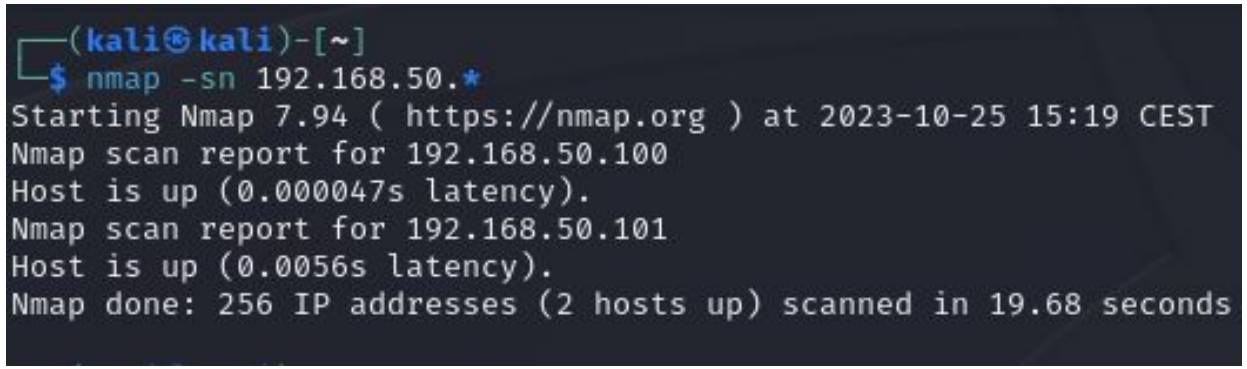
