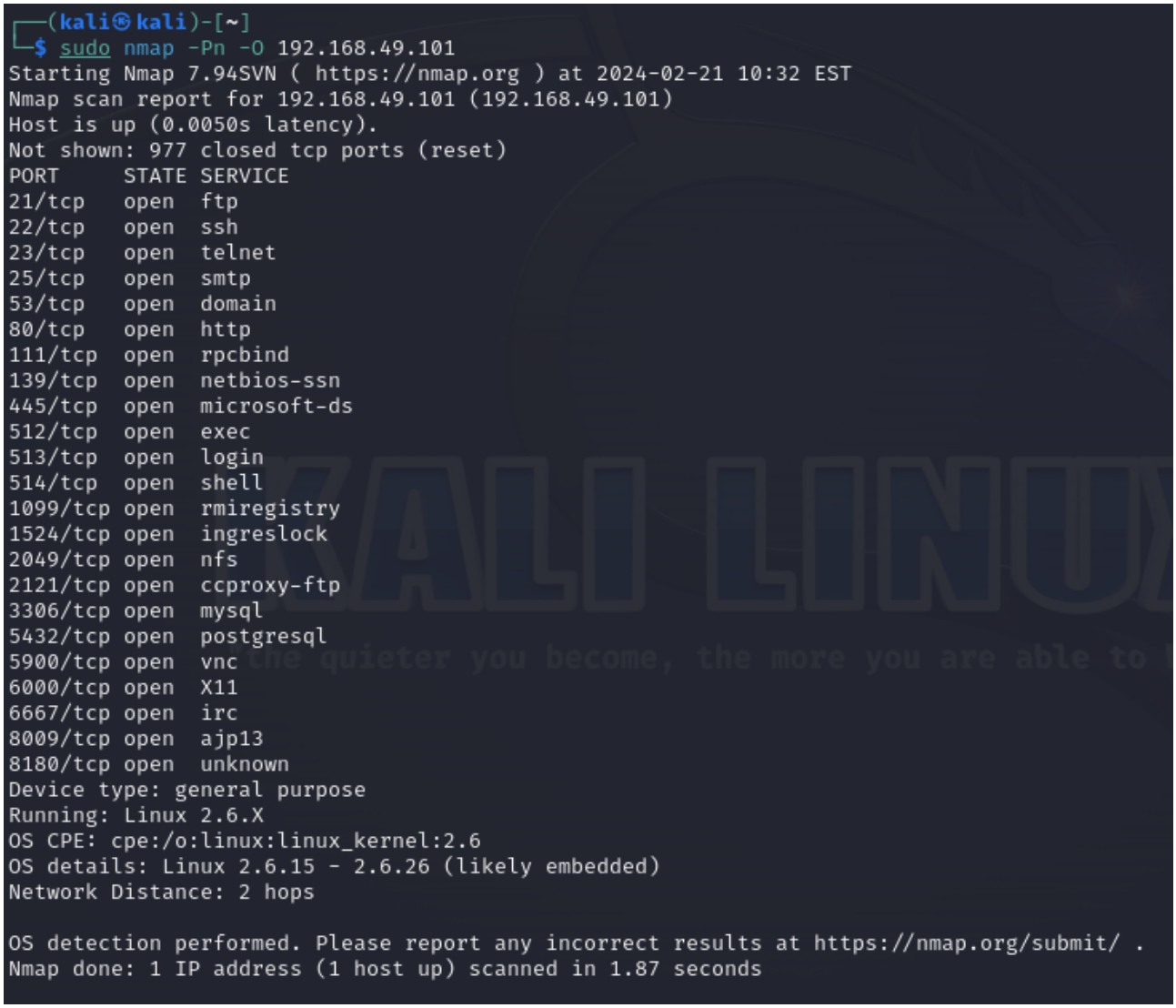
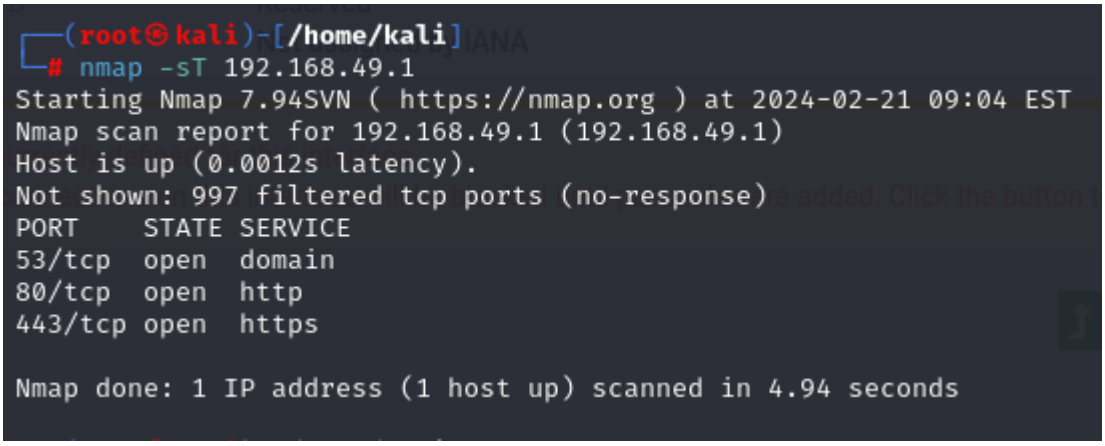
CS2102

