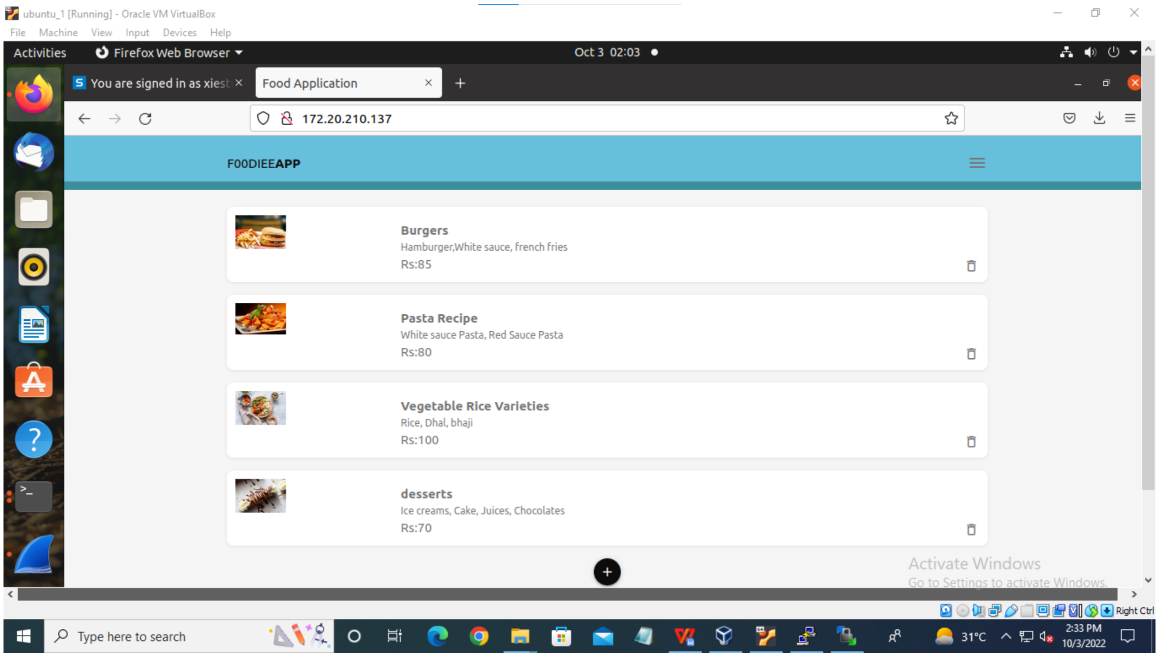
1)