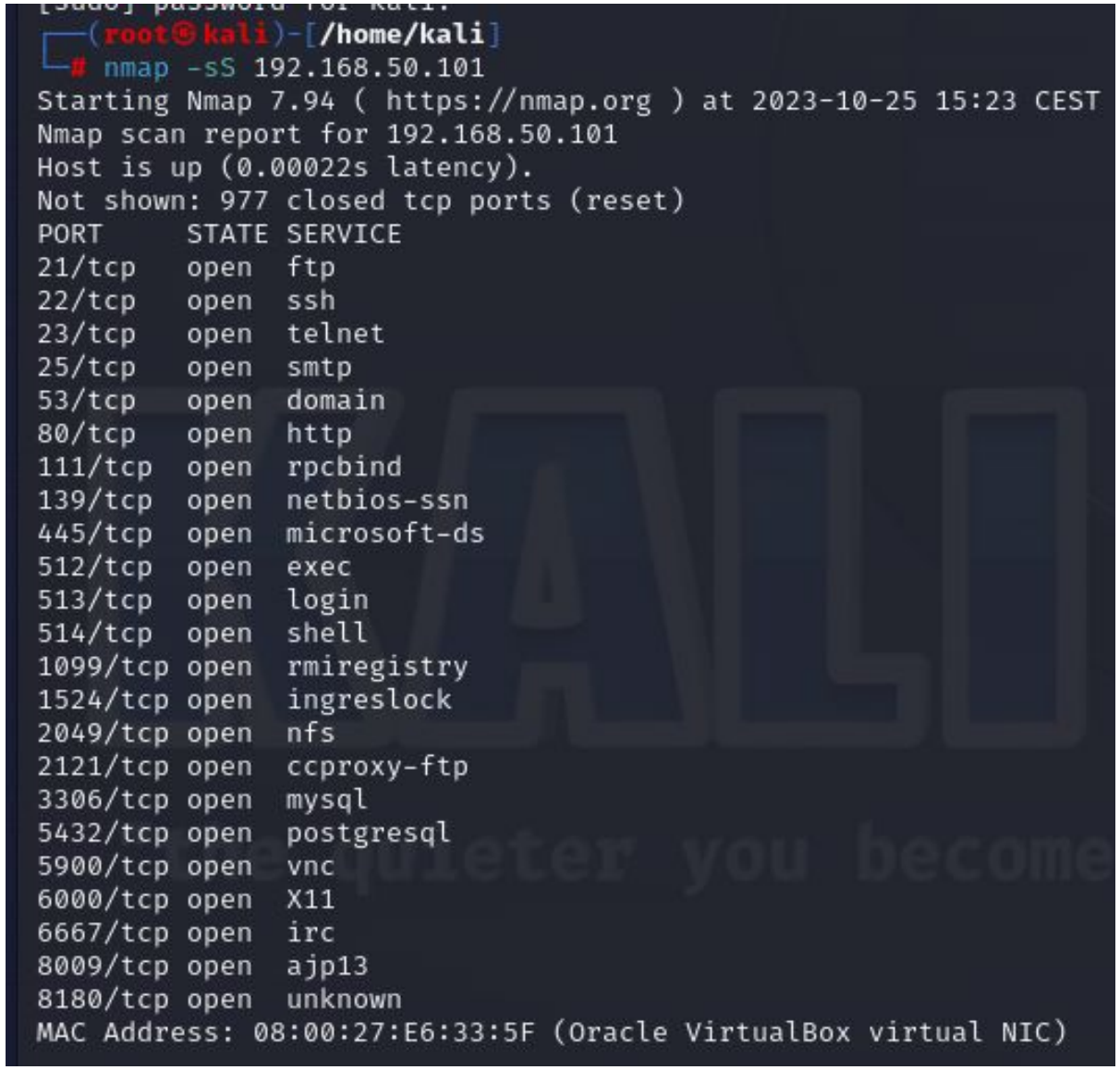
EPICODE

