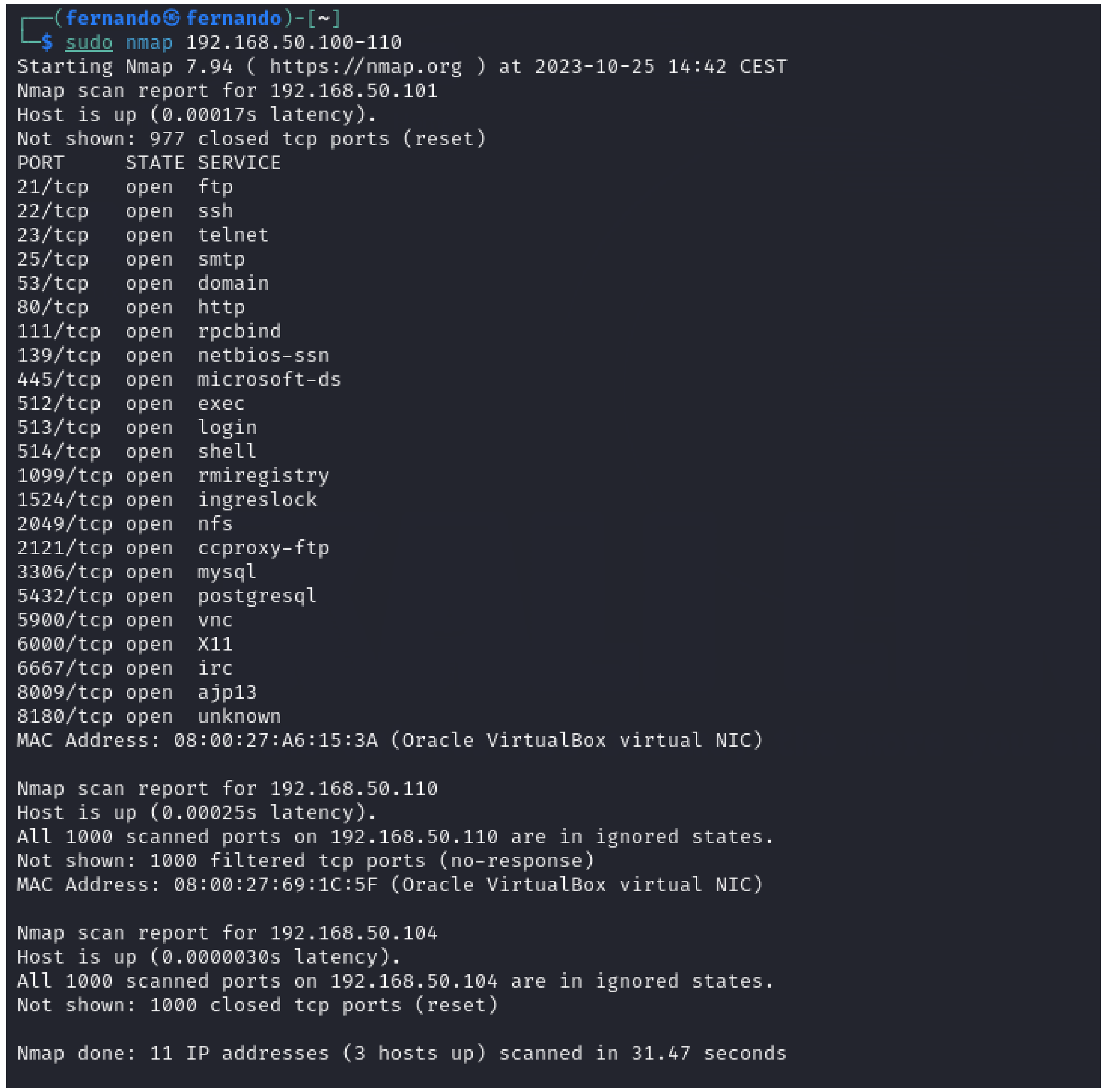
Report S5 L3

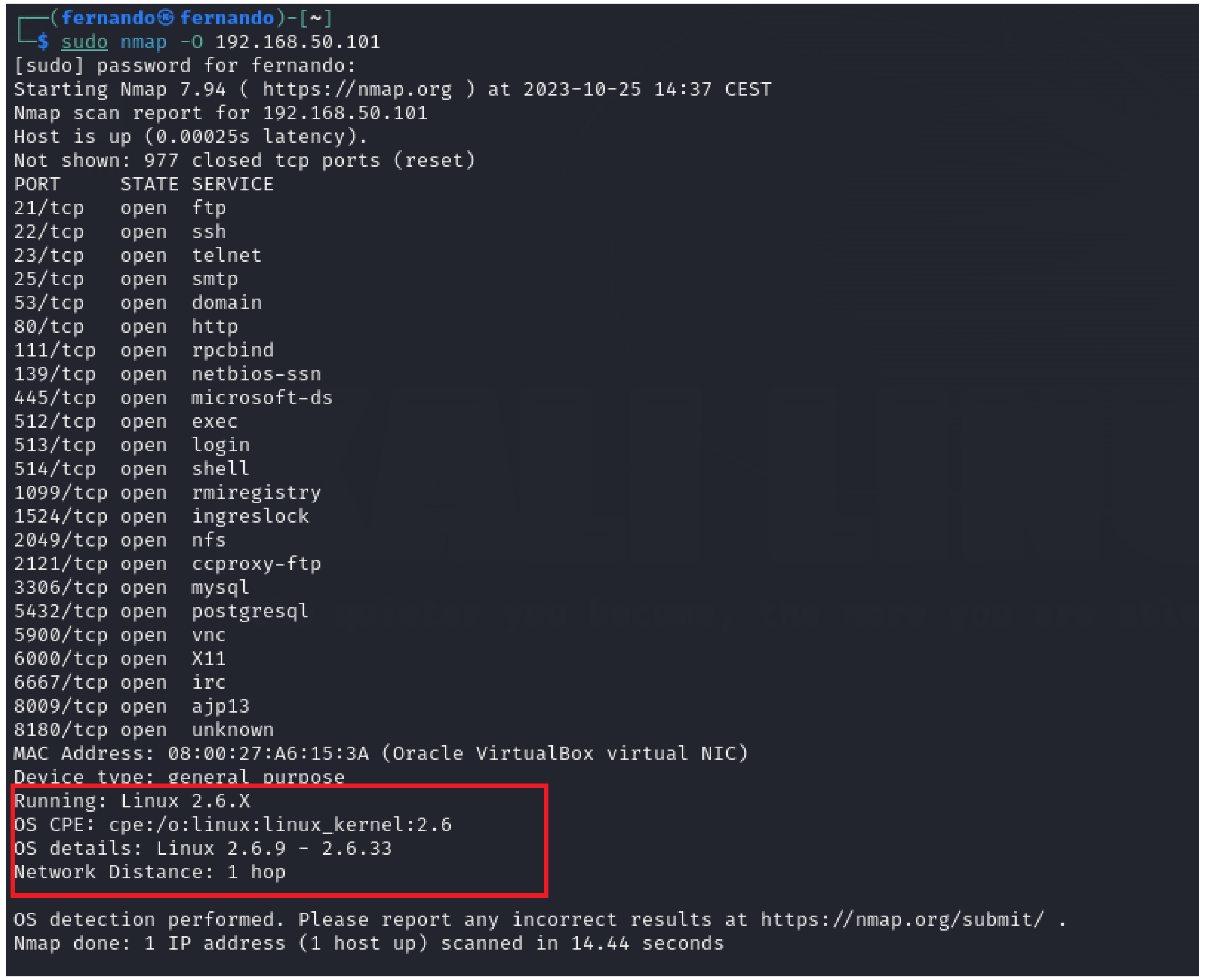
Abbiamo effettuato uno scan con nmap su un range di IP per individuare quelli disponibili. Risultano tre IP:

-192.168.50.104 che è la macchina dalle quale stiamo lavorando
-192.168.50.101
-192.168.50.110