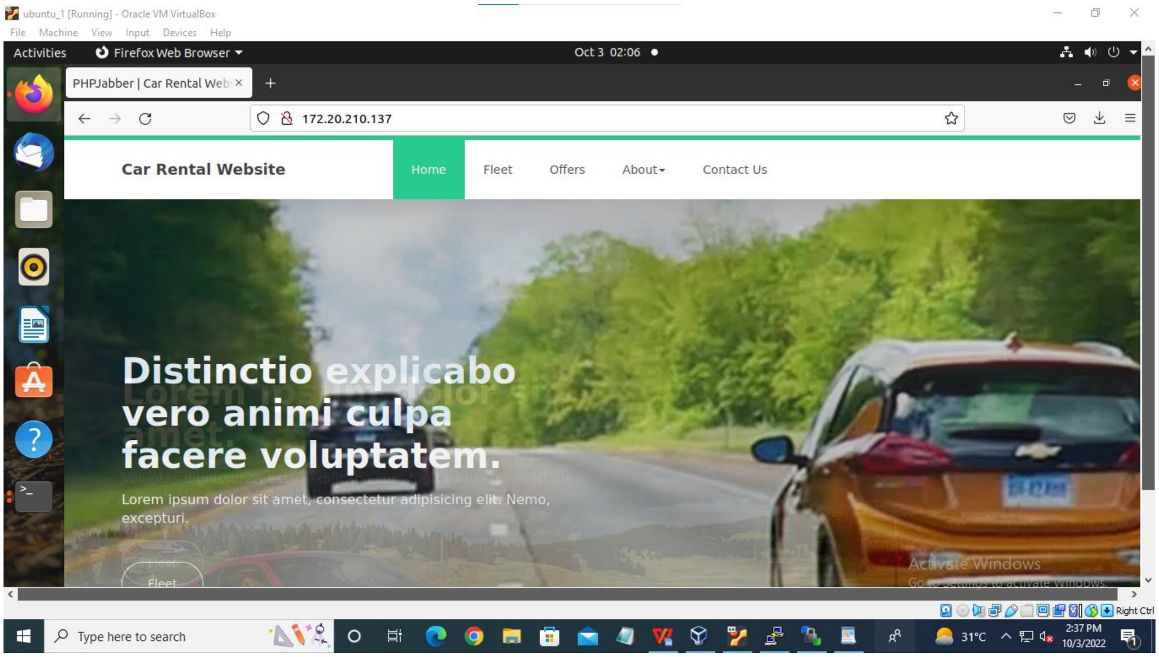


Burgers
Hamburger,White sauce, french fries
Rs:85

Pasta Recipe
White sauce Pasta, Red Sauce Pasta
Rs:80

Vegetable Rice Varieties
Rice, Dhal, bhaji
Rs:100

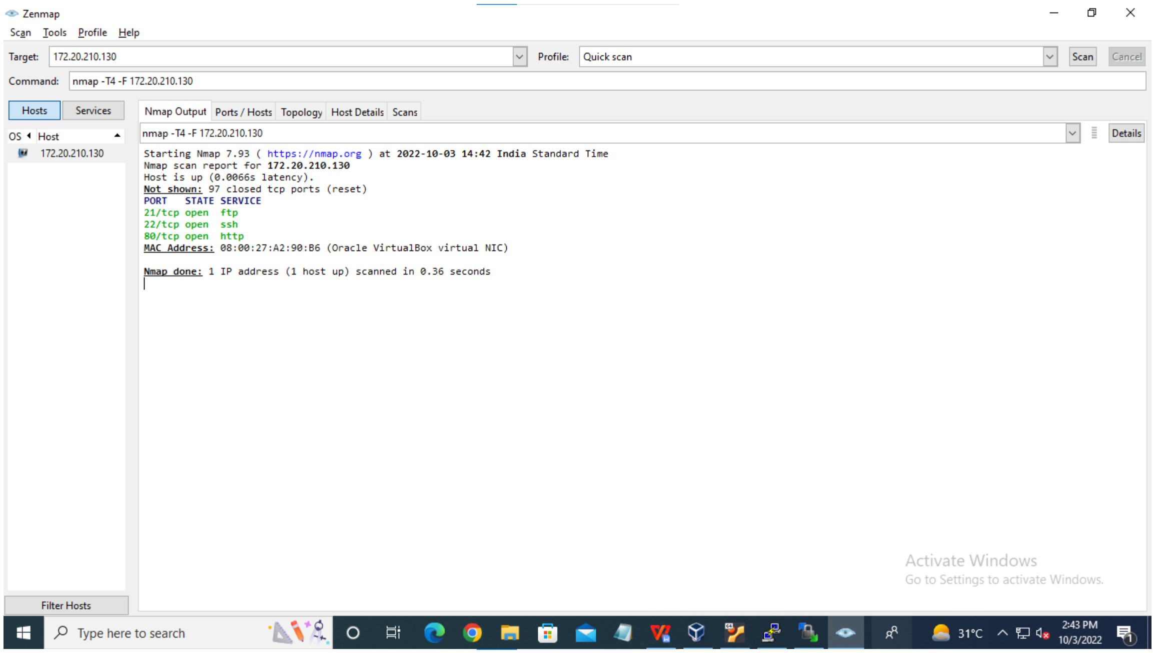
desserts
Ice creams, Cake, Juices, Chocolates
Rs:70



Distinctio explicabo vero animi culpa facere voluptatem.

Lorem ipsum dolor sit amet, consectetur adipisicing elit. Nemo, excepturi.

2 B)

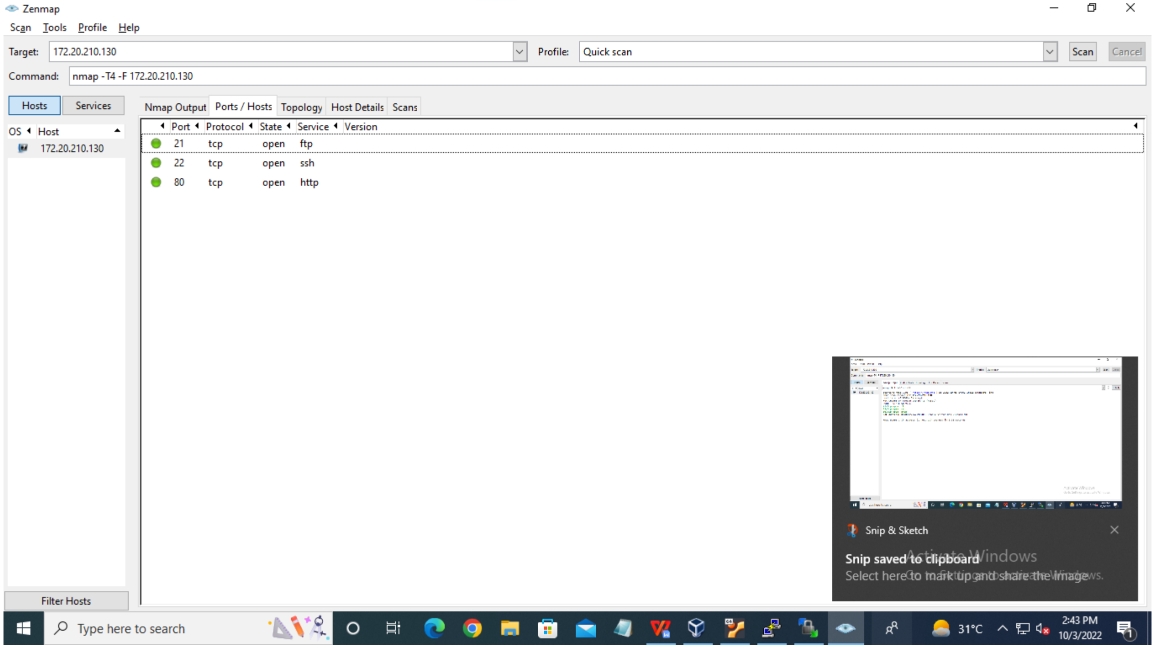


Target: 172.20.210.130

Profile: Quick scan

Command: nmap -T4 -F 172.20.210.130

```
Starting Nmap 7.93 ( https://nmap.org ) at 2022-10-03 14:42 India Standard Time
Nmap scan report for 172.20.210.130
Host is up (0.0066s latency).
Not shown: 97 closed tcp ports (reset)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:A2:90:B6 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.36 seconds
```