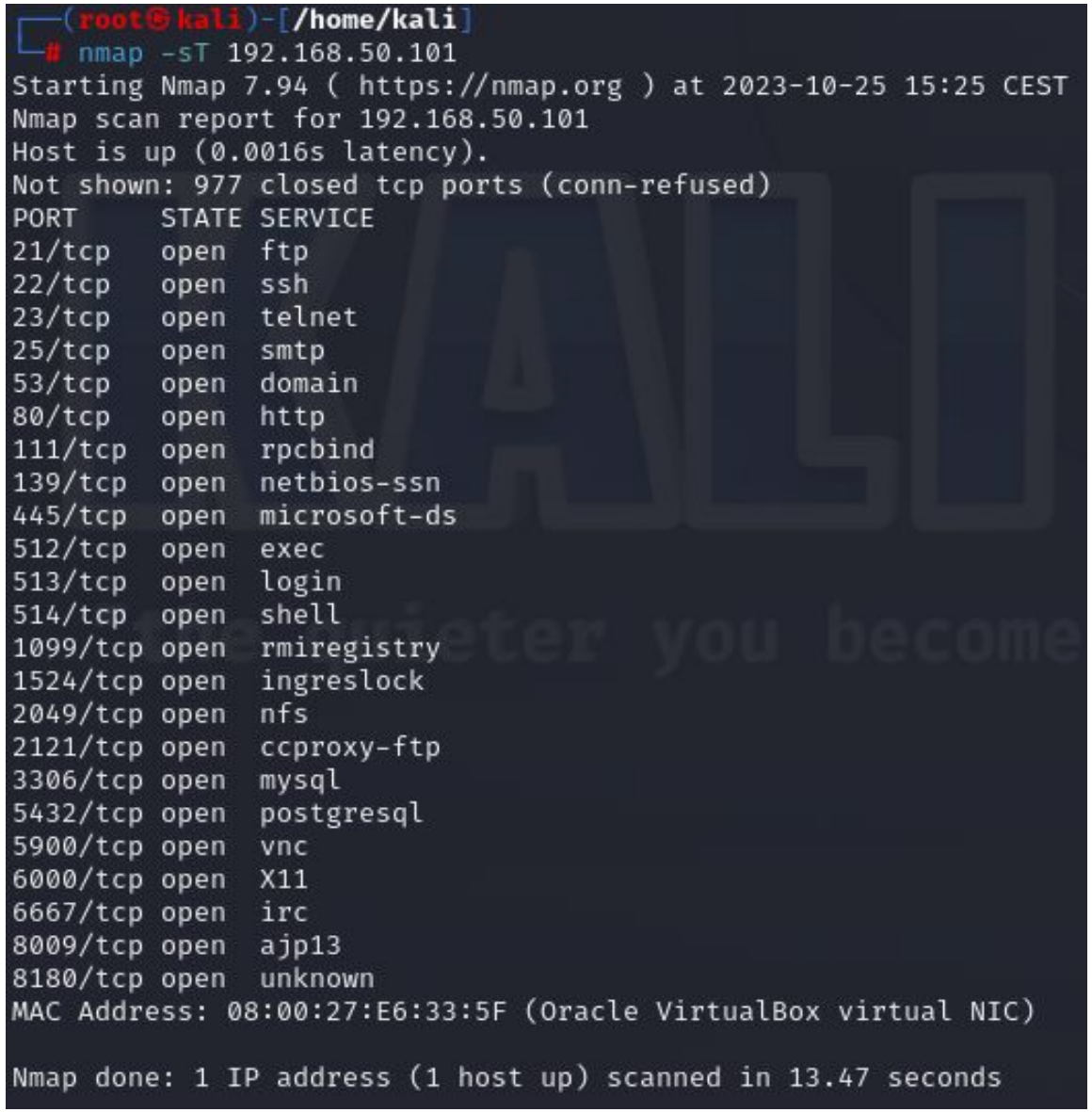
Progetto Alessandro Moscetti 25/10



Tramite l'opzione di nmap 'sn' siamo andati a controllare gli host attivi tramite ping.
Utilizzando il carattere '*' nell'ip target sono andato a scansionare tutti gli ip compresi tra il 192.168.50.0 e il 192.168.50.255.
Sapendo che '192.168.50.100' è il nostro ip sulla rete, sappiamo di conseguenza l'ip della macchina target.

