tcp   closed http
587/tcp  closed submission
5432/tcp closed postgresql
8080/tcp closed http-proxy
8081/tcp open   blackice-icecap

Nmap scan report for 172.31.100.13
Host is up (0.00060s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT     STATE SERVICE
3389/tcp open  ms-wbt-server

Nmap scan report for 172.31.100.15
Host is up (0.00040s latency).
Not shown: 999 closed tcp ports (conn-refused)
```

5.Exlusion of particular ip address

$ nmap   172.31.100.0/24 --exclude <ip address>

- If we want to exclude some ip address froma range of ip addresses then we use --exclude flag for that

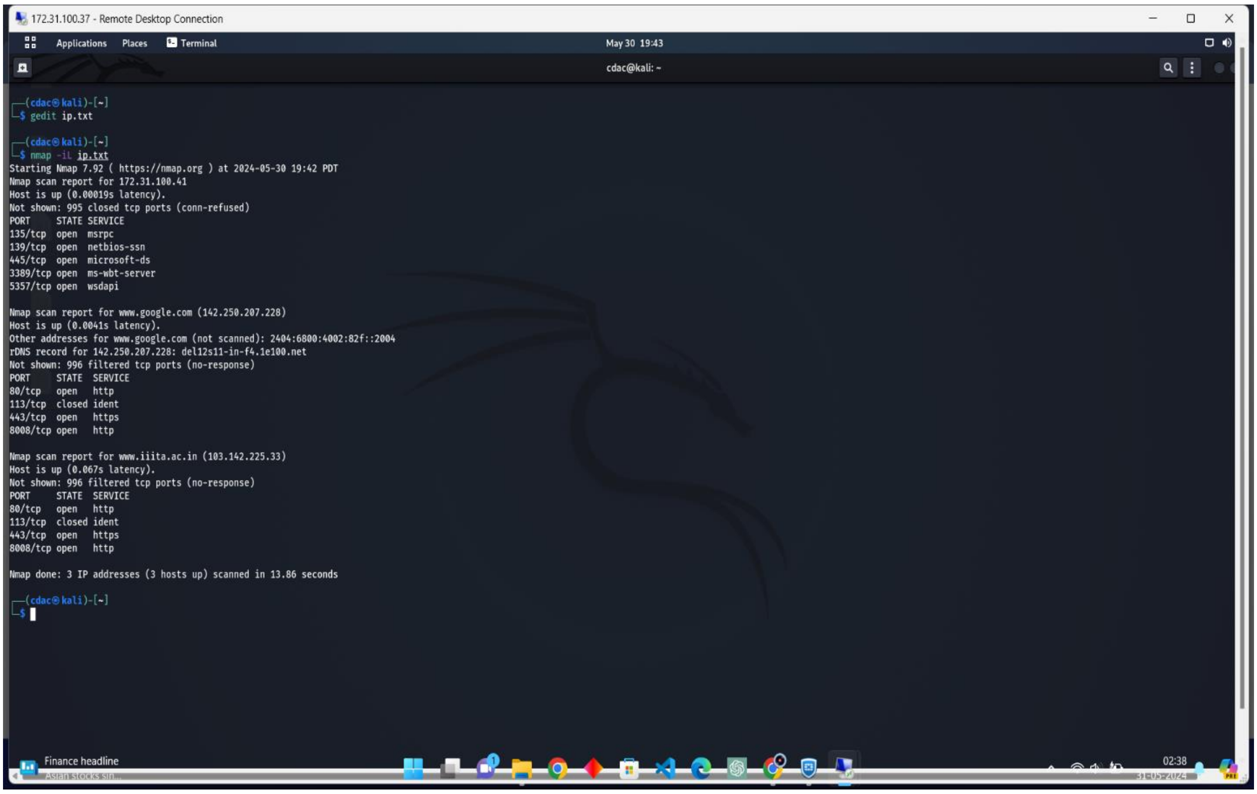


