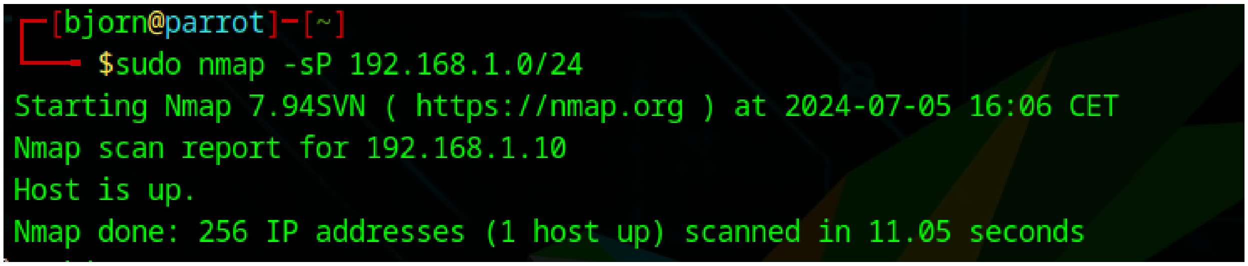
PHASE 3:

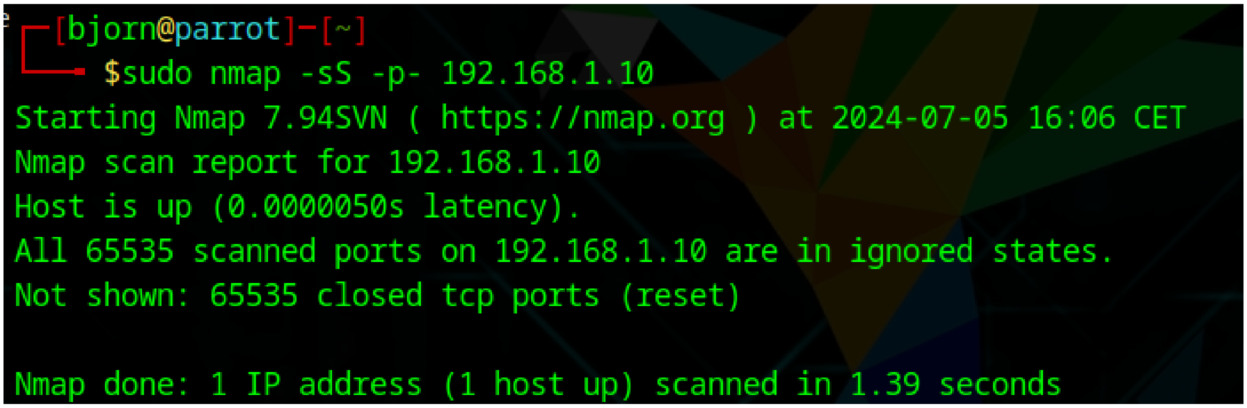
1. Ping Scan (`sudo nmap -sP 192.168.1.0/24`)



```
┌─[bjorn@parrot]─[~]
└──╼ $sudo nmap -sP 192.168.1.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-05 16:06 CET
Nmap scan report for 192.168.1.10
Host is up.
Nmap done: 256 IP addresses (1 host up) scanned in 11.05 seconds
```

- Identified one live host (`192.168.1.10`) on the network.