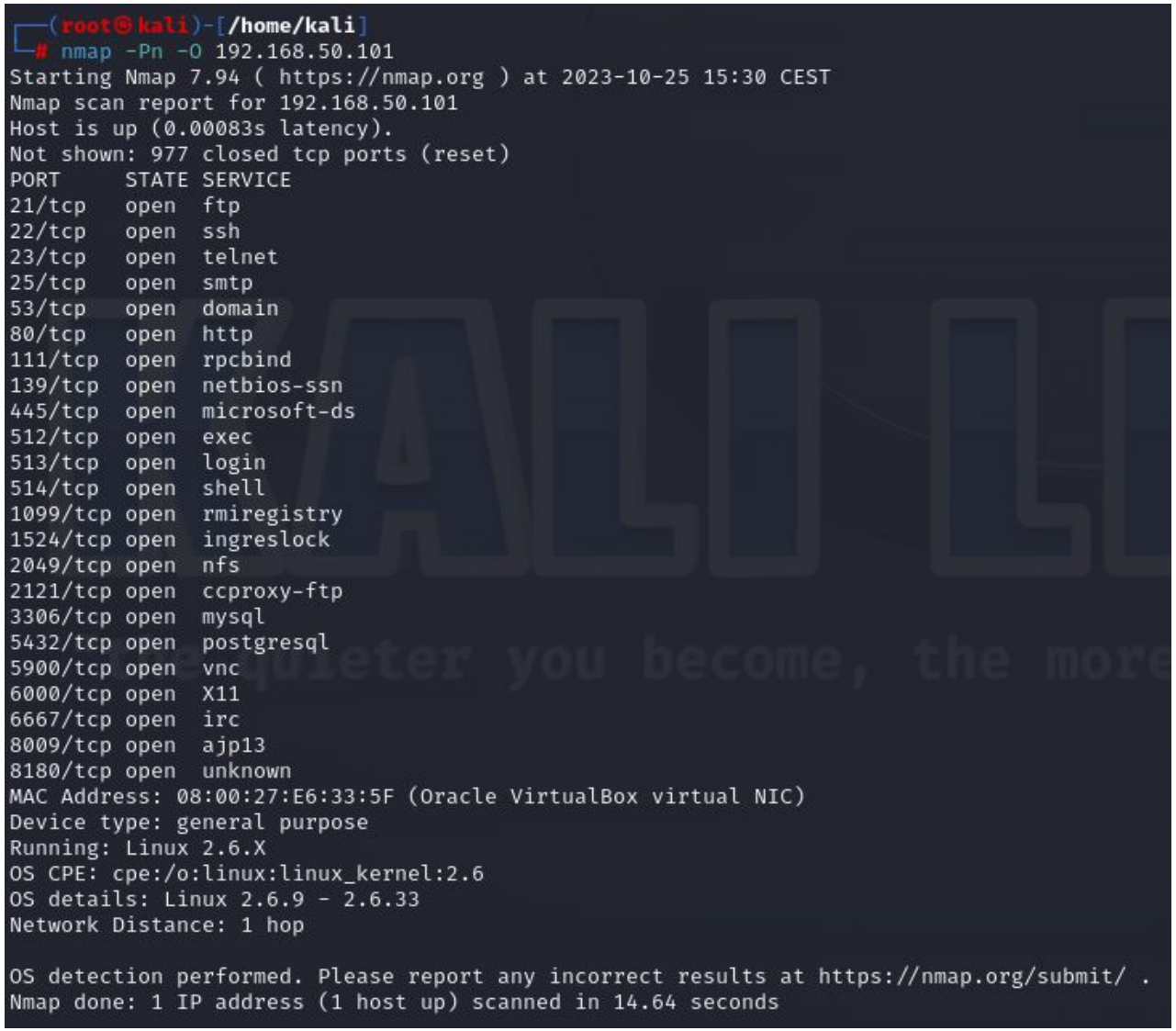


Tramite l'opzione di nmap 'sS' siamo andati a effettuare un Syn scan sull'ip trovato in precedenza. Questa opzione è il metodo meno invasivo perchè non completa la 3-way-handshake ma si interrompe alla ricezione del syn/ack, ma potrebbe di conseguenza non essere accurata al 100%. Nell'output possiamo notare le varie porte aperte con il relativo servizio e il MAC Address dell'host.