```
┌──(cdac㉿kali)-[~]
└─$ nmap  172.31.100.* --exclude 172.31.100.100
Starting Nmap 7.92 ( https://nmap.org ) at 2024-05-30 19:21 PDT
Nmap scan report for 172.31.100.2
Host is up (0.00054s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT     STATE SERVICE
22/tcp   open  ssh
3389/tcp open  ms-wbt-server

Nmap scan report for 172.31.100.6
Host is up (0.00066s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT     STATE SERVICE
3389/tcp open  ms-wbt-server

Nmap scan report for 172.31.100.8
Host is up (0.00059s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT     STATE SERVICE
3389/tcp open  ms-wbt-server

Nmap scan report for 172.31.100.9
Host is up (0.00075s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server

Nmap scan report for 172.31.100.11
Host is up (0.0012s latency).
Not shown: 983 filtered tcp ports (no-response), 10 filtered tcp ports (host-unreach)
PORT     STATE  SERVICE
22/tcp   open   ssh
25/tcp   closed smtp
80/tcp   closed http
587/tcp  closed submission
5432/tcp closed postgresql
8080/tcp closed http-proxy
8081/tcp open   blackice-icecap

Nmap scan report for 172.31.100.13
Host is up (0.00071s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT     STATE SERVICE
3389/tcp open  ms-wbt-server

Nmap scan report for 172.31.100.15
Host is up (0.00060s latency).
Not shown: 999 closed tcp ports (conn-refused)
```

6. Scanning of ip from file

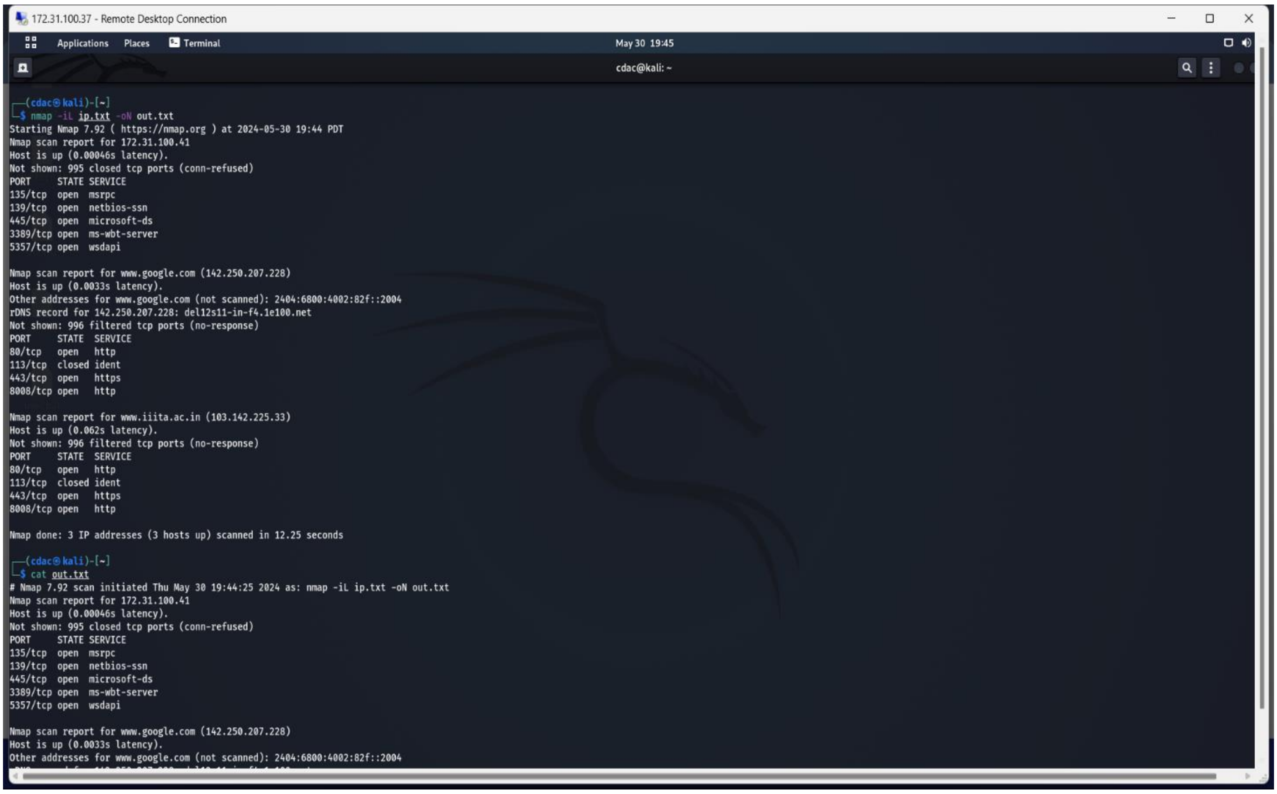
$ nmap -iL <input file>

- Given a input of ip addresses in a file we can read file and scan the given ip by using -iL flag



