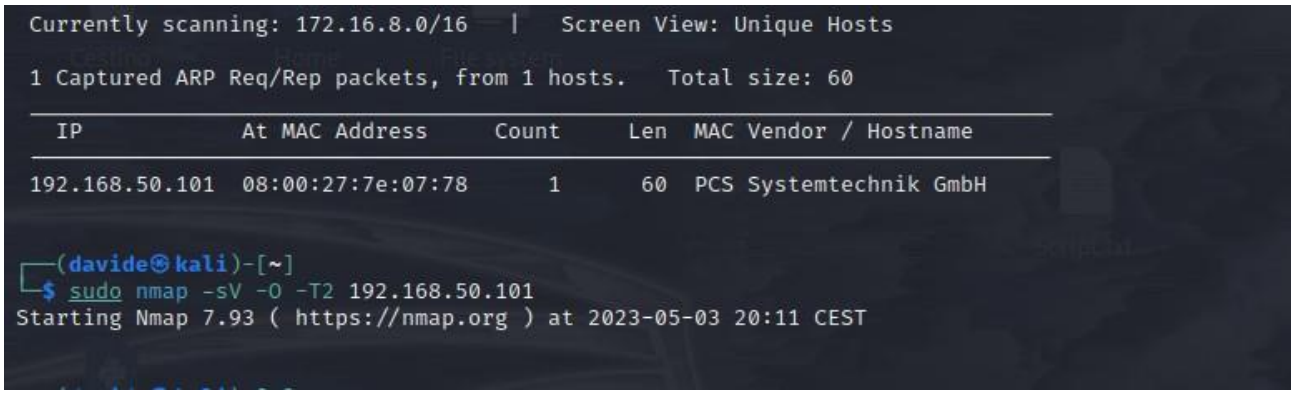
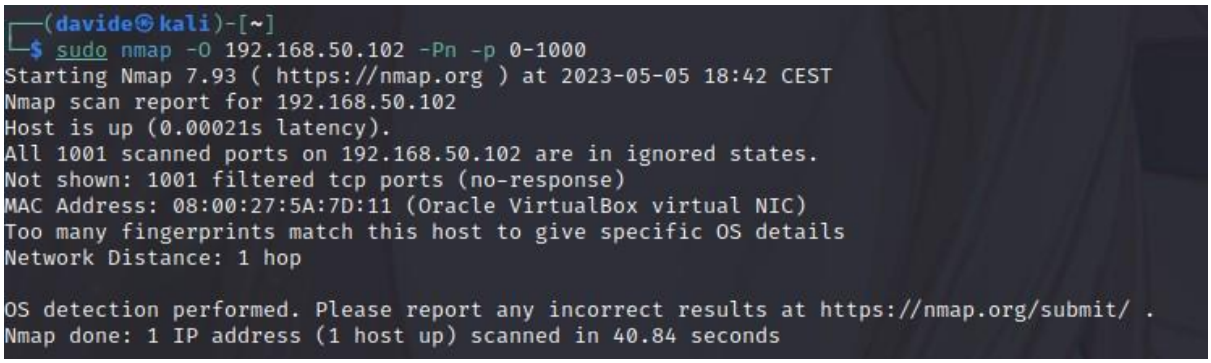
Netdiscover per trovare l'indirizzo IP del presunto Windows che vogliamo scannerizzare:

(ho sostituito in seguito l'indirizzo IP della macchina, la foto è precedente alle vicissitudini dell'esercizio)