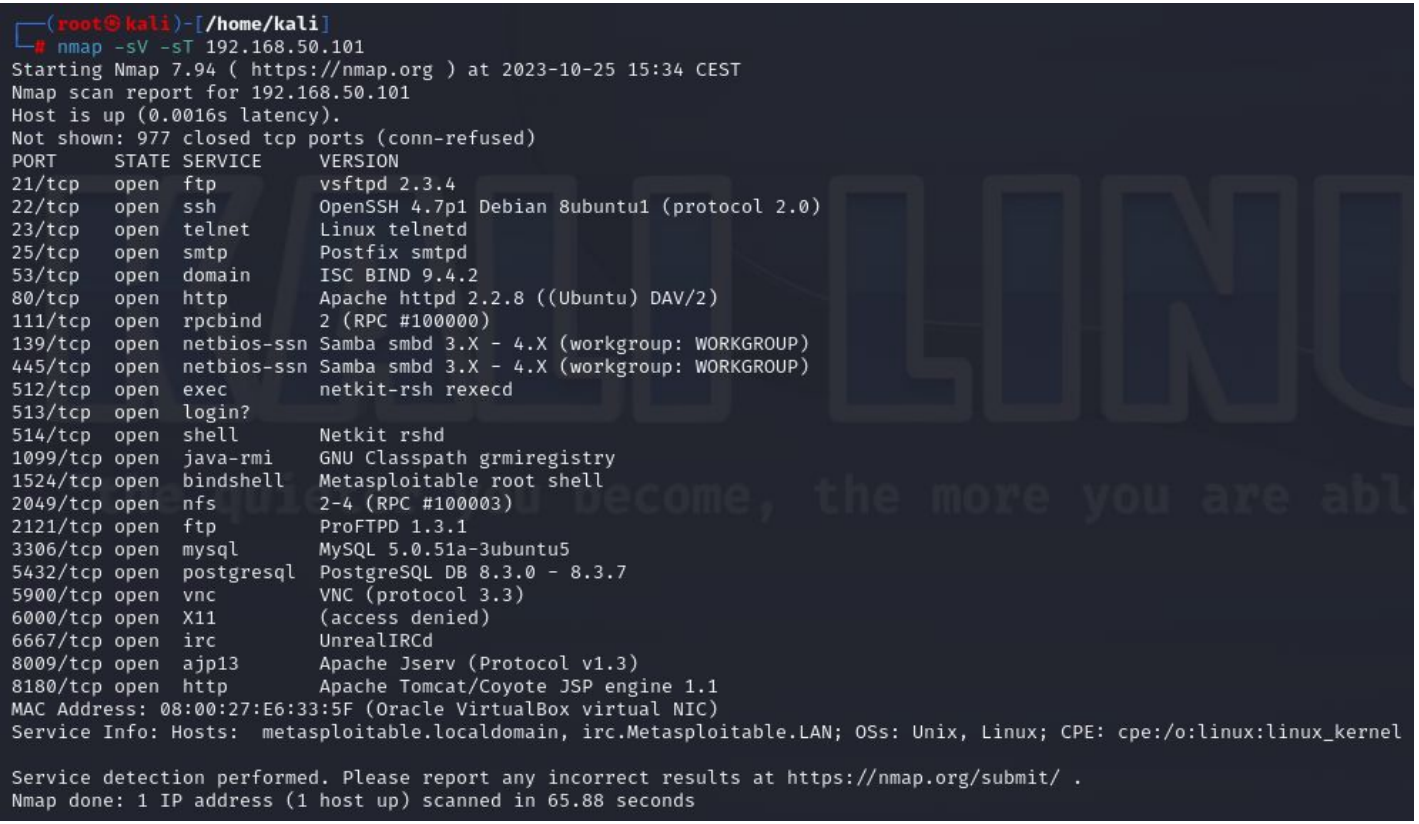


Tramite l'opzione di nmap 'sT' siamo andati a effettuare una scansione TCP Connect sull'ip. Questa opzione è più invasiva e lenta della precedente, ma più affidabile.

Possiamo notare che non ci sia differenza tra gli output con le opzioni ‘sS’ e ‘sT.
La differenza sta nell’affidabilità degli output e il ‘rumore’ creato dalle scansioni.



Per la fase di Os fingerprint siamo andati ad utilizzare l'omonima opzione con ‘-O’ implementato da ‘-Pn’ per non inviare ulteriori ping nella scansione.
Così facendo siamo andati a vedere il sistema operativo dell’host in questo caso ‘Linux 2.6.X’.