Target: 172.20.210.130

Profile: Quick scan

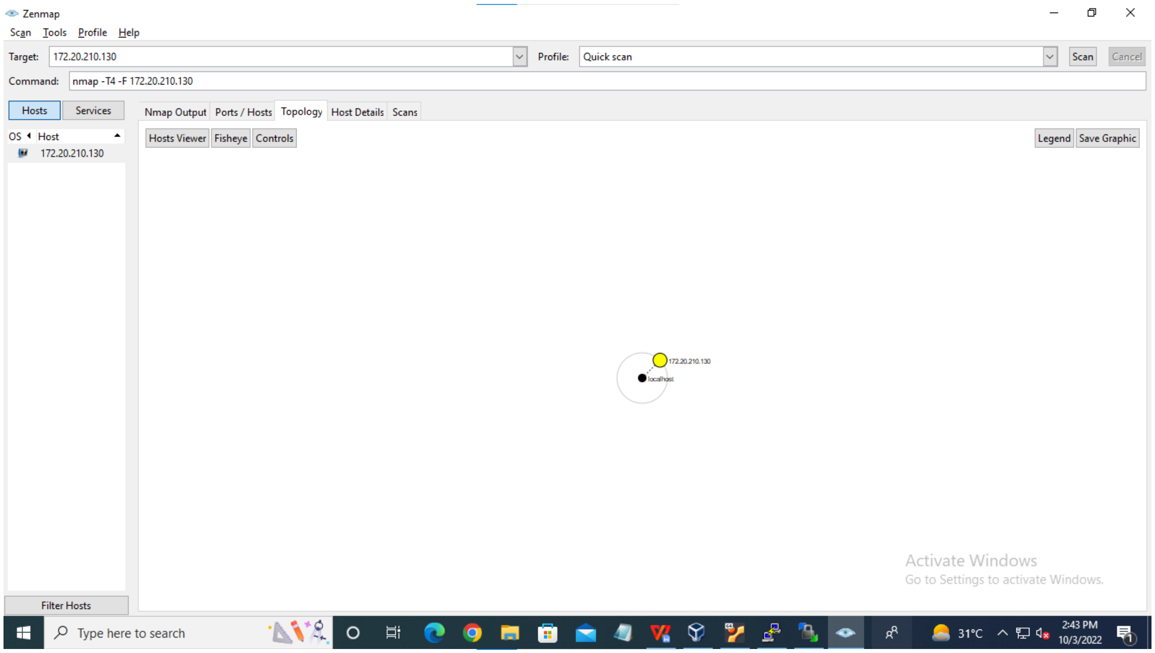
Command: nmap -T4 -F 172.20.210.130

Host: 172.20.210.130

Port	Protocol	State	Service	Version
21	tcp	open	ftp	
22	tcp	open	ssh	
80	tcp	open	http	

