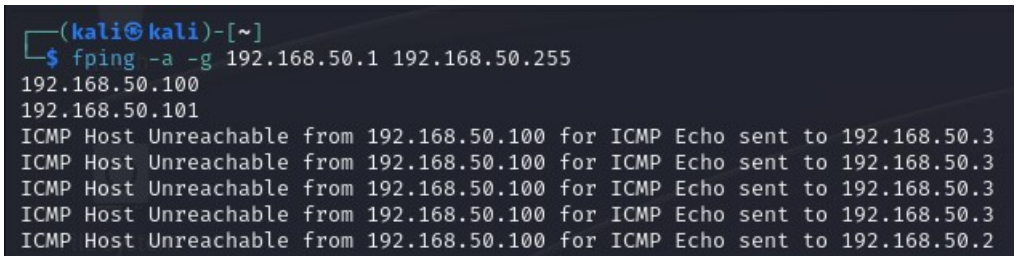
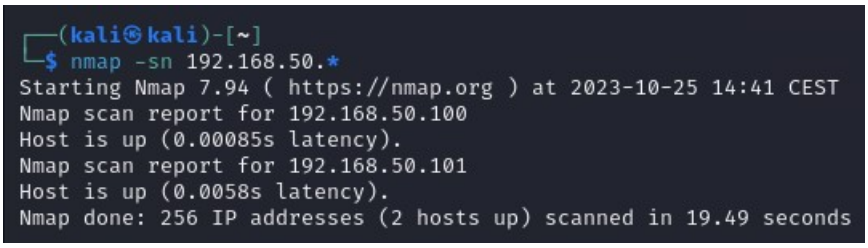
In questo esercizio dobbiamo procedere alla scansione di due macchine target tramite il programma Nmap.

Per prima cosa effetuiamo un ping sweep sulla rete 192.168.50.0 per verificare quali inidirzzi IP sono attivi.

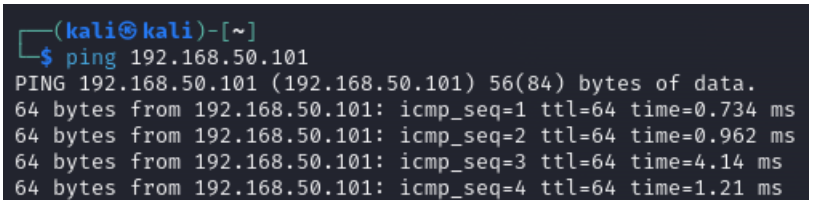


Riceviamo due IP attivi come risposta. Sapendo che il primo è il nostro, capiamo che 192.168.50.101 è l'IP di Metasploitable; sappiamo inoltre che il protocollo ICMP è attivo (avendo ricevuto risposta).
Avremmo potuto anche usare il comando nmap -sn con l'IP della rete target.