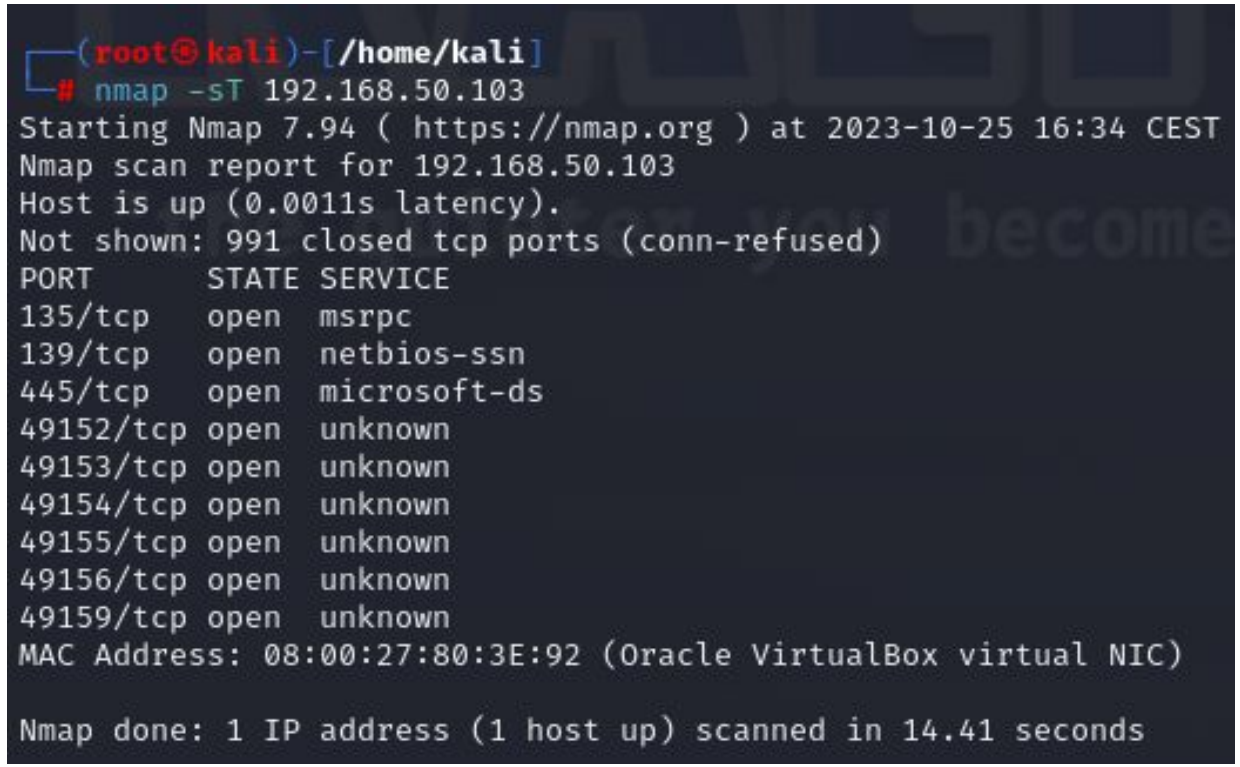
Tramite l'opzione 'sV' siamo andati a effettuare una Version detection.
Con questa opzione andiamo a vedere anche la versione e dettagli dei servizi, per il resto è a tutti gli effetti come la scansione TCP Connect.