Snip saved to clipboard

Select here to mark up and share the image

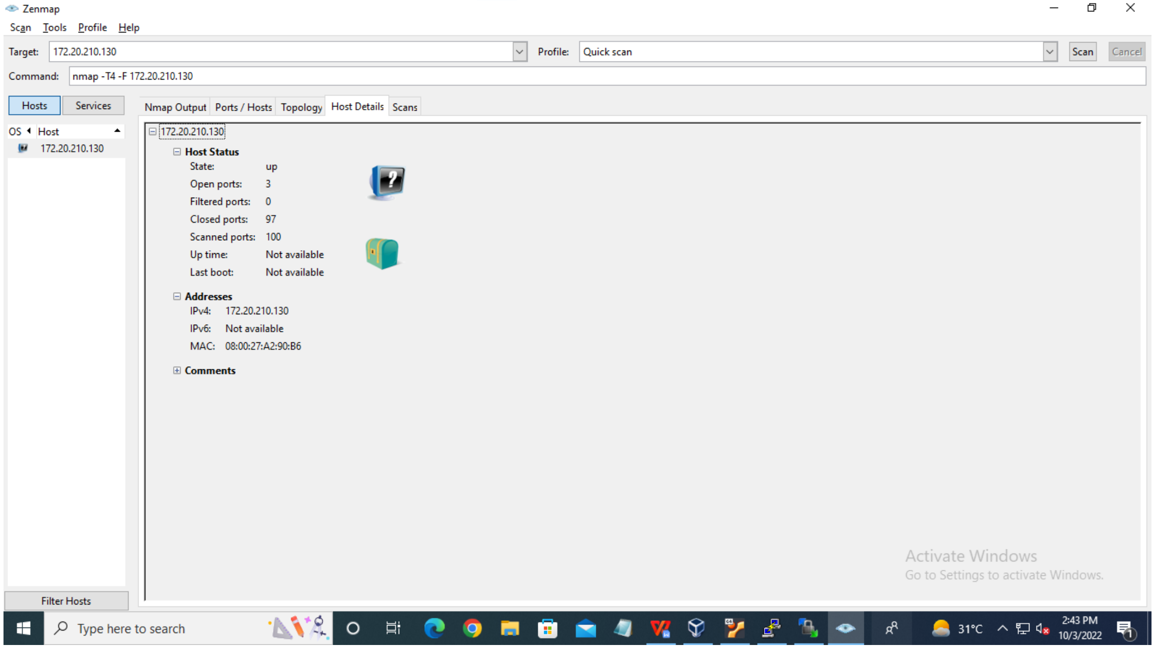


Target: 172.20.210.130

Profile: Quick scan

Command: nmap -T4 -F 172.20.210.130

172.20.210.130



Target: 172.20.210.130

Profile: Quick scan

Command: nmap -T4 -F 172.20.210.130

172.20.210.130

172.20.210.130

Host Status

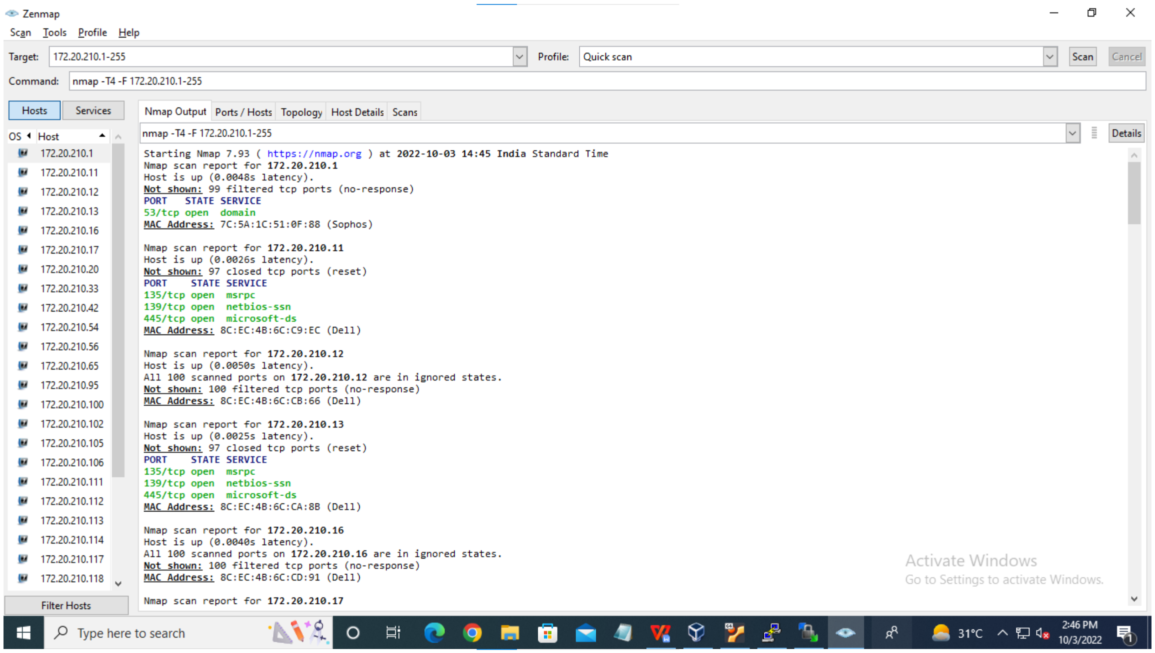
State:	up
Open ports:	3
Filtered ports:	0
Closed ports:	97
Scanned ports:	100
Up time:	Not available
Last boot:	Not available

