Other nmap scan MASSCAN and RUSTSCAN

host discovery

```
sudo nmap -n -sn -PE -PP -PM -PS21,22,23,25,80,110,443,445,3389 -
PA21,22,23,25,80,110,443,445,3389 --source-port 53 -oN {FileName} {IP}
```

```
nmap -Pn -p- -T4 IP | grep open | awk '{print $1}'| cut -d '/' -f1 | tr '\n' ','
```

Host discovery

```
nmap -sn 192.168.50.1-253
nmap -v -sn 192.168.50.1-253 -oG ping-sweep.txt
```

#Nmap_scan

**Partial SYN scan (not completing the three-way handshake)

```
sudo nmap -sS 192.168.50.149
```

STEALTH TCP scan more longer thank the stealth scan

```
nmap -sT 192.168.50.149
```

#UDP_scan

```
sudo nmap -sU -sS 192.168.50.149
```

Full scan to have a complete picture of the target

```
sudo nmap -sU -sS 192.168.50.149
```

Network sweep

```
nmap -v -sn 192.168.50.1-253 -oG ping-sweep.txt
grep Up ping-sweep.txt | cut -d " " -f 2
```

Nmap top ports

```
nmap -sT -A --top-ports=20 192.168.50.1-253 -oG top-port-sweep.txt
```

Nmap OS fingerprint scan

```
sudo nmap -O 192.168.50.14 --osscan-guess

sudo nmap -sV -p 443 --script "vuln" 192.168.50.124
sudo nmap -sV -p 443 --script "http-vuln-cve2021-41773" 192.168.50.124 APACHE
```

#ATTENTION

Note that OS Fingerprinting is not always 100% accurate, often due to network devices like firewalls or proxies that rewrite packet headers in between the communication.

Banners can be modified by system administrators and intentionally set to fake service names to mislead potential attackers.

#Scripts

```
nmap --script http-headers 192.168.50.6
```

#help_on_the_script

This command will help you to understand better how the script is working

```
nmap --script-help http-headers
```

#Windows_machine_internal_scanning_powershell

```
Test-NetConnection -Port 445 192.168.50.151
```

The *Test-NetConnection*[15] function checks if an IP responds to ICMP and whether a specified TCP port on the target host is open.

For instance, from the Windows 11 client, we can verify if the SMB port 445 is open on a domain controller as follows.

#Parsing_the_response

Retrieving the IP open:

`grep open results.txt| cut -d " " -f2 `