```
┌──(cdac㉿kali)-[~]
└─$ gedit ip.txt

┌──(cdac㉿kali)-[~]
└─$ nmap -iL ip.txt
Starting Nmap 7.92 ( https://nmap.org ) at 2024-05-30 19:42 PDT
Nmap scan report for 172.31.100.41
Host is up (0.00019s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
5357/tcp open  wsdapi

Nmap scan report for www.google.com (142.250.207.228)
Host is up (0.0041s latency).
Other addresses for www.google.com (not scanned): 2404:6800:4002:82f::2004
rDNS record for 142.250.207.228: del12s11-in-f4.1e100.net
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE  SERVICE
80/tcp   open   http
113/tcp  closed ident
443/tcp  open   https
8008/tcp open   http

Nmap scan report for www.iiita.ac.in (103.142.225.33)
Host is up (0.067s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE  SERVICE
80/tcp   open   http
113/tcp  closed ident
443/tcp  open   https
8008/tcp open   http

Nmap done: 3 IP addresses (3 hosts up) scanned in 13.86 seconds

┌──(cdac㉿kali)-[~]
└─$ 
```

- Soring the output of command
  $ nmap -iL <input file> -oN <output file>
  We can store the output of command in a file using a flag -oN

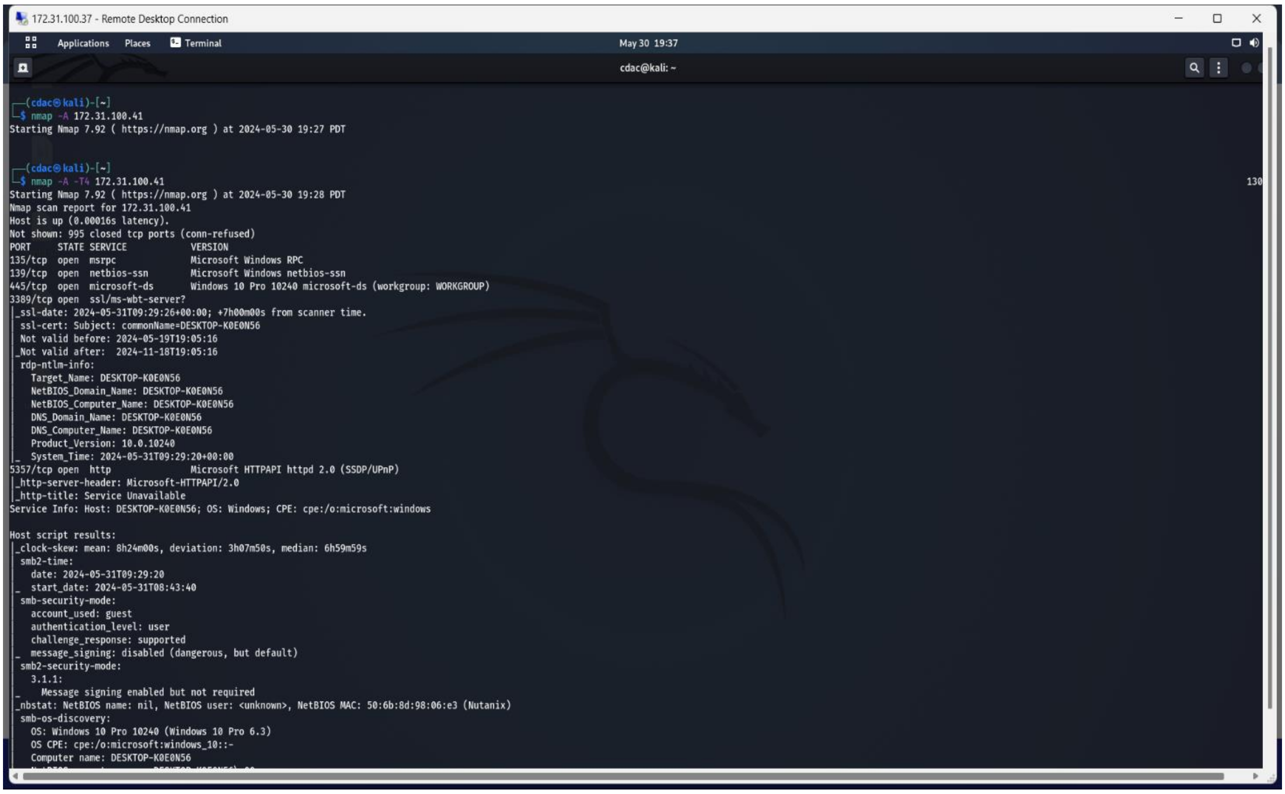


```
┌──(cdac㉿kali)-[~]
└─$ nmap -iL ip.txt -oN out.txt
Starting Nmap 7.92 ( https://nmap.org ) at 2024-05-30 19:44 PDT
Nmap scan report for 172.31.100.41
Host is up (0.00046s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
5357/tcp open  wsdapi

Nmap scan report for www.google.com (142.250.207.228)
Host is up (0.0033s latency).
Other addresses for www.google.com (not scanned): 2404:6800:4002:82f::2004
rDNS record for 142.250.207.228: del12s11-in-f4.1e100.net
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE  SERVICE
80/tcp   open   http
113/tcp  closed ident
443/tcp  open   https
8008/tcp open   http

Nmap scan report for www.iiita.ac.in (103.142.225.33)
Host is up (0.062s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE  SERVICE
80/tcp   open   http
113/tcp  closed ident
443/tcp  open   https
8008/tcp open   http

Nmap done: 3 IP addresses (3 hosts up) scanned in 12.25 seconds

┌──(cdac㉿kali)-[~]
└─$ cat out.txt
# Nmap 7.92 scan initiated Thu May 30 19:44:25 2024 as: nmap -iL ip.txt -oN out.txt
Nmap scan report for 172.31.100.41
Host is up (0.00046s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
5357/tcp open  wsdapi