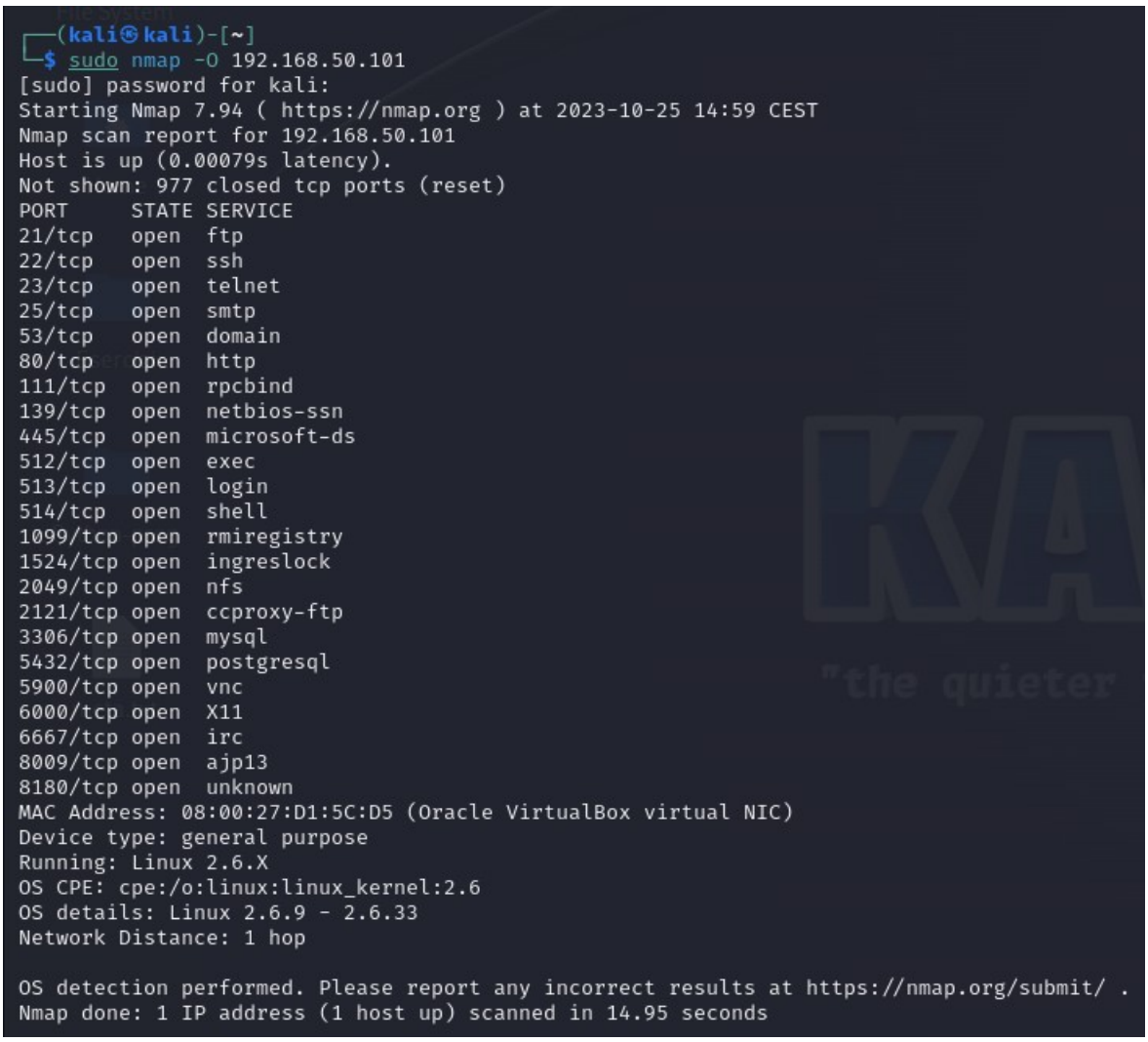


Abbiamo usato l'asterisco come wildcard per scansionare l'intera rete, ma avremmo potuto impostare un range di inidirizzi o scrivere l'indirizzo di rete in formato CIDR.

Procediamo ora con un normale ping per ricevere più informazioni.