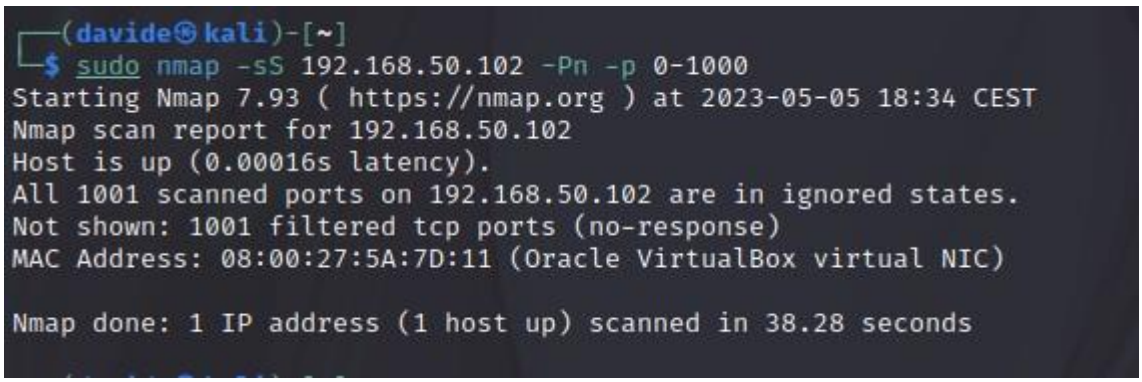


Proviamo diversi tipi di scansioni ma il risultato viene costantemente filtrato dal Firewall:

-O



-sS



-sT

```
┌──(davide㉿kali)-[~]
└─$ sudo nmap -sT 192.168.50.102 -Pn -p 0-1000
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-05 18:37 CEST
Stats: 0:02:59 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 76.92% done; ETC: 18:41 (0:00:50 remaining)
Stats: 0:03:00 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 77.42% done; ETC: 18:41 (0:00:49 remaining)
Nmap scan report for 192.168.50.102
Host is up.
All 1001 scanned ports on 192.168.50.102 are in ignored states.
Not shown: 1001 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 229.02 seconds
```

-sV

```
┌──(davide㉿kali)-[~]
└─$ sudo nmap -sV 192.168.50.102 -Pn -p 0-1000
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-05 18:33 CEST
Stats: 0:00:12 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Nmap scan report for 192.168.50.102
Host is up (0.00020s latency).
All 1001 scanned ports on 192.168.50.102 are in ignored states.
Not shown: 1001 filtered tcp ports (no-response)
MAC Address: 08:00:27:5A:7D:11 (Oracle VirtualBox virtual NIC)
```

Individuando una forte azione di contrasto del firewall optiamo per scansioni meno rumorose:

Proviamo una -sV su porte specifiche con tempistiche più dilatate nel tempo (-T2)

```
┌──(davide㉿kali)-[~]
└─$ sudo nmap -sV -O -T2 192.168.50.101 -p 0-443
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-03 20:14 CEST
Stats: 0:02:51 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 42.91% done; ETC: 20:20 (0:03:29 remaining)
Stats: 0:02:52 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 43.02% done; ETC: 20:20 (0:03:29 remaining)
Stats: 0:02:58 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 44.48% done; ETC: 20:20 (0:03:25 remaining)
Stats: 0:02:58 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 44.59% done; ETC: 20:20 (0:03:24 remaining)
Stats: 0:04:29 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 69.03% done; ETC: 20:20 (0:01:54 remaining)
Stats: 0:04:29 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 69.14% done; ETC: 20:20 (0:01:54 remaining)
Stats: 0:06:10 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 95.95% done; ETC: 20:20 (0:00:15 remaining)
Nmap scan report for 192.168.50.101
Host is up (0.00022s latency).
All 444 scanned ports on 192.168.50.101 are in ignored states.
Not shown: 444 filtered tcp ports (no-response)
MAC Address: 08:00:27:7E:07:78 (Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

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 404.23 seconds

┌──(davide㉿kali)-[~]
└─$ sudo nmap -sV -O -T1 192.168.50.101 -p 135.139.445.5357
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-03 20:22 CEST
Error #487: Your port specifications are illegal.  Example of proper form: "-100,200-1024,T:3000-4000,U:60000-"
QUITTING!

┌──(davide㉿kali)-[~]
└─$ sudo nmap -sV -O -T1 192.168.50.101 -p 135,139,445,5357
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-03 20:22 CEST
Stats: 0:00:58 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 12.50% done; ETC: 20:27 (0:03:30 remaining)
```

-T1 restituisce con una scansione stealth sS e T1 il risultato delle 3 porte presunte aperte da Windows. Adesso le visualizziamo tramite nmap ma risultano filtrate.

Pertanto dopo aver provato per diversi giorni a scansionare e tentare di entrare con msfconsole posso dire che al momento con le mie conoscenze ed il firewall attivo non riesco a entrare nella macchina.