Nmap scan report for www.google.com (142.250.207.228)
Host is up (0.0033s latency).
Other addresses for www.google.com (not scanned): 2404:6800:4002:82f::2004
```

7.OS detection

$ nmap -A -T4 <target ip>

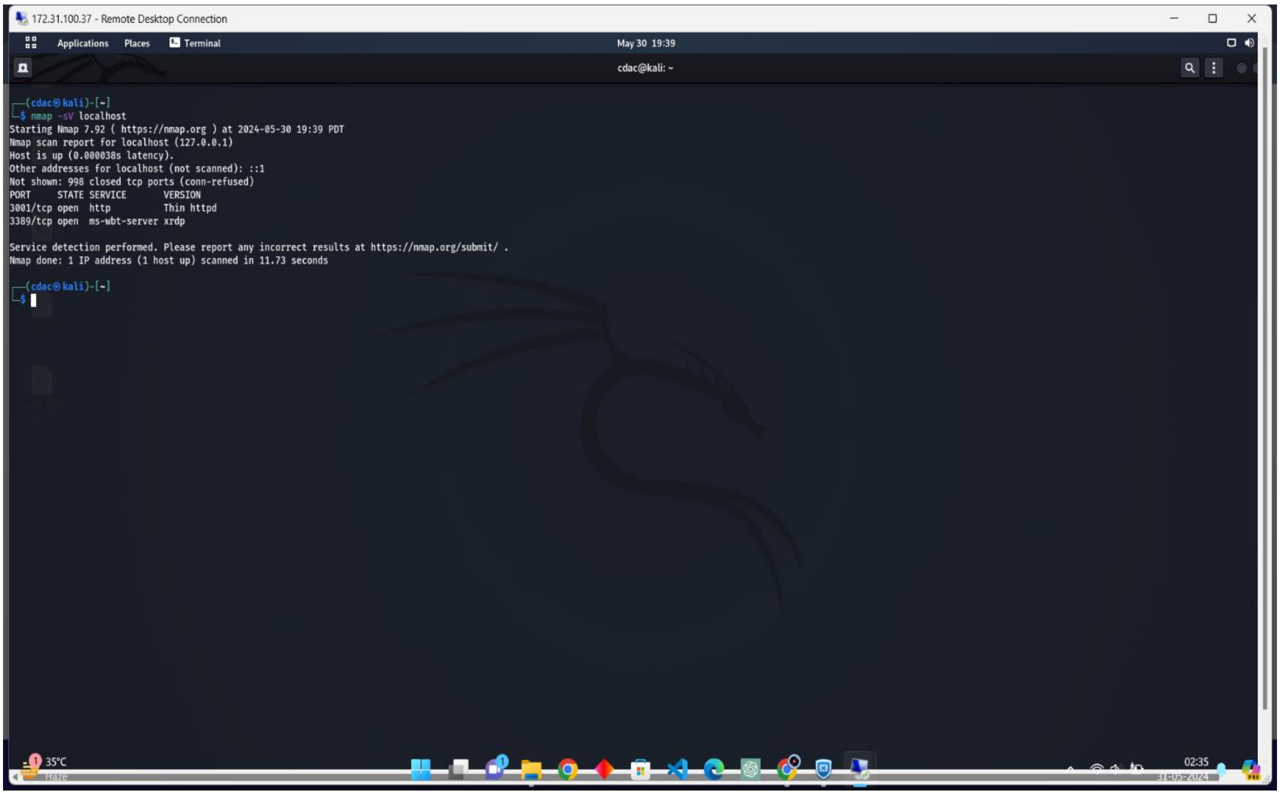
- Using -A flag and -T4 for faster execution



```
┌──(cdac㉿kali)-[~]
└─$ nmap -A 172.31.100.41
Starting Nmap 7.92 ( https://nmap.org ) at 2024-05-30 19:27 PDT