Addresses

IPv4:	172.20.210.130
IPv6:	Not available
MAC:	08:00:27:A2:90:B6

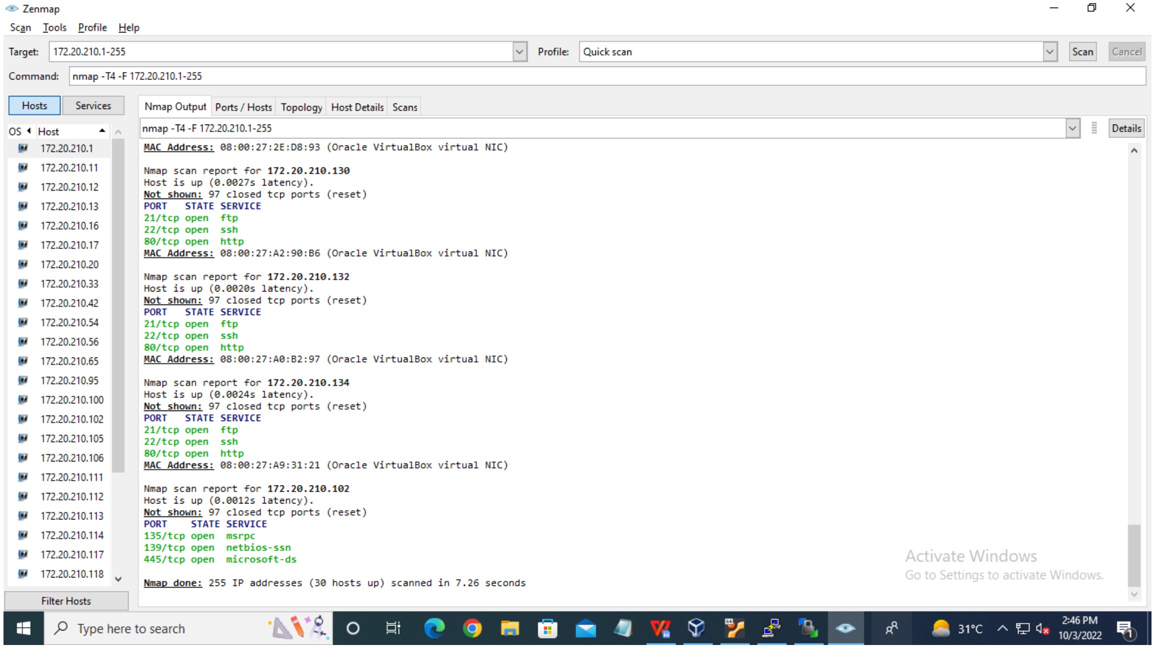
Comments

WHOLE NETWORK :-



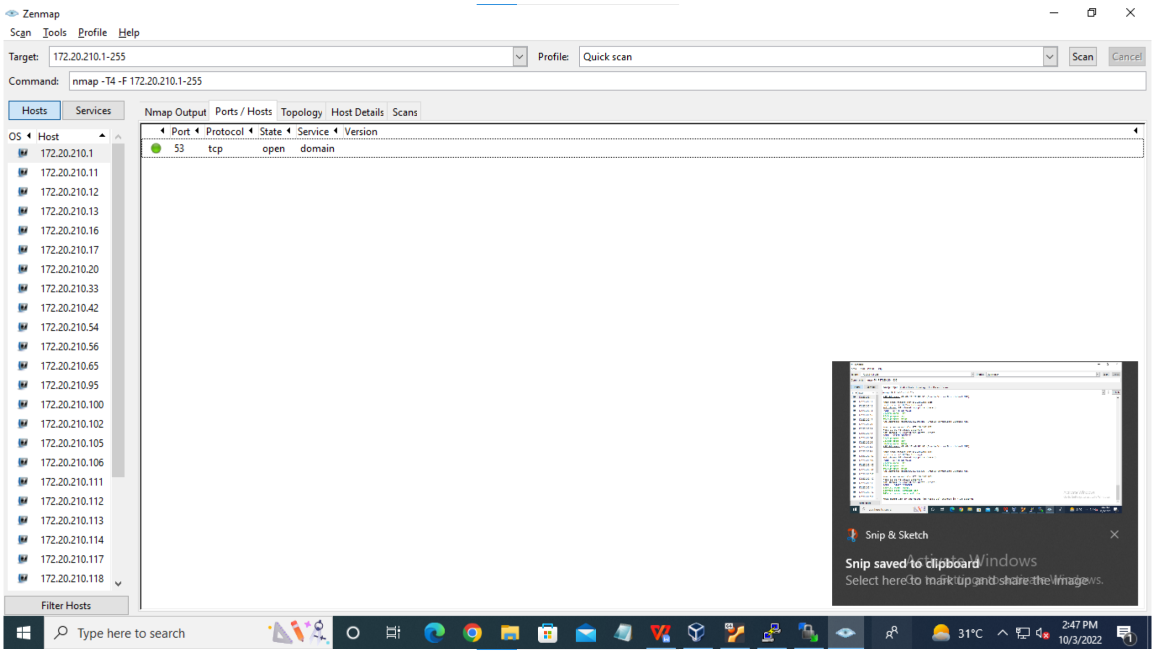
Target: 172.20.210.1-255
Profile: Quick scan
Command: nmap -T4 -F 172.20.210.1-255

```
nmap -T4 -F 172.20.210.1-255
Starting Nmap 7.93 ( https://nmap.org ) at 2022-10-03 14:45 India Standard Time
Nmap scan report for 172.20.210.1
Host is up (0.0048s latency).
Not shown: 99 filtered tcp ports (no-response)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 7C:5A:1C:51:0F:88 (Sophos)

Nmap scan report for 172.20.210.11
Host is up (0.0026s latency).
Not shown: 97 closed tcp ports (reset)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 8C:EC:4B:6C:C9:EC (Dell)

Nmap scan report for 172.20.210.12
Host is up (0.0050s latency).
All 100 scanned ports on 172.20.210.12 are in ignored states.
Not shown: 100 filtered tcp ports (no-response)
MAC Address: 8C:EC:4B:6C:CB:66 (Dell)

Nmap scan report for 172.20.210.13
Host is up (0.0025s latency).
Not shown: 97 closed tcp ports (reset)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 8C:EC:4B:6C:CA:8B (Dell)

Nmap scan report for 172.20.210.16
Host is up (0.0040s latency).
All 100 scanned ports on 172.20.210.16 are in ignored states.
Not shown: 100 filtered tcp ports (no-response)
MAC Address: 8C:EC:4B:6C:CD:91 (Dell)

Nmap scan report for 172.20.210.17
```



Target: 172.20.210.1-255
Profile: Quick scan
Command: nmap -T4 -F 172.20.210.1-255

```
nmap -T4 -F 172.20.210.1-255
MAC Address: 08:00:27:2E:D8:93 (Oracle VirtualBox virtual NIC)

Nmap scan report for 172.20.210.130
Host is up (0.0027s latency).
Not shown: 97 closed tcp ports (reset)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:A2:90:B6 (Oracle VirtualBox virtual NIC)

Nmap scan report for 172.20.210.132
Host is up (0.0020s latency).
Not shown: 97 closed tcp ports (reset)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:A0:B2:97 (Oracle VirtualBox virtual NIC)

Nmap scan report for 172.20.210.134
Host is up (0.0024s latency).
Not shown: 97 closed tcp ports (reset)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:A9:31:21 (Oracle VirtualBox virtual NIC)

Nmap scan report for 172.20.210.102
Host is up (0.0012s latency).
Not shown: 97 closed tcp ports (reset)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 255 IP addresses (30 hosts up) scanned in 7.26 seconds
```