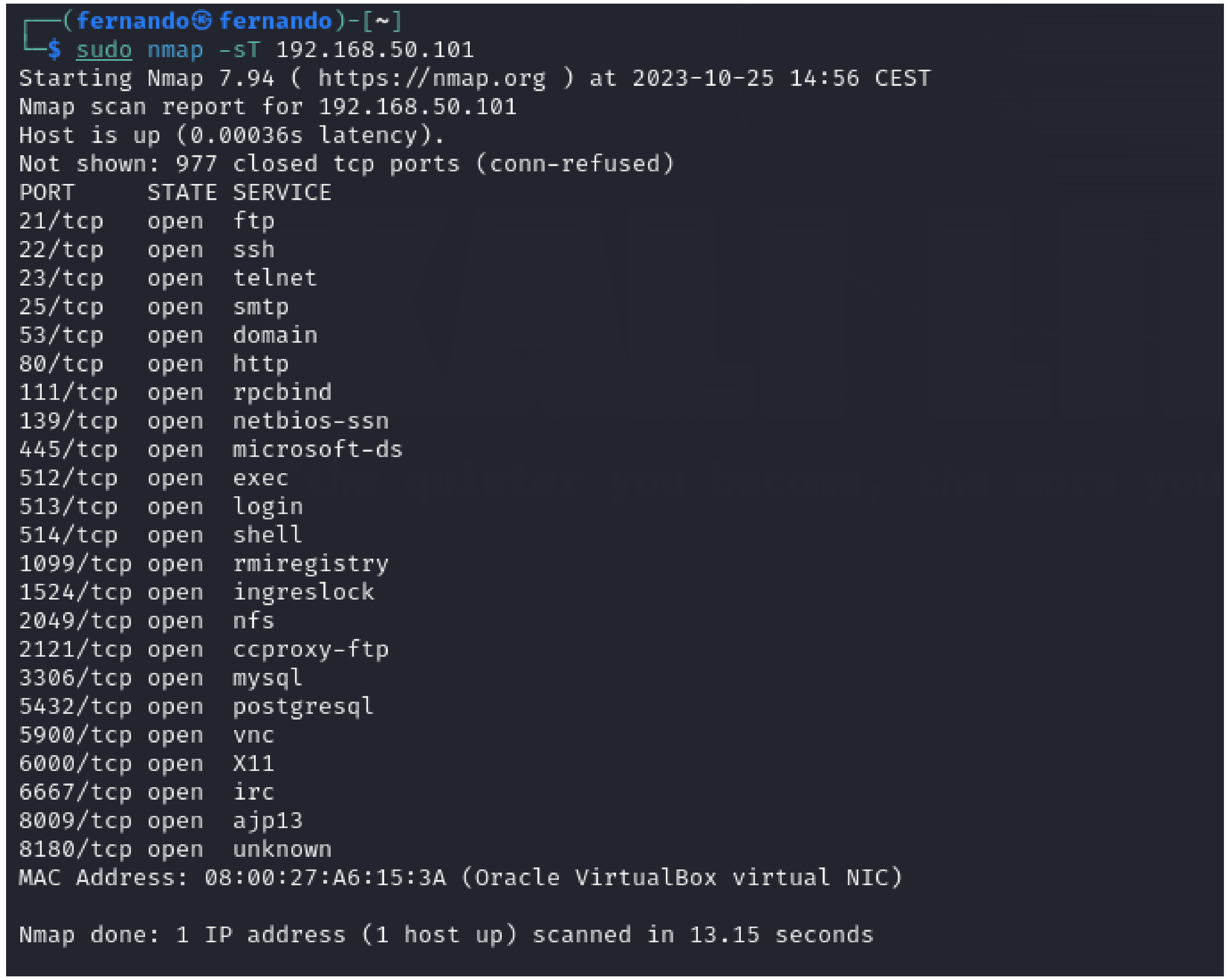
```
┌──(fernando㉿fernando)-[~]
└─$ sudo nmap 192.168.50.100-110
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 14:42 CEST
Nmap scan report for 192.168.50.101
Host is up (0.00017s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   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
MAC Address: 08:00:27:A6:15:3A (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.50.110
Host is up (0.00025s latency).
All 1000 scanned ports on 192.168.50.110 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:69:1C:5F (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.50.104
Host is up (0.0000030s latency).