┌──(cdac㉿kali)-[~]
└─$ nmap -A -T4 172.31.100.41                                                130
Starting Nmap 7.92 ( https://nmap.org ) at 2024-05-30 19:28 PDT
Nmap scan report for 172.31.100.41
Host is up (0.00016s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT     STATE SERVICE            VERSION
135/tcp  open  msrpc              Microsoft Windows RPC
139/tcp  open  netbios-ssn        Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds       Windows 10 Pro 10240 microsoft-ds (workgroup: WORKGROUP)
3389/tcp open  ssl/ms-wbt-server?
|_ssl-date: 2024-05-31T09:29:26+00:00; +7h00m00s from scanner time.
| ssl-cert: Subject: commonName=DESKTOP-K0E0N56
| Not valid before: 2024-05-19T19:05:16
|_Not valid after:  2024-11-18T19:05:16
| rdp-ntlm-info:
|   Target_Name: DESKTOP-K0E0N56
|   NetBIOS_Domain_Name: DESKTOP-K0E0N56
|   NetBIOS_Computer_Name: DESKTOP-K0E0N56
|   DNS_Domain_Name: DESKTOP-K0E0N56
|   DNS_Computer_Name: DESKTOP-K0E0N56
|   Product_Version: 10.0.10240
|_  System_Time: 2024-05-31T09:29:20+00:00
5357/tcp open  http               Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
Service Info: Host: DESKTOP-K0E0N56; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 8h24m00s, deviation: 3h07m50s, median: 6h59m59s
| smb2-time:
|   date: 2024-05-31T09:29:20
|_  start_date: 2024-05-31T08:43:40
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