Target: 172.20.210.1-255

Profile: Quick scan

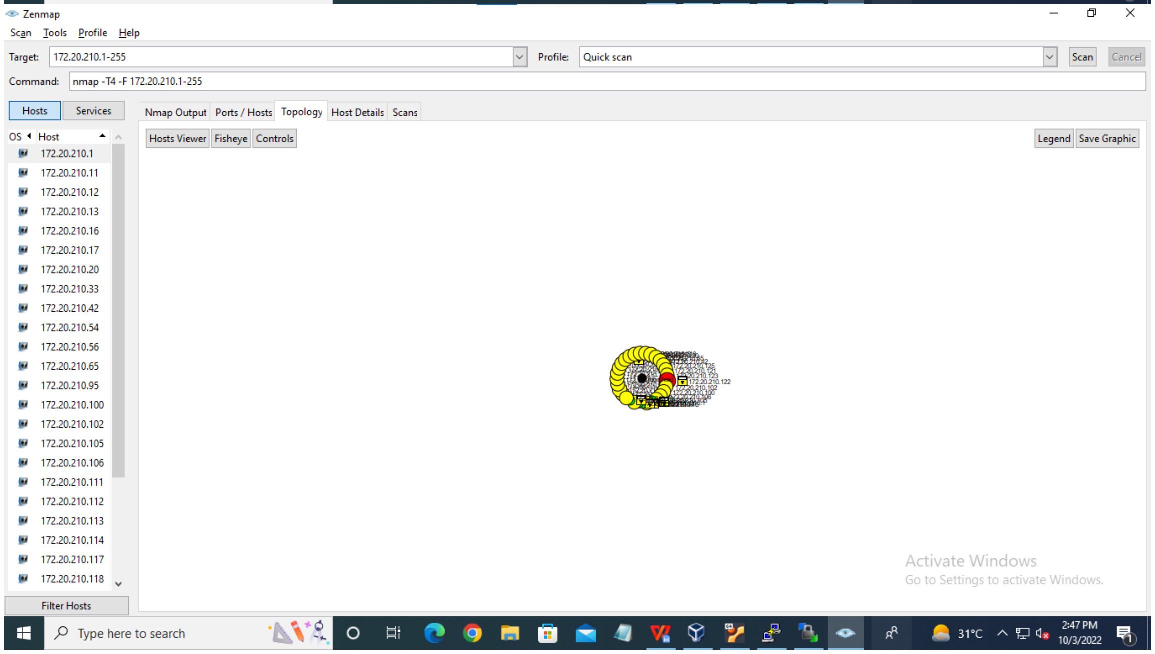
Command: nmap -T4 -F 172.20.210.1-255

Port	Protocol	State	Service	Version
53	tcp	open	domain	

```
OS  Host
    172.20.210.1
    172.20.210.11
    172.20.210.12
    172.20.210.13
    172.20.210.16
    172.20.210.17
    172.20.210.20
    172.20.210.33
    172.20.210.42
    172.20.210.54
    172.20.210.56
    172.20.210.65
    172.20.210.95
    172.20.210.100
    172.20.210.102
    172.20.210.105
    172.20.210.106
    172.20.210.111
    172.20.210.112
    172.20.210.113
    172.20.210.114
    172.20.210.117
    172.20.210.118
```

Snip saved to clipboard

Select here to mark up and share the image.



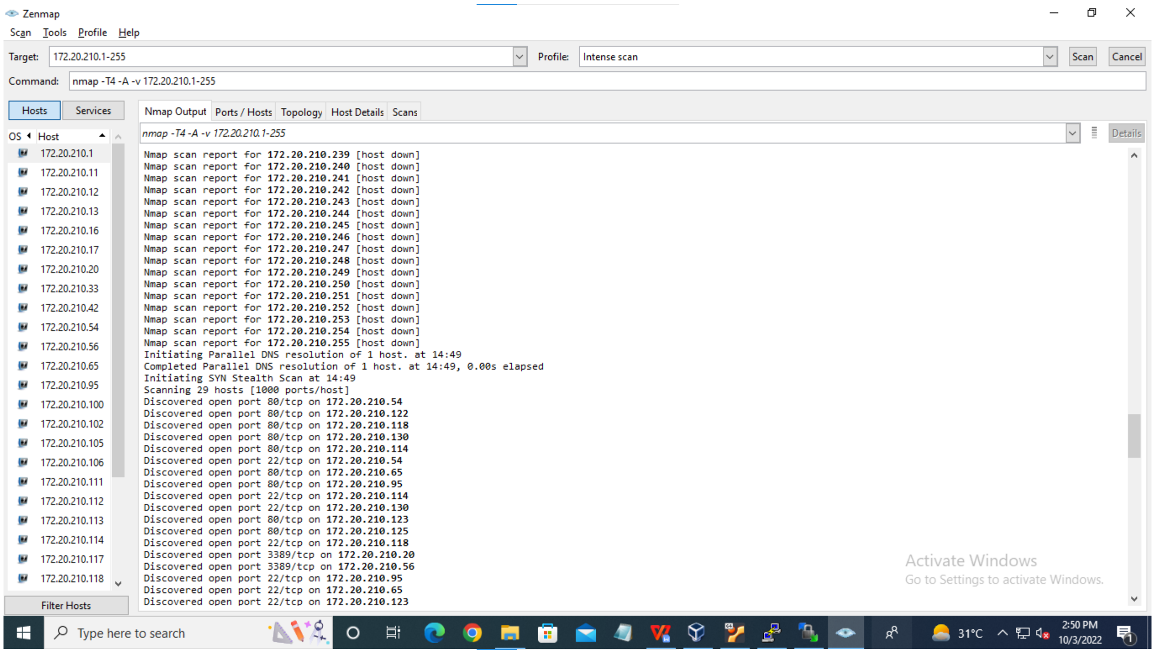
Target: 172.20.210.1-255

Profile: Quick scan

Command: nmap -T4 -F 172.20.210.1-255

```
OS  Host
    172.20.210.1
    172.20.210.11
    172.20.210.12
    172.20.210.13
    172.20.210.16
    172.20.210.17
    172.20.210.20
    172.20.210.33
    172.20.210.42
    172.20.210.54
    172.20.210.56
    172.20.210.65
    172.20.210.95
    172.20.210.100
    172.20.210.102
    172.20.210.105
    172.20.210.106
    172.20.210.111
    172.20.210.112
    172.20.210.113
    172.20.210.114
    172.20.210.117
    172.20.210.118
```