Andando ad effettuare lo stesso esercizio con la nostra macchina Windows non troveremo alcun risultato senza disattivare o aggirare il Firewall del sistema operativo.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS 192.168.50.103
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 16:33 CEST
Nmap scan report for 192.168.50.103
Host is up (0.00057s latency).
Not shown: 991 closed tcp ports (reset)
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
49159/tcp open  unknown
MAC Address: 08:00:27:80:3E:92 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.85 seconds
```

Ripetendo i passaggi troveremo le informazioni della macchina Windows.
In questa immagine l'output con l'opzione Syn scan.

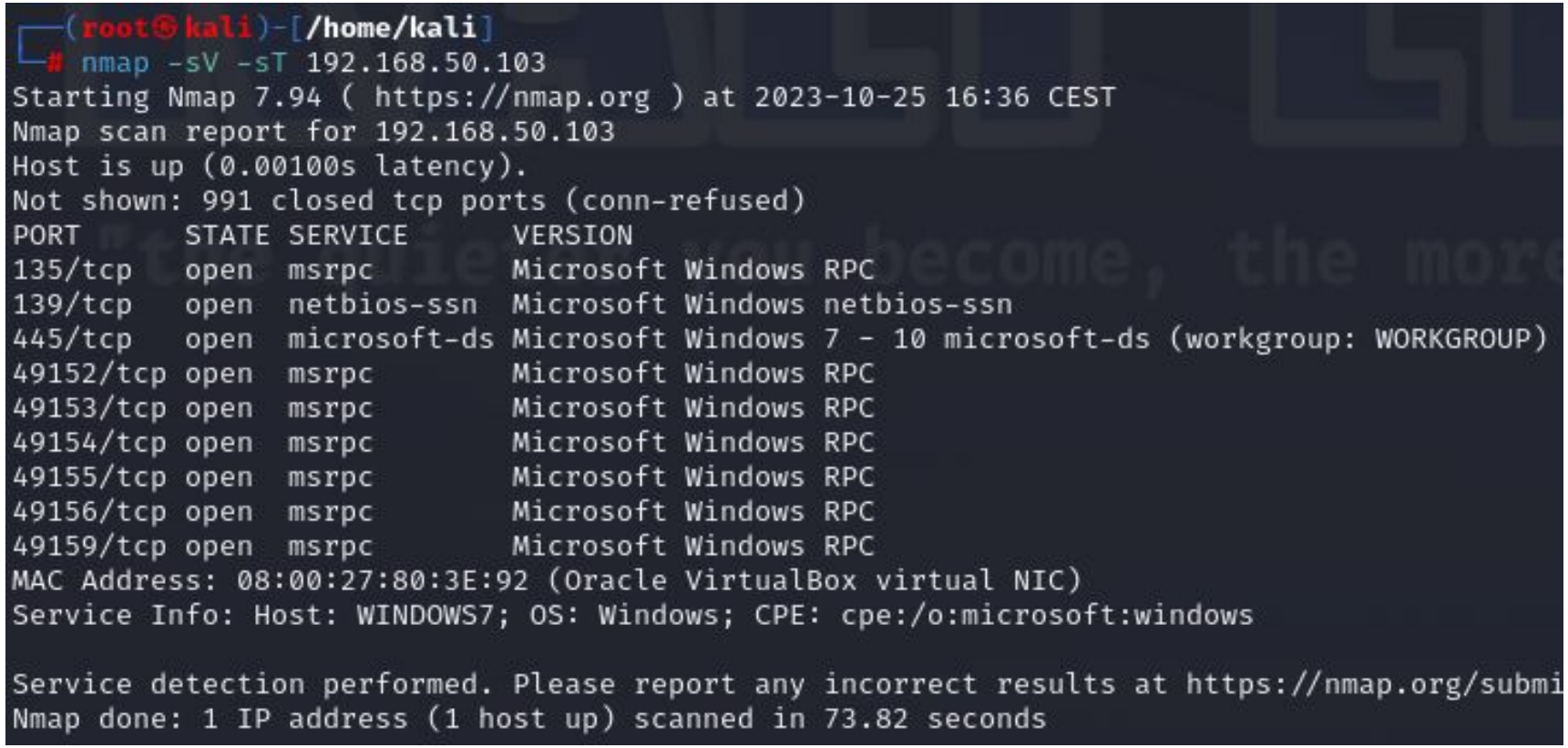


In questa immagine l'output con l'opzione di scansione TCP Control su macchina Windows.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -Pn -O 192.168.50.103
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 16:35 CEST
Nmap scan report for 192.168.50.103
Host is up (0.0011s latency).
Not shown: 991 closed tcp ports (reset)
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
49159/tcp open  unknown
MAC Address: 08:00:27:80:3E:92 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:
/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
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 15.44 seconds
```

In questa immagine l'output con l'opzione di scansione Os fingerprint con cui scopriamo il sistema operativo in uso dalla macchina Windows.



In questa immagine l'output con l'opzione '-sV' per effettuare la scansione della versione dei servizi sulla macchina Windows.

Grazie per l’attenzione.