All 1000 scanned ports on 192.168.50.104 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 11 IP addresses (3 hosts up) scanned in 31.47 seconds
```

Facendo un nmap -O 192.168.50.10 notiamo che il sistema operativo è Linux come mostrato in figura



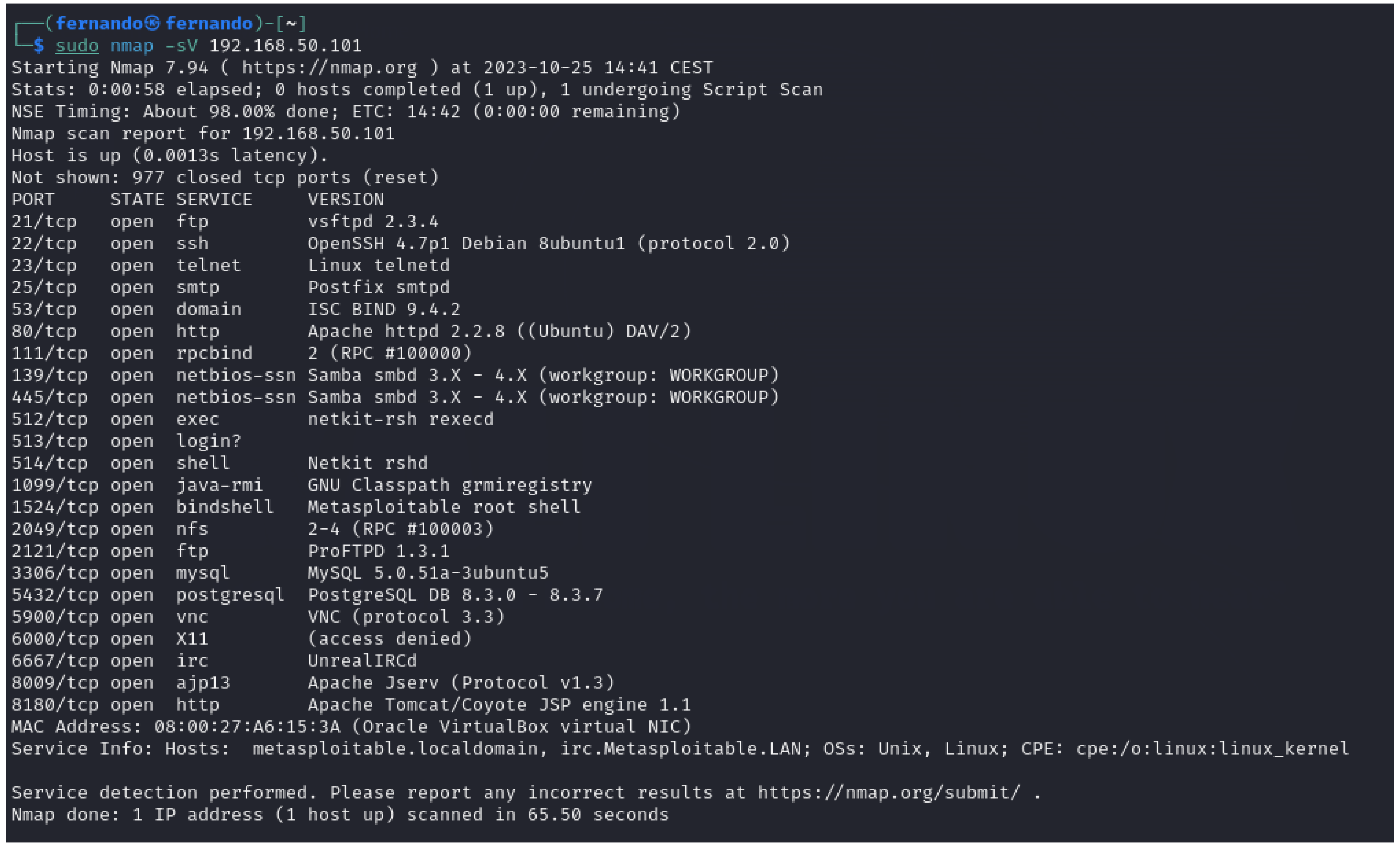
```
┌──(fernando㉿fernando)-[~]
└─$ sudo nmap -O 192.168.50.101
[sudo] password for fernando:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 14:37 CEST
Nmap scan report for 192.168.50.101
Host is up (0.00025s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  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
MAC Address: 08:00:27:A6:15:3A (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
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 14.44 seconds
```