INTENSE SCAN FOR WHOLE NETWORK :-

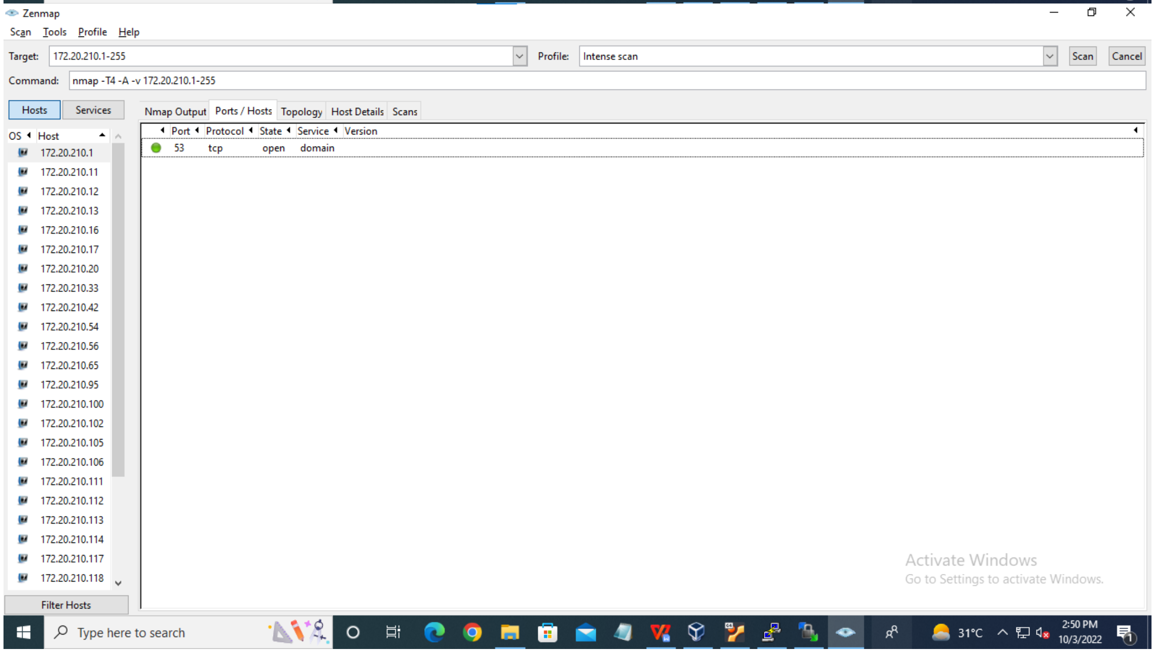


Target: 172.20.210.1-255
Profile: Intense scan
Command: nmap -T4 -A -v 172.20.210.1-255

```
172.20.210.1
172.20.210.11
172.20.210.12
172.20.210.13
172.20.210.16
172.20.210.17
172.20.210.20
172.20.210.33
172.20.210.42
172.20.210.54
172.20.210.56
172.20.210.65
172.20.210.95
172.20.210.100
172.20.210.102
172.20.210.105
172.20.210.106
172.20.210.111
172.20.210.112
172.20.210.113
172.20.210.114
172.20.210.117
172.20.210.118
```

nmap -T4 -A -v 172.20.210.1-255

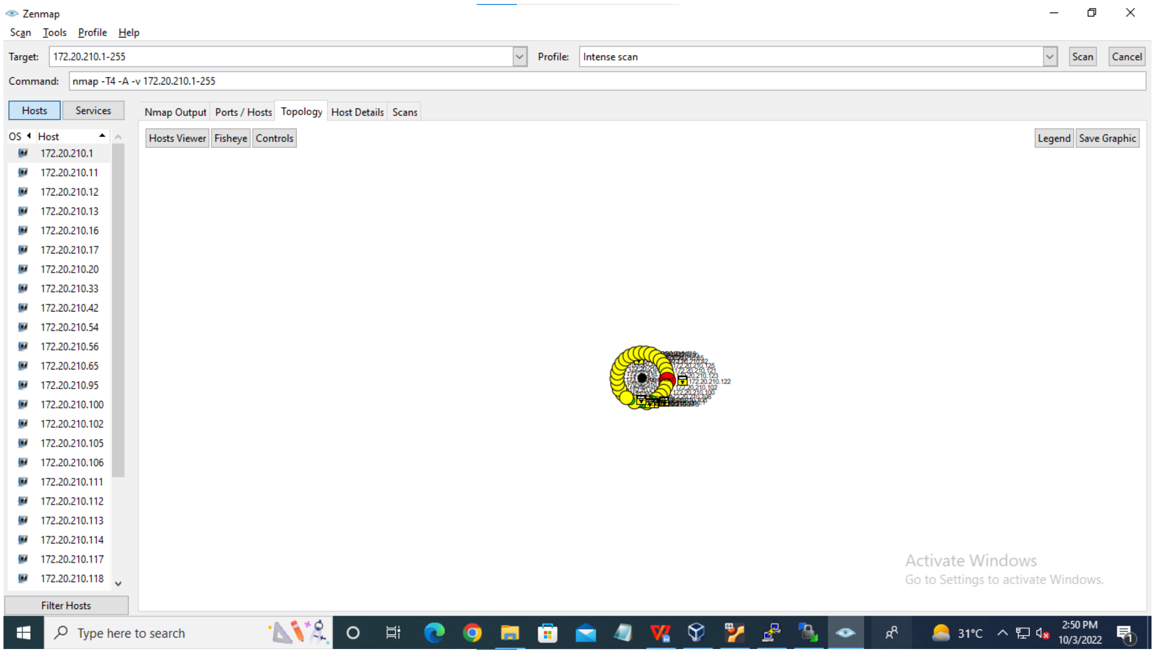
```
Nmap scan report for 172.20.210.239 [host down]
Nmap scan report for 172.20.210.240 [host down]
Nmap scan report for 172.20.210.241 [host down]
Nmap scan report for 172.20.210.242 [host down]
Nmap scan report for 172.20.210.243 [host down]
Nmap scan report for 172.20.210.244 [host down]
Nmap scan report for 172.20.210.245 [host down]
Nmap scan report for 172.20.210.246 [host down]
Nmap scan report for 172.20.210.247 [host down]
Nmap scan report for 172.20.210.248 [host down]
Nmap scan report for 172.20.210.249 [host down]
Nmap scan report for 172.20.210.250 [host down]
Nmap scan report for 172.20.210.251 [host down]
Nmap scan report for 172.20.210.252 [host down]
Nmap scan report for 172.20.210.253 [host down]
Nmap scan report for 172.20.210.254 [host down]
Nmap scan report for 172.20.210.255 [host down]
Initiating Parallel DNS resolution of 1 host. at 14:49
Completed Parallel DNS resolution of 1 host. at 14:49, 0.00s elapsed
Initiating SYN Stealth Scan at 14:49
Scanning 29 hosts [1000 ports/host]
Discovered open port 80/tcp on 172.20.210.54
Discovered open port 80/tcp on 172.20.210.122
Discovered open port 80/tcp on 172.20.210.118
Discovered open port 80/tcp on 172.20.210.130
Discovered open port 80/tcp on 172.20.210.114
Discovered open port 22/tcp on 172.20.210.54
Discovered open port 80/tcp on 172.20.210.65
Discovered open port 80/tcp on 172.20.210.95
Discovered open port 22/tcp on 172.20.210.114
Discovered open port 22/tcp on 172.20.210.130
Discovered open port 80/tcp on 172.20.210.123
Discovered open port 80/tcp on 172.20.210.125
Discovered open port 22/tcp on 172.20.210.118
Discovered open port 3389/tcp on 172.20.210.20
Discovered open port 3389/tcp on 172.20.210.56
Discovered open port 22/tcp on 172.20.210.95
Discovered open port 22/tcp on 172.20.210.65
Discovered open port 22/tcp on 172.20.210.123
```