2. TCP SYN Scan (`sudo nmap -sS -p- 192.168.1.10`)

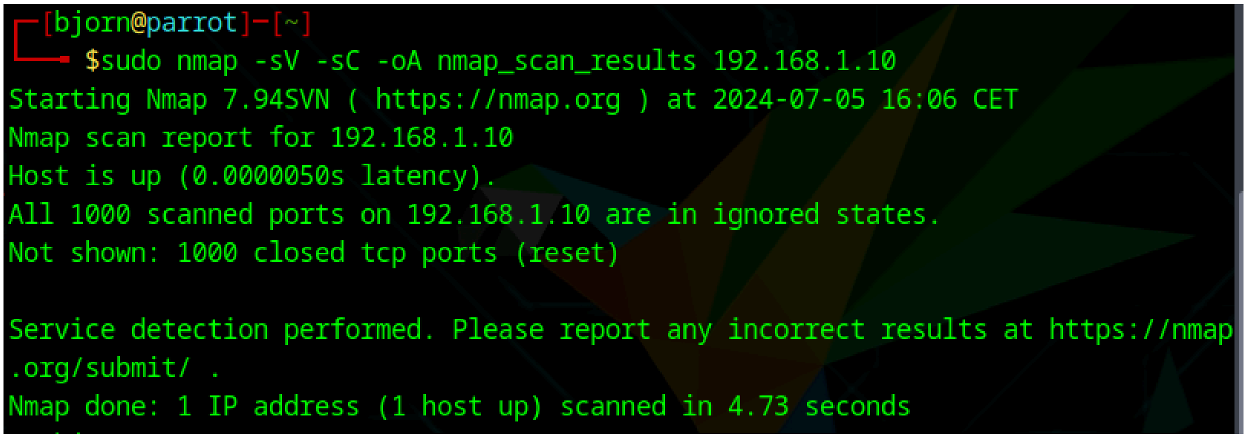


```
┌─[bjorn@parrot]─[~]
└──╼ $sudo nmap -sS -p- 192.168.1.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-05 16:06 CET
Nmap scan report for 192.168.1.10
Host is up (0.0000050s latency).
All 65535 scanned ports on 192.168.1.10 are in ignored states.
Not shown: 65535 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 1.39 seconds
```

- All 65,535 scanned ports on `192.168.1.10` are in "ignored" states, indicating they are likely filtered by a firewall or another security measure.

3. Service Version Detection and Script Scanning (`sudo nmap -sV -sC -oA nmap_scan_results 192.168.1.10`)

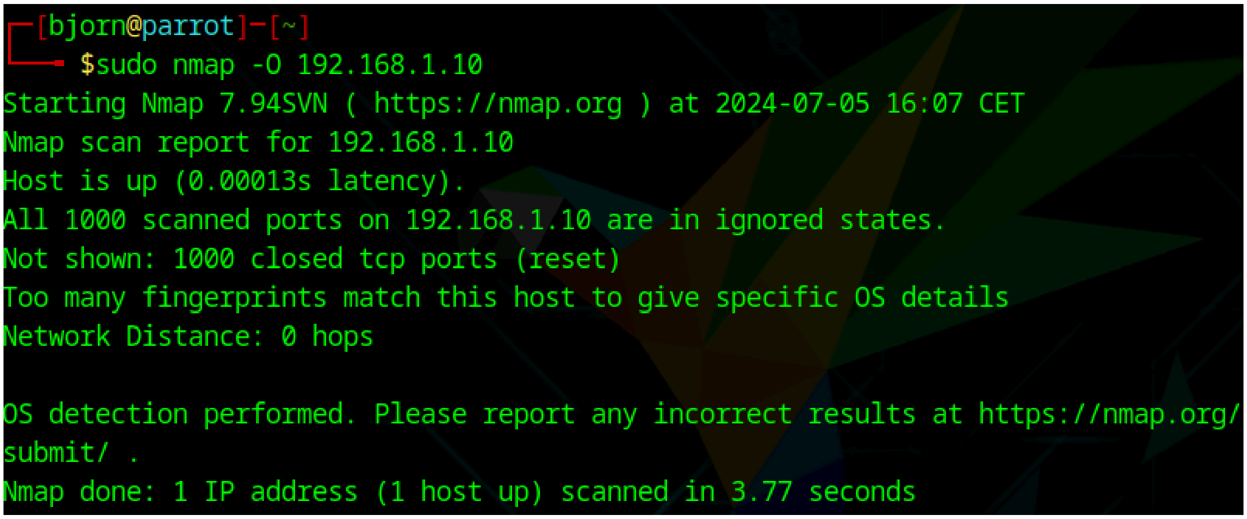


```
┌─[bjorn@parrot]─[~]
└──╼ $sudo nmap -sV -sC -oA nmap_scan_results 192.168.1.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-05 16:06 CET
Nmap scan report for 192.168.1.10
Host is up (0.0000050s latency).
All 1000 scanned ports on 192.168.1.10 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.73 seconds
```