|_nbstat: NetBIOS name: nil, NetBIOS user: <unknown>, NetBIOS MAC: 50:6b:8d:98:06:e3 (Nutanix)
| smb-os-discovery:
|   OS: Windows 10 Pro 10240 (Windows 10 Pro 6.3)
|   OS CPE: cpe:/o:microsoft:windows_10::-
|   Computer name: DESKTOP-K0E0N56
```

8.Scanning version of services running on target ip

- $ nmap -sV <target ip>



```
┌──(cdac㉿kali)-[~]
└─$ nmap -sV localhost
Starting Nmap 7.92 ( https://nmap.org ) at 2024-05-30 19:39 PDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000038s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 998 closed tcp ports (conn-refused)
PORT     STATE SERVICE       VERSION
3001/tcp open  http          Thin httpd
3389/tcp open  ms-wbt-server xrdp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.73 seconds

┌──(cdac㉿kali)-[~]
└─$ 
```

9.Scanning foe TCP or UDP services only

- $ nmap -sT <target ip>
  By flag -sT it will return the ports which are running on TCP protocol

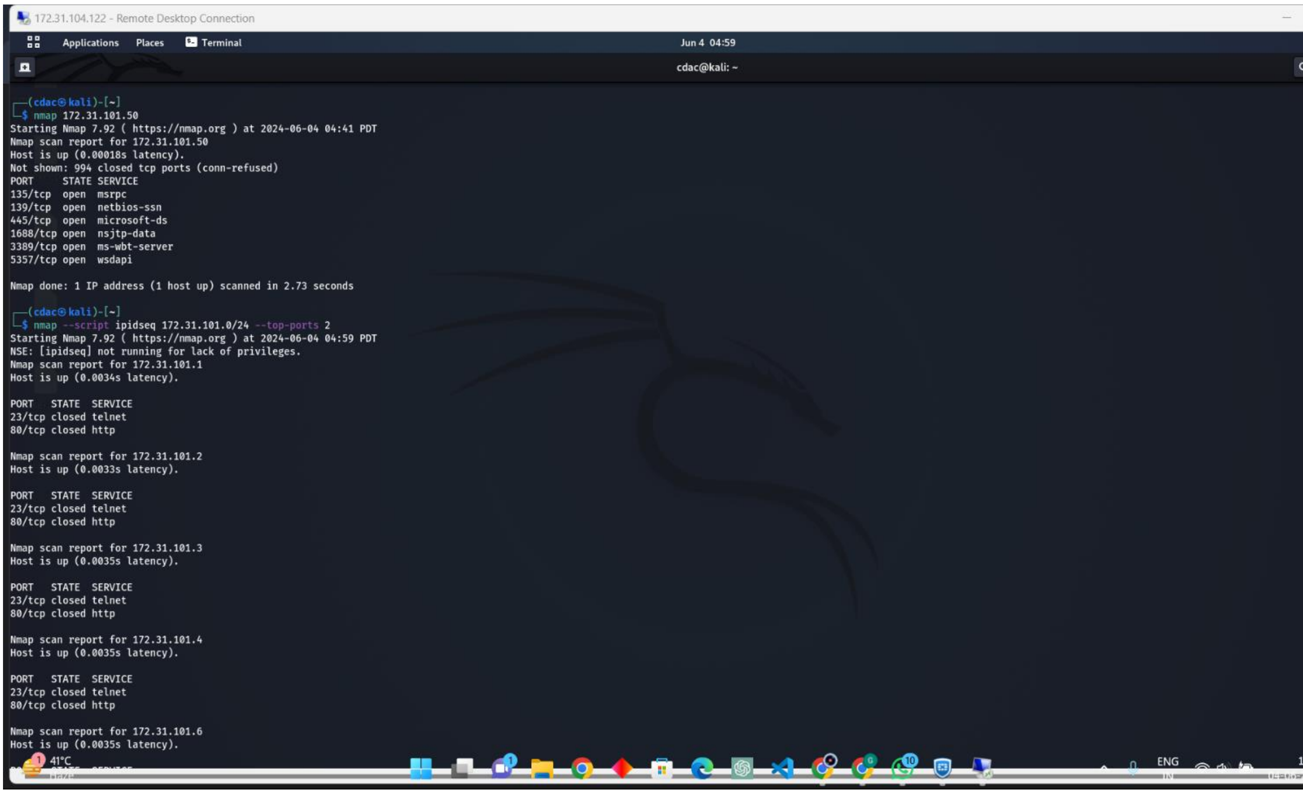
- $ nmap -sU <target ip>
  By flag -sU it will return the ports which are running on UDP protocol

10. Scan live host on network

- $ nmap -sP <network address>

11. Zombie Scanning

- For scanning the ip which support incremental IPID(IP identification) We use script –ipidseq to see which ip addresses support incremental ipid so that we can perform zombie scanning .
  $ nmap –script ipidseq <ip range>



