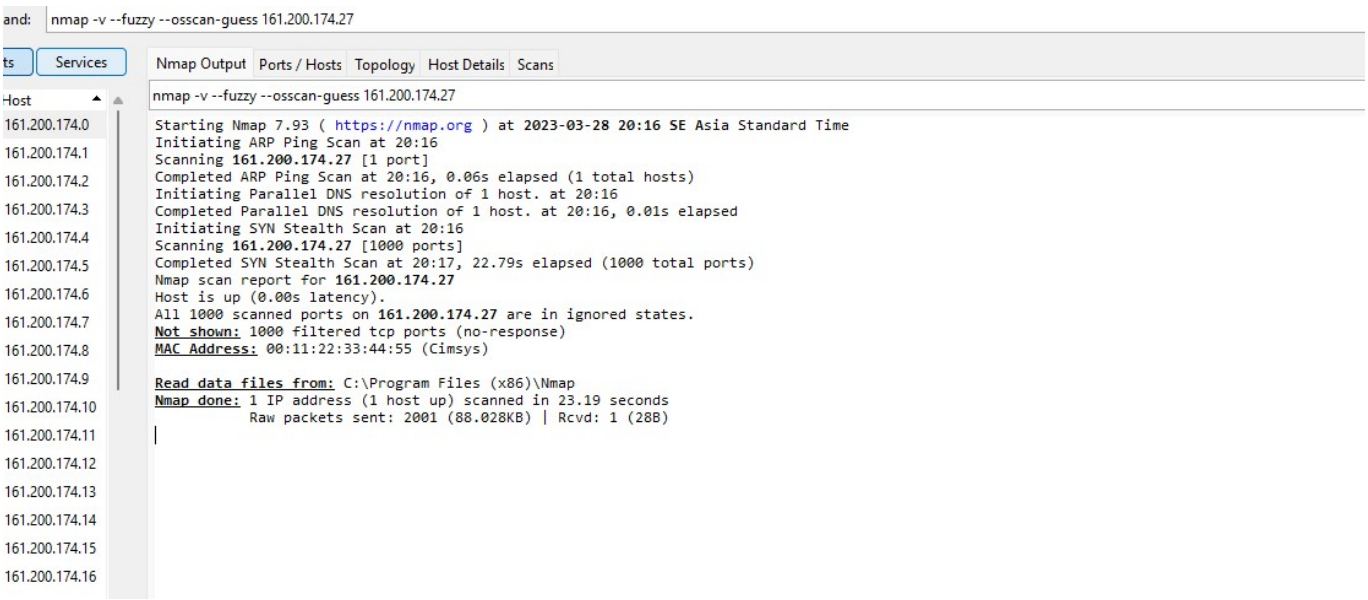
Activity 11: Network Scanner with NMAP

Student: Pirawat Wareetanyarat

---

1. Please connect to your university network (e.g ChulaWIFI or eduroam). We will use a simple ping scan to identify online hosts. Don't forget to substitute 10.201.3.0 with your network address. Please explain the parameters (-sn).

```
nmap -v -sn 10.201.3.0/2
```



Ans.

-sn means to perform ping scan .

2. Pick an ip address from the list in exercise 1 (maybe get the ip address of your friend). We will try to detect the OS from the network footprint.

Ans. I choose 161.200.174.24. Below is what i get.

```
Completed NSE at 20:25, 0.00s elapsed
Initiating NSE at 20:25
Completed NSE at 20:25, 0.00s elapsed
Nmap scan report for 161.200.174.24
Host is up (0.021s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE  SERVICE  VERSION
1433/tcp closed ms-sql-s
MAC Address: 00:11:22:33:44:55 (Cimsys)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: router|switch|bridge|specialized
Running: Cisco IOS 12.X, Cisco NX-OS 4.X|5.X, Digi embedded, Telco Systems embedded, Tripp Lite NetOS 7.X
OS CPE: cpe:/h:cisco:6506_router cpe:/o:cisco:ios:12.2 cpe:/o:cisco:nexus_7000 cpe:/o:cisco:nx_os:4.2.6 cpe:/o:cisco:nx_os:5.2 cpe:/h:telco_systems:t-
marc_250 cpe:/o:tripplite:netos:7.5.2t1
OS details: Cisco 6506 router (IOS 12.2), Cisco Nexus 7000 switch (NX-OS 4.2.6), Cisco NX-OS 4.0(1a)N1(1), Cisco NX-OS 5.2, Digi One SP serial-to-Ethernet
bridge, Telco Systems T-Marc 250, Tripp Lite NetOS 7.5.2t1
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   20.92 ms 161.200.174.24

NSE: Script Post-scanning.
Initiating NSE at 20:25
Completed NSE at 20:25, 0.00s elapsed
Initiating NSE at 20:25
Completed NSE at 20:25, 0.00s elapsed
Initiating NSE at 20:25
Completed NSE at 20:25, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 34.07 seconds
           Raw packets sent: 3016 (134.422KB) | Rcvd: 11 (566B)
```

3. Assuming that you are asked to identify all web servers on a campus, which command will you use to obtain the information. Please explain with an explicit example

Ans.

```
nmap -p 80,8080,443,8443 -sV -oA web-servers-scan 192.168.1.0/24
```

These are the options used in this command:

- p specifies the scan ports. We provide the HTTP and HTTPS ports 80, 8080, 443 and 8443 for web servers.
- sV enables version detection, which attempts to identify the software version running on the examined ports. This helps to uniquely identify web servers.
- oA specifies the name and format of the output file. Here, we utilize the web-servers-scan format to save the results in three distinct formats: standard, XML, and grepable.

This command scans all hosts within the specified IP address range for the specified ports and determines whether web server software is operating on those ports. The result will contain the IP addresses of the hosts with open web server ports, as well as the software versions and other details regarding the services running on those ports.