- All 1,000 scanned ports on `192.168.1.10` are in "ignored" states.
- Service detection was performed, but no specific services or vulnerabilities were identified due to port states.

4. OS Detection (`sudo nmap -O 192.168.1.10`)

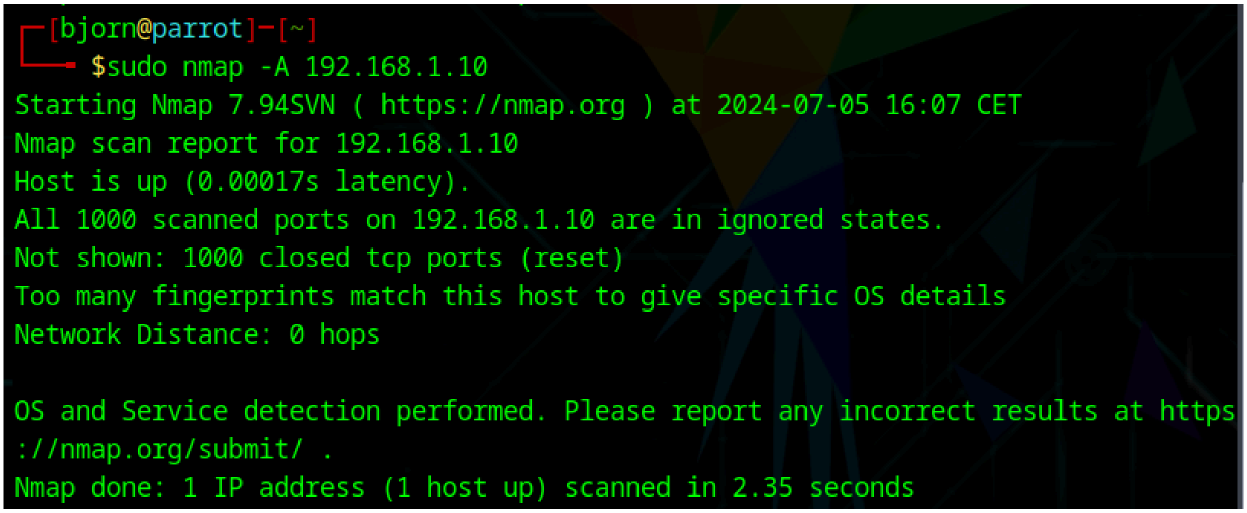


```
┌─[bjorn@parrot]─[~]
└──╼ $sudo nmap -O 192.168.1.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-05 16:07 CET
Nmap scan report for 192.168.1.10
Host is up (0.00013s latency).
All 1000 scanned ports on 192.168.1.10 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.77 seconds
```

- Too many fingerprints match this host to provide specific OS details.
- OS detection suggests the host is hiding detailed information about its operating system, potentially through firewall or filtering configurations.

5. Aggressive Scan (`sudo nmap -A 192.168.1.10`)



```
┌─[bjorn@parrot]─[~]
└──╼ $sudo nmap -A 192.168.1.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-05 16:07 CET
Nmap scan report for 192.168.1.10
Host is up (0.00017s latency).
All 1000 scanned ports on 192.168.1.10 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

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 2.35 seconds
```

- All 1,000 scanned ports on `192.168.1.10` are in "ignored" states.
- OS and service detection were performed but did not provide specific details due to port states and potential filtering.