```
┌──(cdac㉿kali)-[~]
└─$ nmap 172.31.101.50
Starting Nmap 7.92 ( https://nmap.org ) at 2024-06-04 04:41 PDT
Nmap scan report for 172.31.101.50
Host is up (0.00018s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1688/tcp open  nsjtp-data
3389/tcp open  ms-wbt-server
5357/tcp open  wsdapi

Nmap done: 1 IP address (1 host up) scanned in 2.73 seconds

┌──(cdac㉿kali)-[~]
└─$ nmap --script ipidseq 172.31.101.0/24 --top-ports 2
Starting Nmap 7.92 ( https://nmap.org ) at 2024-06-04 04:59 PDT
NSE: [ipidseq] not running for lack of privileges.
Nmap scan report for 172.31.101.1
Host is up (0.0034s latency).

PORT   STATE  SERVICE
23/tcp closed telnet
80/tcp closed http

Nmap scan report for 172.31.101.2
Host is up (0.0033s latency).

PORT   STATE  SERVICE
23/tcp closed telnet
80/tcp closed http

Nmap scan report for 172.31.101.3
Host is up (0.0035s latency).

PORT   STATE  SERVICE
23/tcp closed telnet
80/tcp closed http

Nmap scan report for 172.31.101.4
Host is up (0.0035s latency).

PORT   STATE  SERVICE
23/tcp closed telnet
80/tcp closed http

Nmap scan report for 172.31.101.6
Host is up (0.0035s latency).
```

- Then after getting ip address we can perform zombie scanning

  $ nmap -Pn -sI <zombie host> <target ip>

12. Firewall detection

$ nmap -sA <taget ip>

- This command return filtered if firewall detected and unfiltered if no firewall detected .

13. Bypassing Firewall

$ nmap -mtu 8 <target ip>

- This command contain mtu flag (maximum transmission unit) of multiple of 8 like 8 , 16 ,24

14. Evading Firewall

$ nmap -sS <target ip>

- This command evade firewall while scanning the targeted network or host .