Queste sono le porte aperte trovate grazie al comando nmap -sT 192.168.50.101



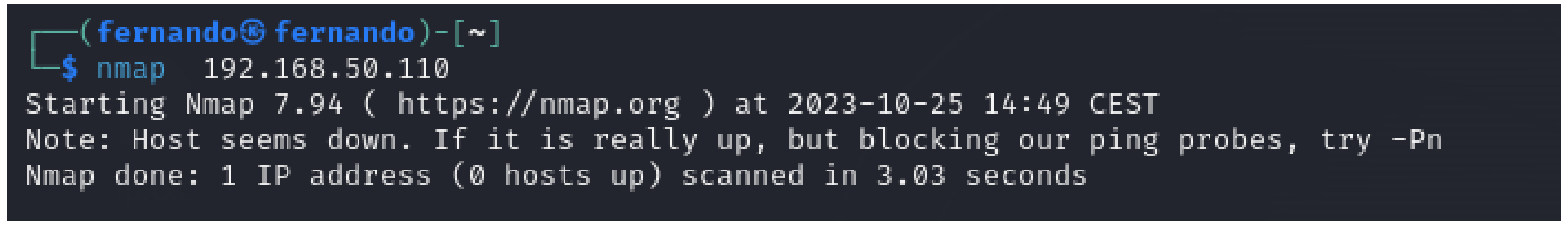
```
┌──(fernando㉿fernando)-[~]
└─$ sudo nmap -sT 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 14:56 CEST
Nmap scan report for 192.168.50.101
Host is up (0.00036s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
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
MAC Address: 08:00:27:A6:15:3A (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.15 seconds
```

Queste sono le versioni dei servizi in ascolto ricavate con il comando nmap -sV 192.168.50.101