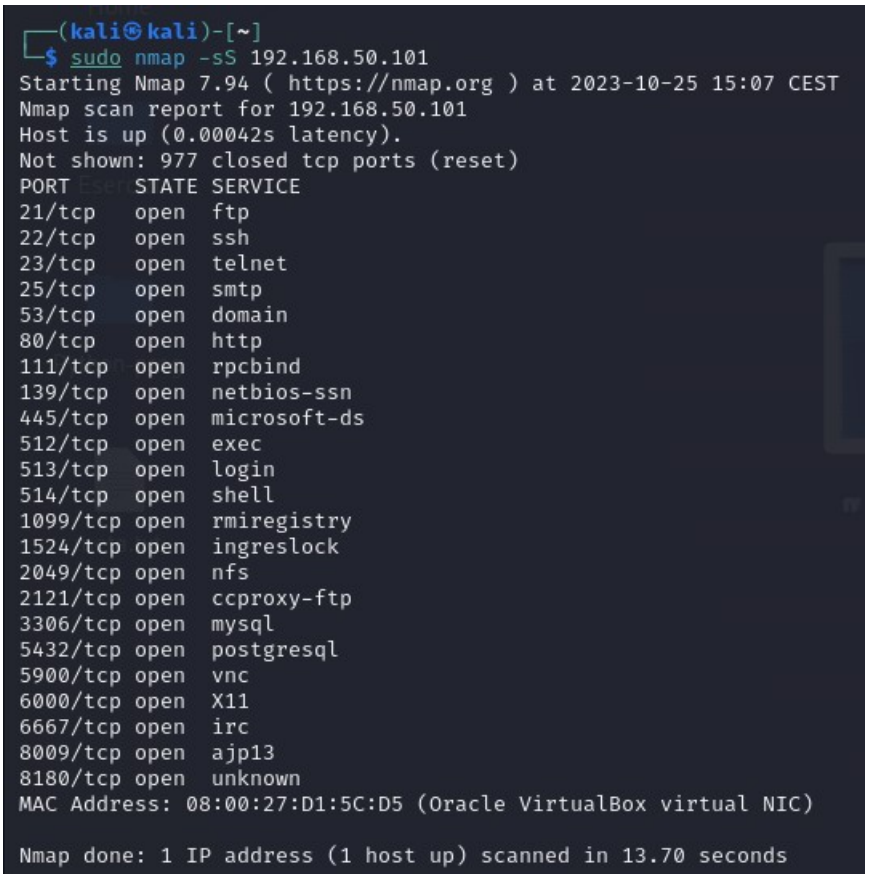


In questo caso vediamo informazioni relative alla grandezza del pacchetto, il tempo che il pacchetto ha impiegato per giungere a destino e il “time to live”, cioè il numero massimo di salti che il pacchetto può compiere prima di venire distrutto (è un metodo per non lasciare il pacchetto in un loop infinito e non creare latenze).
Adesso usiamo nmap per capire quale sistema operativo è presente sulla macchina target. Uitilizziamo il comando nmap -O.



Con questo comando riceviamo molte informazioni. In primo luogo notiamo che il sistema operativo identificato è Linux.
Inoltre possiamo vedere quali sono le porte aperte e i relativi servizi attivi sull'host target.
Essendo le due macchine sulla stessa rete abbiamo una Network distance di 1 salto solo (ci fosse stato di mezzo un firewall, un router-gateway avremmo avuto 2 salti).

Procediamo ora con due diversi tipi di scansioni.
Per primo andiamo a fare una scansione stealth, che sfrutta solo la prima parte della three way handshake del protocollo TCP (quindi il “syn” inviato dalla macchina attaccante a quella target). Si dice scansione stealth perché non crea molto rumore, facendo solo un passaggio; può però restituire risultati che non sono al 100% corretti. Usiamo il comando nmap -sS.



In questo caso come risultato abbiamo solo le porte attive (e relativi servizi).

Procediamo ora con una scansione più invasiva, che completa la three way handshake; usiamo il comando nmap -sT.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sT 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 15:12 CEST
Nmap scan report for 192.168.50.101
Host is up (0.0038s latency).
Not shown: 977 closed tcp ports (conn-refused)
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 13.53 seconds
```

In questo caso i risultati sono identici alla scansione stealth, ma può essere dovuto al semplice fatto che siamo all'interno di un laboratorio virtuale e stiamo scansionando un solo IP.

In ultimo cerchiamo di recupereare informazioni sulle versioni dei vari servizi attivi su questo host. Per farlo usiamo il comando nmap -sV.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 15:23 CEST
Nmap scan report for 192.168.50.101
Host is up (0.0013s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 65.85 seconds
```

Come possiamo vedere qui abbiamo informazioni sulle versioni di tutti i servizi sulle porte attive.

Procediamo ora con la scansione della seconda macchina target. Sappiamo che l'indirizzo è 192.168.50.102 e che c'è un firewall che non ci permette di pingare le due macchine. Usiamo allora il comando nmap -Pn -O per identificare il sistema operativo senza lanciare un ping (-Pn).