Target: 172.20.210.1-255
Profile: Intense scan
Command: nmap -T4 -A -v 172.20.210.1-255

```
172.20.210.1
172.20.210.11
172.20.210.12
172.20.210.13
172.20.210.16
172.20.210.17
172.20.210.20
172.20.210.33
172.20.210.42
172.20.210.54
172.20.210.56
172.20.210.65
172.20.210.95
172.20.210.100
172.20.210.102
172.20.210.105
172.20.210.106
172.20.210.111
172.20.210.112
172.20.210.113
172.20.210.114
172.20.210.117
172.20.210.118
```

	Port	Protocol	State	Service	Version
●	53	tcp	open	domain	



Zenmap

Scan Tools Profile Help

Target: 172.20.210.1-255 Profile: Intense scan Scan Cancel

Command: nmap -T4 -A -v 172.20.210.1-255

Hosts Services

Nmap Output Ports / Hosts Topology Host Details Scans

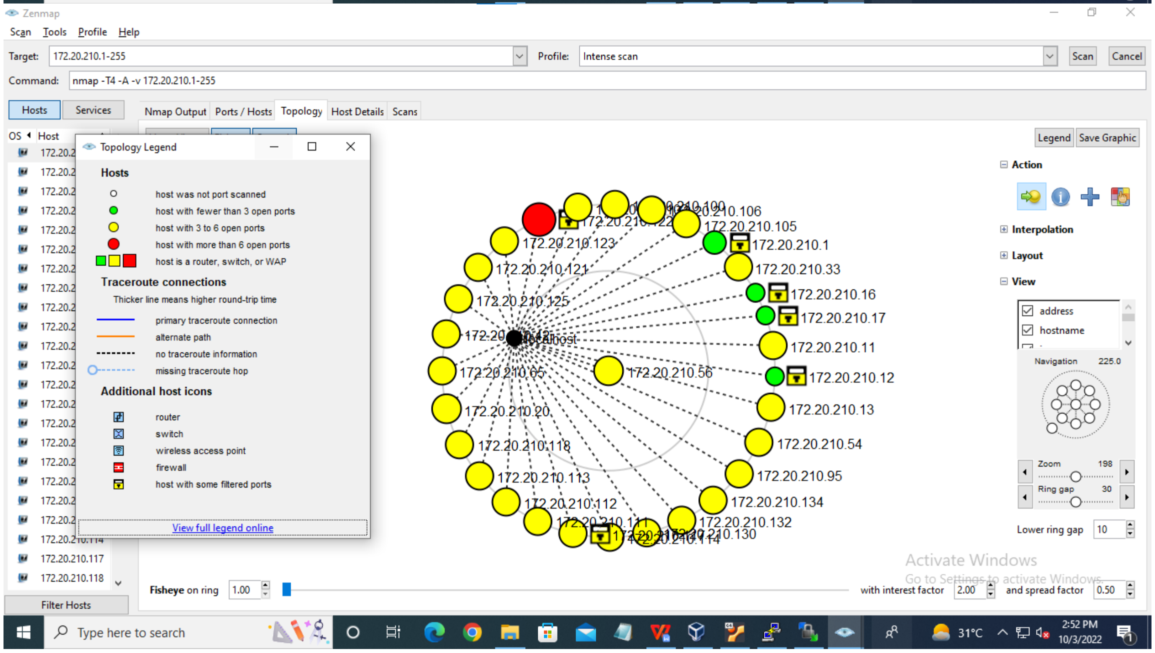
Hosts Viewer Fisheye Controls

Legend Save Graphic

OS Host

172.20.210.1
172.20.210.11
172.20.210.12
172.20.210.13
172.20.210.16
172.20.210.17
172.20.210.20
172.20.210.33
172.20.210.42
172.20.210.54
172.20.210.56
172.20.210.65
172.20.210.95
172.20.210.100
172.20.210.102
172.20.210.105
172.20.210.106
172.20.210.111
172.20.210.112
172.20.210.113
172.20.210.114
172.20.210.117
172.20.210.118

Filter Hosts



Zenmap

Scan Tools Profile Help

Target: 172.20.210.1-255 Profile: Intense scan Scan Cancel

Command: nmap -T4 -A -v 172.20.210.1-255

Hosts Services

Nmap Output Ports / Hosts Topology Host Details Scans

Legend Save Graphic

OS Host

172.20.2
172.20.2
172.20.2
172.20.2
172.20.2
172.20.2
172.20.2
172.20.2
172.20.2
172.20.2
172.20.2
172.20.2
172.20.2
172.20.2
172.20.2
172.20.2
172.20.2
172.20.2
172.20.2
172.20.2
172.20.210.114
172.20.210.117
172.20.210.118

Filter Hosts

Topology Legend

Hosts

○ host was not port scanned
🟢 host with fewer than 3 open ports
🟡 host with 3 to 6 open ports
🔴 host with more than 6 open ports
🟩🟨🟥 host is a router, switch, or WAP

Traceroute connections

Thicker line means higher round-trip time

primary traceroute connection
alternate path
no traceroute information
missing traceroute hop

Additional host icons

router
switch
wireless access point
firewall
host with some filtered ports

View full legend online

Action

Interpolation

Layout

View

☑ address
☑ hostname

Navigation 225.0

Zoom 198

Ring gap 30

Lower ring gap 10

Fisheye on ring 1.00 with interest factor 2.00 and spread factor 0.50