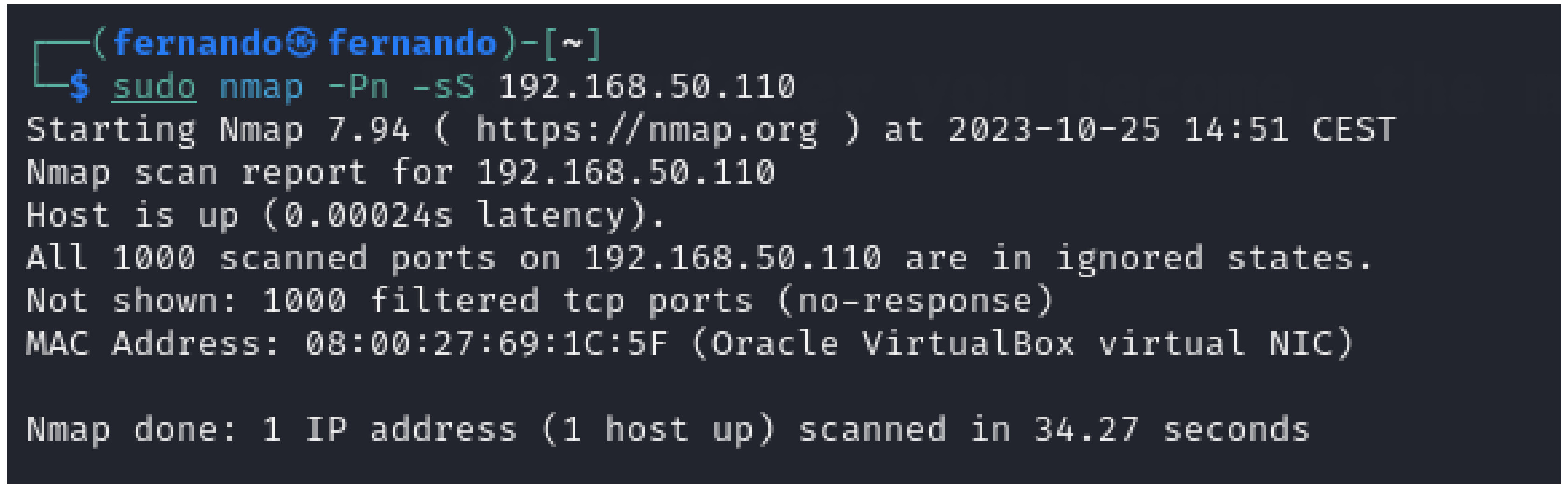
```
┌──(fernando㉿fernando)-[~]
└─$ sudo nmap -sV 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 14:41 CEST
Stats: 0:00:58 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.00% done; ETC: 14:42 (0:00:00 remaining)
Nmap scan report for 192.168.50.101
Host is up (0.0013s latency).
Not shown: 977 closed tcp ports (reset)
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
MAC Address: 08:00:27:A6:15:3A (Oracle VirtualBox virtual NIC)
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 65.50 seconds
```

Provando a scansionare il secondo IP trovato
nmap ci avverte che potrebbe essere bloccato
il protocollo ICMP quindi di fare una prova con
l’opzione -Pn che evita di fare il ping all’IP indicato



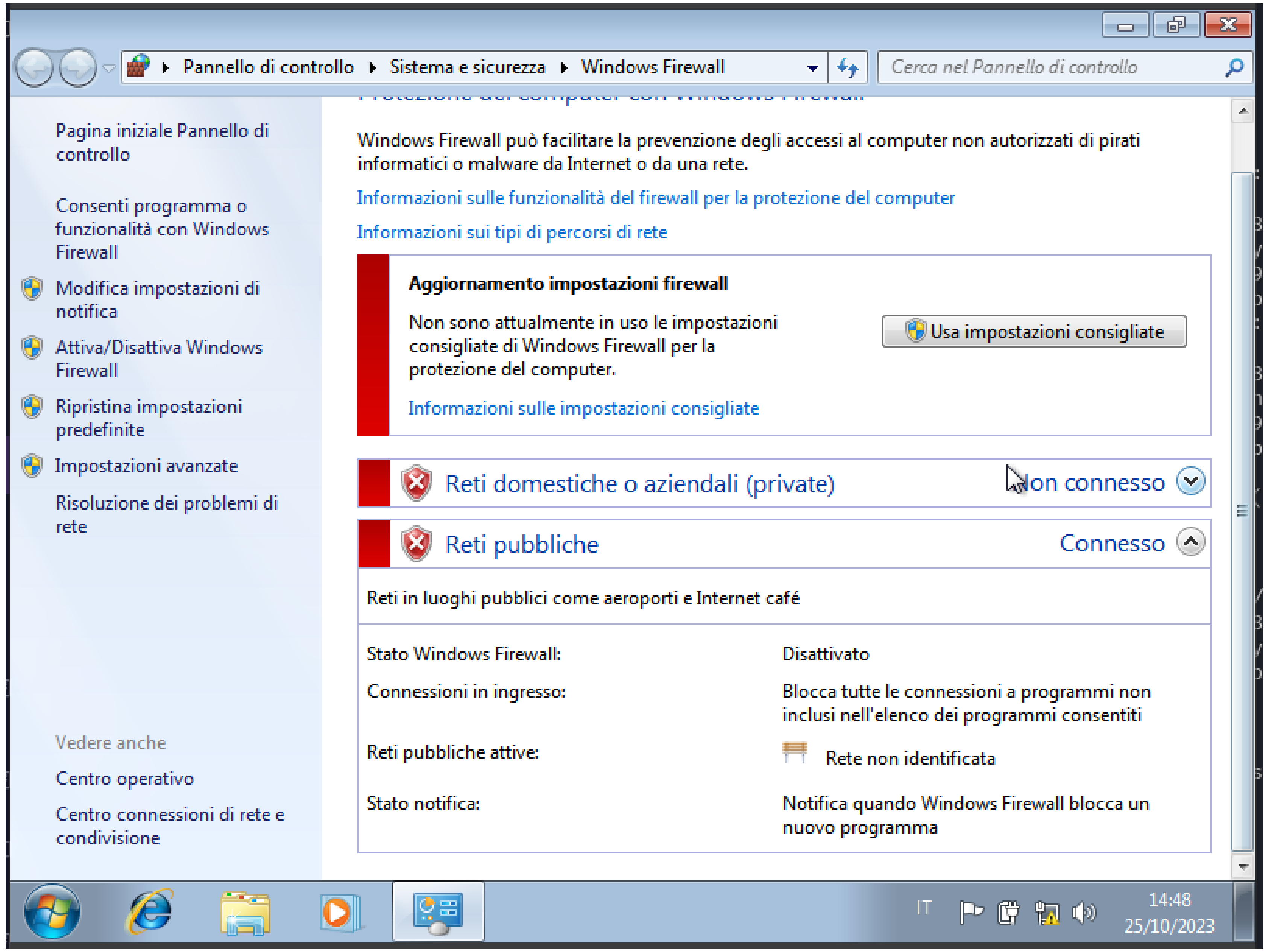
```
┌──(fernando㉿fernando)-[~]
└─$ nmap  192.168.50.110
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 14:49 CEST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.03 seconds
```