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -Pn -O 192.168.50.102
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 15:46 CEST
Nmap scan report for 192.168.50.102
Host is up (0.00058s 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:B5:C8:63 (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 37.06 seconds
```

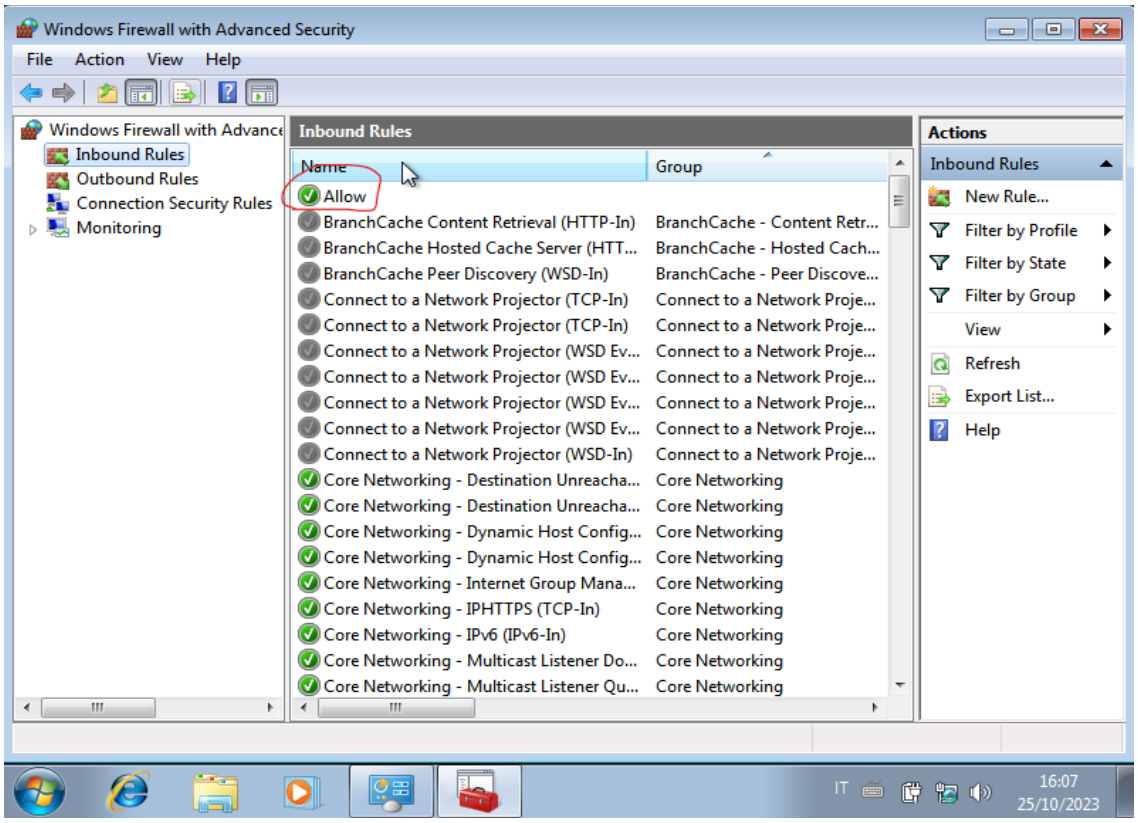
In questo caso ci viene riportato che troppe impronte corrispondono all'host e quindi nmap non è in grado di identificarne il sistema operativo.

Per il momento procediamo con le altre scansioni (stealth, TCP connect, version detection) sempre escludendo il ping.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.50.102
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 15:51 CEST
Nmap scan report for 192.168.50.102
Host is up (0.00076s 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:B5:C8:63 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 34.37 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -sT 192.168.50.102
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 15:52 CEST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.03 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -Pn -sT 192.168.50.102
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 15:53 CEST
Nmap scan report for 192.168.50.102
Host is up.
All 1000 scanned ports on 192.168.50.102 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 214.42 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -Pn -sV 192.168.50.102
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 15:58 CEST
Nmap scan report for 192.168.50.102
Host is up.
All 1000 scanned ports on 192.168.50.102 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 214.69 seconds
```

Nuovamente non riusciamo ad effettuare la scansione. Proviamo allora a settare una regola nel firewall

della macchina target che permetta la connessione tra le macchine.



Ora riproviamo a identificare il sistema operativo.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.50.102
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 16:09 CEST
Nmap scan report for 192.168.50.102
Host is up (0.00070s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
MAC Address: 08:00:27:B5:C8:63 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 c
Aggressive OS guesses: Microsoft Windows Phone 7.5 or 8.0 (98%), Microsoft Windows Embedded
7 (97%), Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (96%), Microsof
), Microsoft Windows 8 Enterprise (92%)
No exact OS matches for host (test conditions non-ideal).
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 21.84 seconds
```

Adesso riceviamo un nuovo tipo di risposta, in cui ci viene data la percentuale di probabilità di un determinato sistema operativo. Date le percentuali, si può dire con ragionevole certezza che si tratta di un sistema Windows.

Effettuiamo di nuovo le altre scansioni e vediamo che i risultati sono più simili a quelli ottenuti con le scansioni di Metasploitable.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.50.102
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 16:13 CEST
Nmap scan report for 192.168.50.102
Host is up (0.00075s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
MAC Address: 08:00:27:B5:C8:63 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 17.27 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -sT 192.168.50.102
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 16:14 CEST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.04 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -Pn -sT 192.168.50.102
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 16:14 CEST
Nmap scan report for 192.168.50.102
Host is up (0.0022s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 17.72 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.50.102
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 16:15 CEST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.13 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -Pn -sV 192.168.50.102
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 16:16 CEST
Nmap scan report for 192.168.50.102
Host is up (0.0033s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: MARCO-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 75.74 seconds
```