LAB 6

COURSE: COMPUTER NETWORK

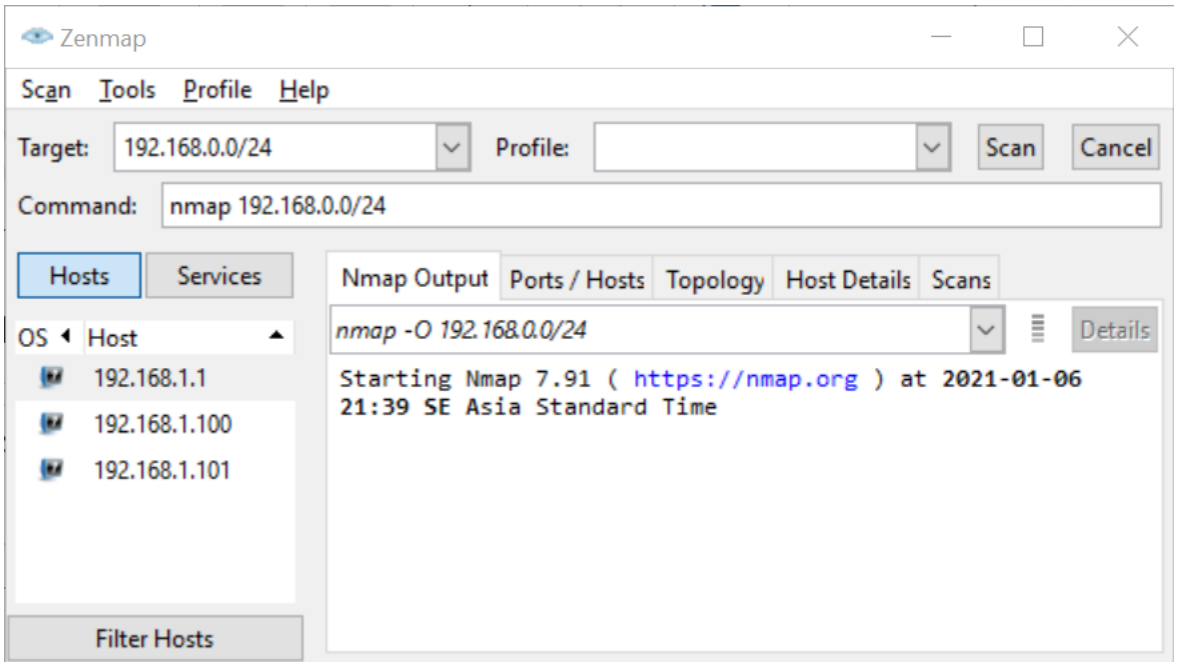
NETWORK SCANNING TOOL

Name:	ID:

Objective

Use NMAP to identify the network

NMAP is a port-scanning tool. It is designed to scan the ports of a network host and determine which ports are “open”. That is which ports have network services listening on them. Download NMAP official page and install it on your machine, you might want to install ZENMAP too, it’s a graphical tool bundled with NMAP. You need to refer to NMAP webpage documents for scanning basics www.nmap.org.



Step 1: Identify the network address that your computer is connected

192.168.251.34

Step 2: Do a scan to determine all running hosts in your network.

Choosing the Profile Quick scan

```
Nmap scan report for 192.168.251.34
Host is up (0.013s latency).
Not shown: 99 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: CE:1C:66:7A:64:D8 (Unknown)

Nmap scan report for THINKBOOK14 (192.168.251.135)
Host is up (0.22s latency).
Not shown: 99 filtered tcp ports (no-response)
PORT   STATE SERVICE
80/tcp open  http
MAC Address: E0:0A:F6:A7:D1:2F (Liteon Technology)

Nmap scan report for 192.168.251.193
Host is up (0.050s latency).
Not shown: 99 filtered tcp ports (no-response)
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 80:B6:55:2E:83:85 (Intel Corporate)

Nmap scan report for MAC-6C1F02 (192.168.251.240)
Host is up (0.026s latency).
Not shown: 99 closed tcp ports (reset)
PORT     STATE SERVICE
5000/tcp open  upnp
MAC Address: 5C:E9:1E:6C:1F:02 (Apple)

Nmap scan report for ComKkk (192.168.251.236)
Host is up (0.00035s latency).
Not shown: 96 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi
```

How many hosts are running? **4 hosts**

Please list all the IP addresses.

- **192.168.251.236**

- **192.168.251.135**
- **192.168.251.240**
- **192.168.251.193**

Step 3: Identify the operating system of all running host.

Using the command “nmap -O {network address/prefix}”.

```
Nmap scan report for 192.168.251.135
Host is up (0.00037s latency).
Not shown: 996 closed tcp ports (reset)
PORT    STATE SERVICE
80/tcp  open  http
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
Device type: general purpose
Running: Microsoft Windows 10|11
OS CPE: cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows_11
OS details: Microsoft Windows 10 1607 - 11 23H2
Network Distance: 0 hops
```

```
Nmap scan report for 192.168.251.193
Host is up (0.050s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 80:B6:55:2E:83:85 (Intel Corporate)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 11|10|2022 (92%), FreeBSD 6.X (88%)
OS CPE: cpe:/o:microsoft:windows_11 cpe:/o:freebsd:freebsd:6.2 cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows_server_2022
Aggressive OS guesses: Microsoft Windows 11 21H2 (92%), FreeBSD 6.2-RELEASE (88%), Microsoft Windows 10 (87%), Microsoft Windows Server 2022 (85%), M
icrosoft Windows 10 1607 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
```

```
Nmap scan report for 192.168.251.236
Host is up (0.00058s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi
Device type: general purpose
Running: Microsoft Windows 10|11
OS CPE: cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows_11
OS details: Microsoft Windows 10 1607 - 11 23H2
Network Distance: 0 hops
```

```
Nmap scan report for 192.168.251.240
Host is up (0.021s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE
5000/tcp open  upnp
7000/tcp open  afs3-fileserver
MAC Address: 5C:E9:1E:6C:1F:02 (Apple)
Device type: general purpose
Running: Apple macOS 11.X|12.X|13.X
OS CPE: cpe:/o:apple:mac_os_x:11 cpe:/o:apple:mac_os_x:12 cpe:/o:apple:mac_os_x:13
OS details: Apple macOS 11 (Big Sur) - 13 (Ventura) or iOS 16 (Darwin 20.6.0 - 22.4.0)
Network Distance: 1 hop
```

List the Operating system corresponding to the IP address

IP address	Operating system
- **192.168.251.236**	Microsoft Windows 10 1607 - 11 23H2
- **192.168.251.135**	Microsoft Windows 10 1607 - 11 23H2
- **192.168.251.240**	Apple macOS 11 (Big Sur) - 13 (Ventura)
- **192.168.251.193**	Microsoft Windows 10 1607 - 11 22H2

Step 4: Identify the IP address of the default gateway. Find out what ports and corresponding services are open on the default gateway?

Port	Service
192.168.251.34	53/tcp