Con il comando -Pn notiamo che tutte
le porte testate non danno risposta



```
┌──(fernando㉿fernando)-[~]
└─$ sudo nmap -Pn -sS 192.168.50.110
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 14:51 CEST
Nmap scan report for 192.168.50.110
Host is up (0.00024s latency).
All 1000 scanned ports on 192.168.50.110 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:69:1C:5F (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 34.27 seconds
```

Ai fini del test ho disattivato il Firewall di Windows 7 (che è la macchina che risponde all'IP 192.168.50.110)


Pannello di controllo ▸ Sistema e sicurezza ▸ Windows Firewall
Cerca nel Pannello di controllo
Pagina iniziale Pannello di controllo
Consenti programma o funzionalità con Windows Firewall
Modifica impostazioni di notifica
Attiva/Disattiva Windows Firewall
Ripristina impostazioni predefinite
Impostazioni avanzate
Risoluzione dei problemi di rete
Vedere anche
Centro operativo
Centro connessioni di rete e condivisione
IT
14:48
25/10/2023

Protezione del computer con Windows Firewall

Windows Firewall può facilitare la prevenzione degli accessi al computer non autorizzati di pirati informatici o malware da Internet o da una rete.

Informazioni sulle funzionalità del firewall per la protezione del computer

Informazioni sui tipi di percorsi di rete

Aggiornamento impostazioni firewall

Non sono attualmente in uso le impostazioni consigliate di Windows Firewall per la protezione del computer.

Usa impostazioni consigliate

Informazioni sulle impostazioni consigliate

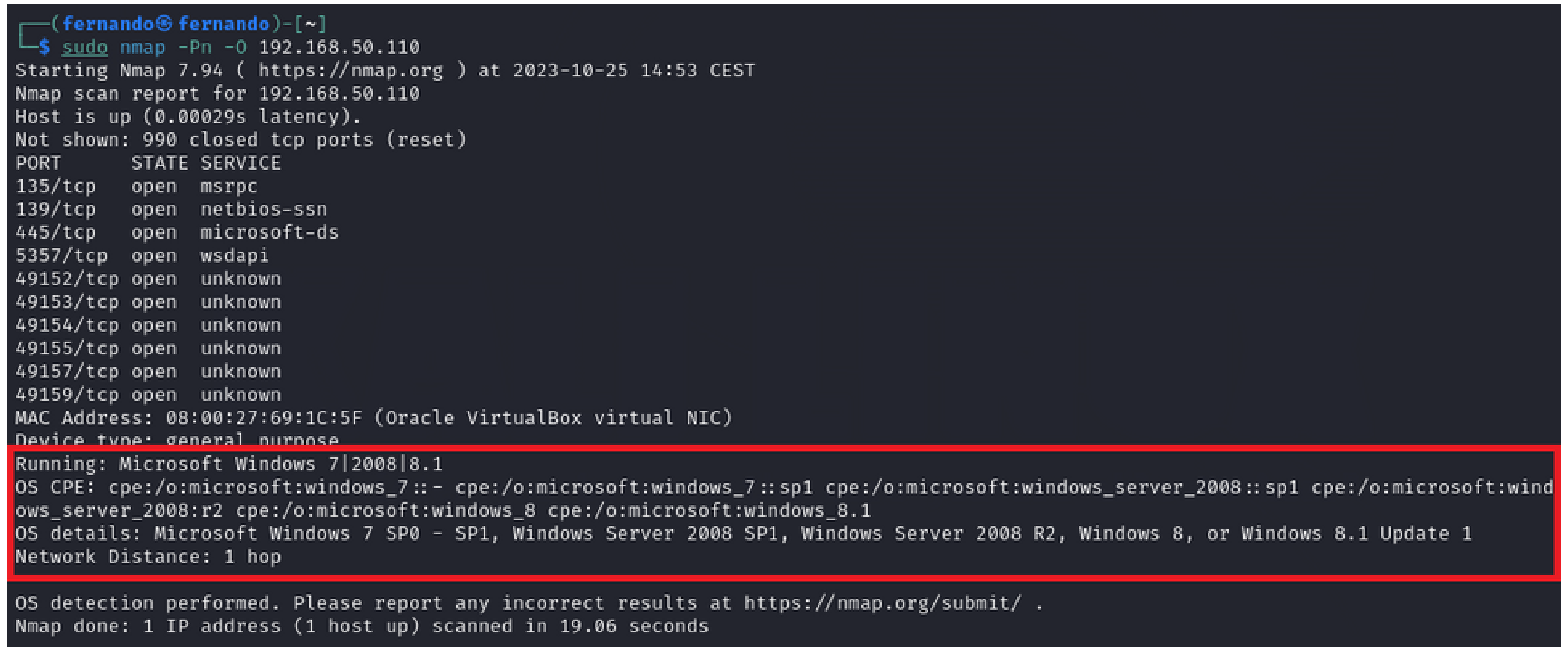
Reti domestiche o aziendali (private) — Non connesso