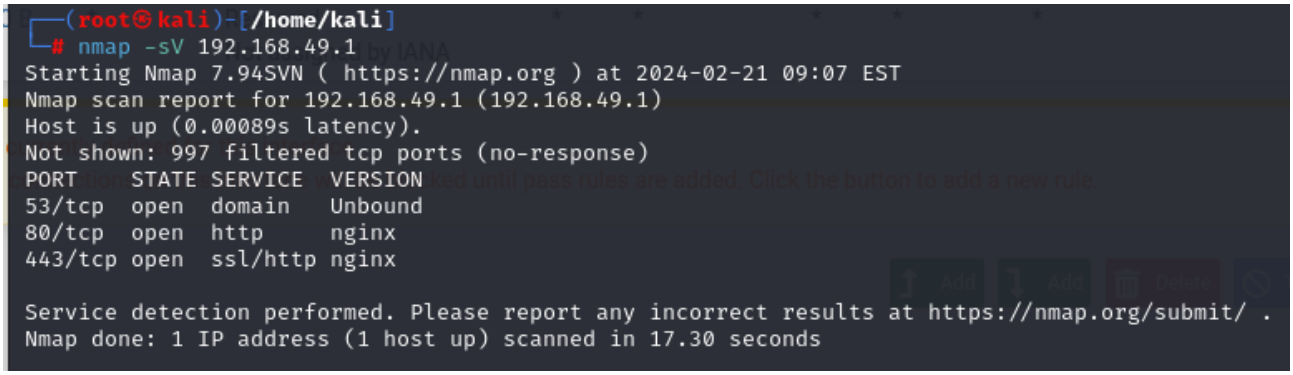


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -Pn -O 192.168.49.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 10:32 EST
Nmap scan report for 192.168.49.101 (192.168.49.101)
Host is up (0.0050s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.15 - 2.6.26 (likely embedded)
Network Distance: 2 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.87 seconds
```

```
┌──(root㉿kali)-[/home/kali]
└─# sudo nmap -sS 192.168.49.101 -T5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 10:19 EST
Nmap scan report for 192.168.49.101 (192.168.49.101)
Host is up (0.0069s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.46 seconds
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap 192.168.49.1/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 09:01 EST
Nmap scan report for 192.168.49.1 (192.168.49.1)
Host is up (0.0011s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https

Nmap scan report for 192.168.49.101 (192.168.49.101)
Host is up (0.0071s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap done: 256 IP addresses (2 hosts up) scanned in 9.23 seconds
```


(root㉿kali)-[/home/kali]
nmap -sT 192.168.49.1
Starting Nmap 7.94SVN (https://nmap.org) at 2024-02-21 09:04 EST
Nmap scan report for 192.168.49.1 (192.168.49.1)
Host is up (0.0012s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT STATE SERVICE
53/tcp open domain
80/tcp open http
443/tcp open https
Nmap done: 1 IP address (1 host up) scanned in 4.94 seconds


(root㉿kali)-[/home/kali]
nmap -sV 192.168.49.1
Starting Nmap 7.94SVN (https://nmap.org) at 2024-02-21 09:07 EST
Nmap scan report for 192.168.49.1 (192.168.49.1)
Host is up (0.00089s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION
53/tcp open domain Unbound
80/tcp open http nginx
443/tcp open ssl/http nginx
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.30 seconds

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -Pn -O 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 09:35 EST
Nmap scan report for 192.168.50.102
Host is up (0.00042s latency).
All 1000 scanned ports on 192.168.50.102 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:48:78:D8 (Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 37.11 seconds

┌──(root㉿kali)-[/home/kali]
└─#
```

In quest ultimo scan anche disattivando l'antivirus non si riesce a trovare le porte aperte perciò ho provato uno scan più aggressivo ma senza risultati positivi

```
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# nmap -Pn -O -T3 -p 80-443 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 09:43 EST
Nmap scan report for 192.168.50.102
Host is up (0.00042s latency).
All 364 scanned ports on 192.168.50.102 are in ignored states.
Not shown: 364 filtered tcp ports (no-response)
MAC Address: 08:00:27:48:78:D8 (Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.47 seconds
```