Reti pubbliche — Connesso

Reti in luoghi pubblici come aeroporti e Internet café

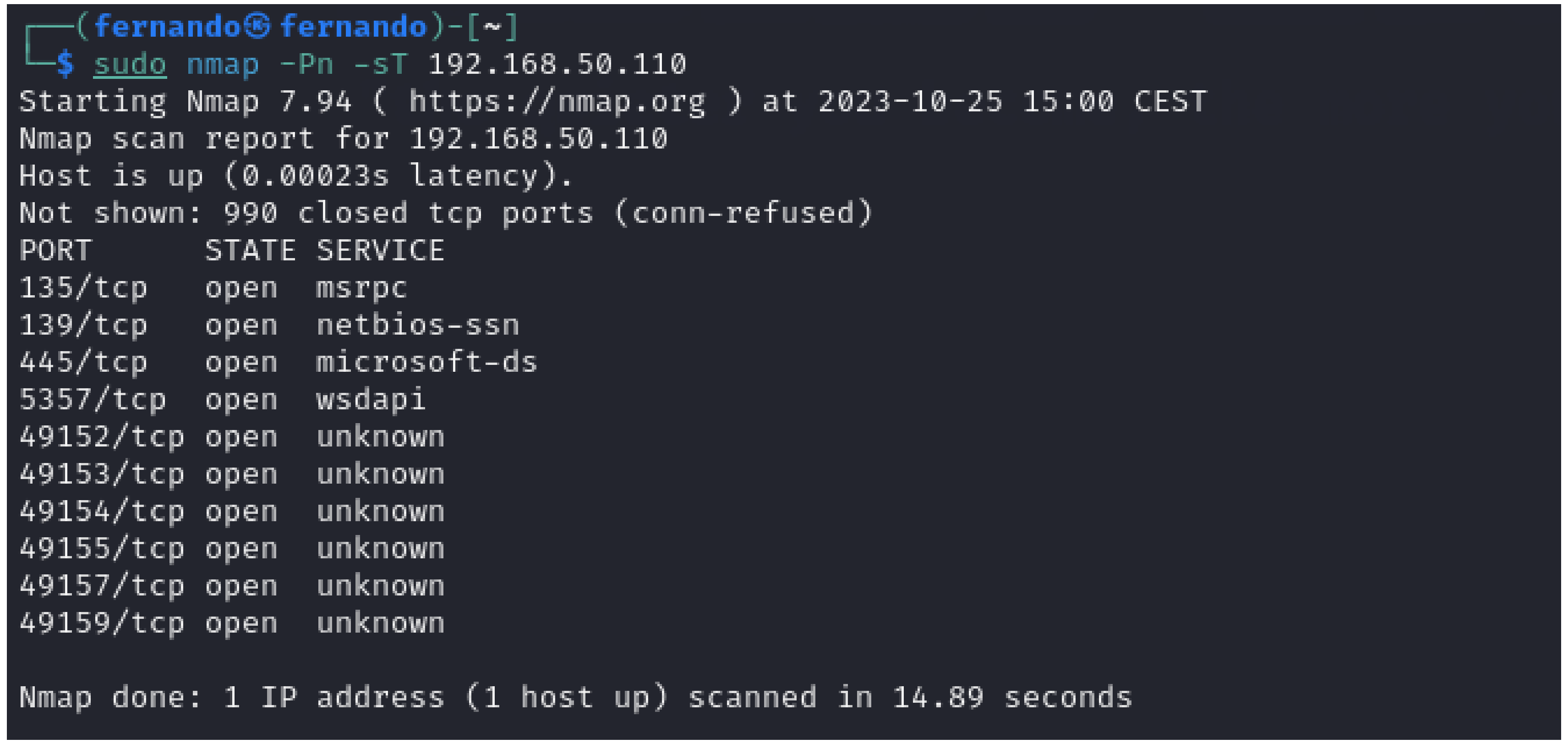
Stato Windows Firewall:	Disattivato
Connessioni in ingresso:	Blocca tutte le connessioni a programmi non inclusi nell'elenco dei programmi consentiti
Reti pubbliche attive:	Rete non identificata
Stato notifica:	Notifica quando Windows Firewall blocca un nuovo programma

Così facendo possiamo notare utilizzando i comandi precedentemente usati che il sitema operativo è Windows



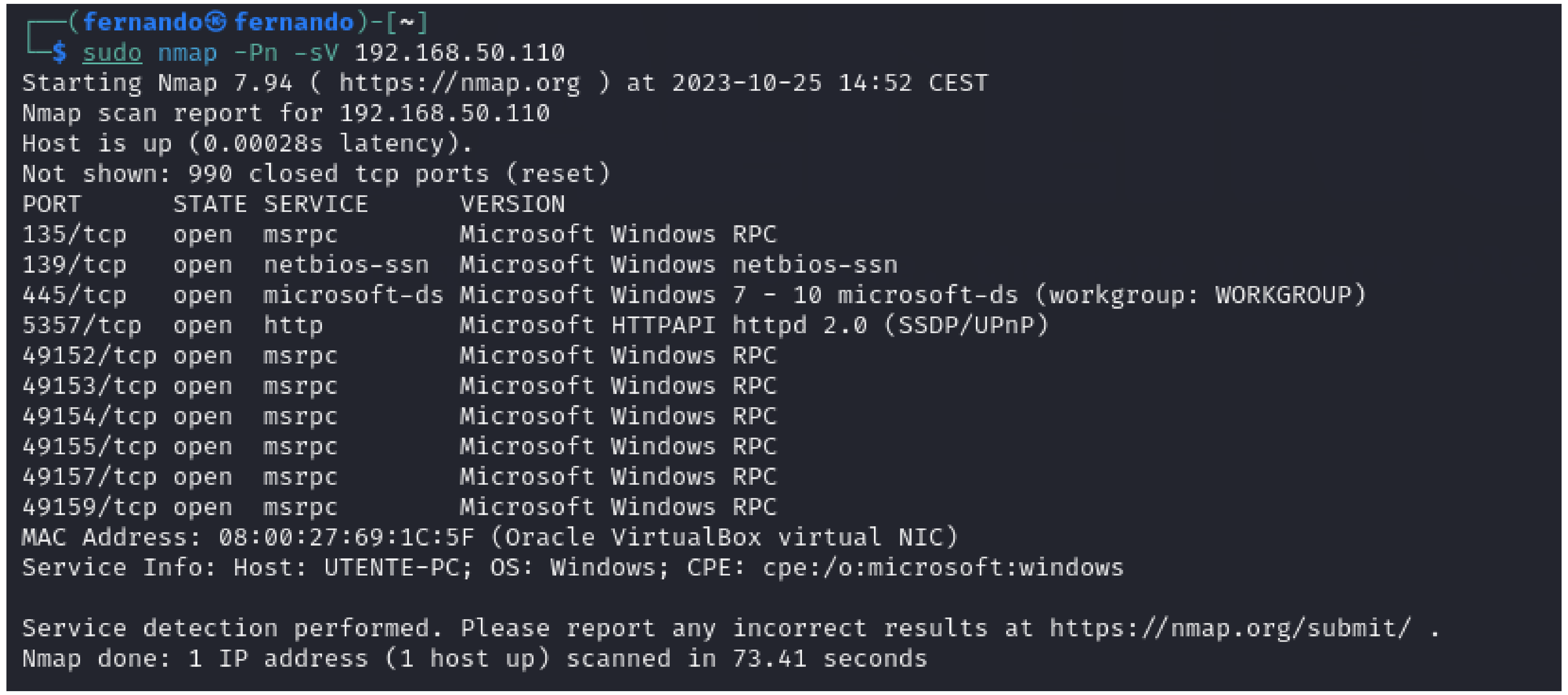
```
┌──(fernando㉿fernando)-[~]
└─$ sudo nmap -Pn -O 192.168.50.110
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 14:53 CEST
Nmap scan report for 192.168.50.110
Host is up (0.00029s latency).
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsdapi
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49157/tcp open  unknown
49159/tcp open  unknown
MAC Address: 08:00:27:69:1C:5F (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:wind
ows_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 19.06 seconds
```

Le porte aperte sono:



```
┌──(fernando㉿fernando)-[~]
└─$ sudo nmap -Pn -sT 192.168.50.110
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 15:00 CEST
Nmap scan report for 192.168.50.110
Host is up (0.00023s latency).
Not shown: 990 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsdapi
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49157/tcp open  unknown
49159/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 14.89 seconds
```

Servizi in ascolto con versione:



```
┌──(fernando㉿fernando)-[~]
└─$ sudo nmap -Pn -sV 192.168.50.110
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 14:52 CEST
Nmap scan report for 192.168.50.110
Host is up (0.00028s latency).
Not shown: 990 closed tcp ports (reset)
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)
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
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
49157/tcp open  msrpc        Microsoft Windows RPC
49159/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:69:1C:5F (Oracle VirtualBox virtual NIC)
Service Info: Host: UTENTE-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 73.41 seconds
```