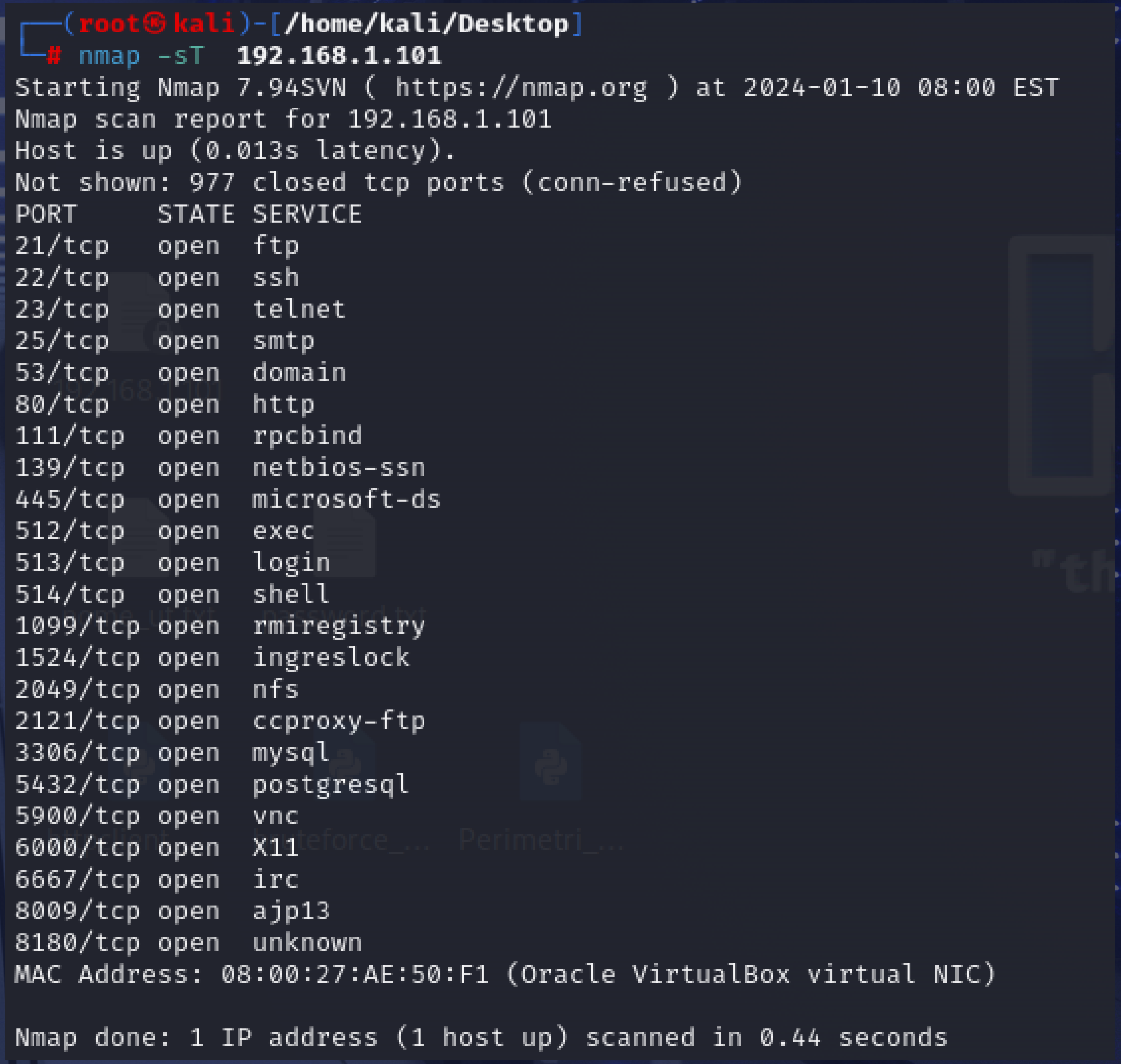
TARGET: METASPOITABLE

-sT=TCP connect

Usa SYN-SYN/ACK-ACK
Molto invasivo per questo motivo, causando molto rumore e aumentando il rischio di essere scoperti.

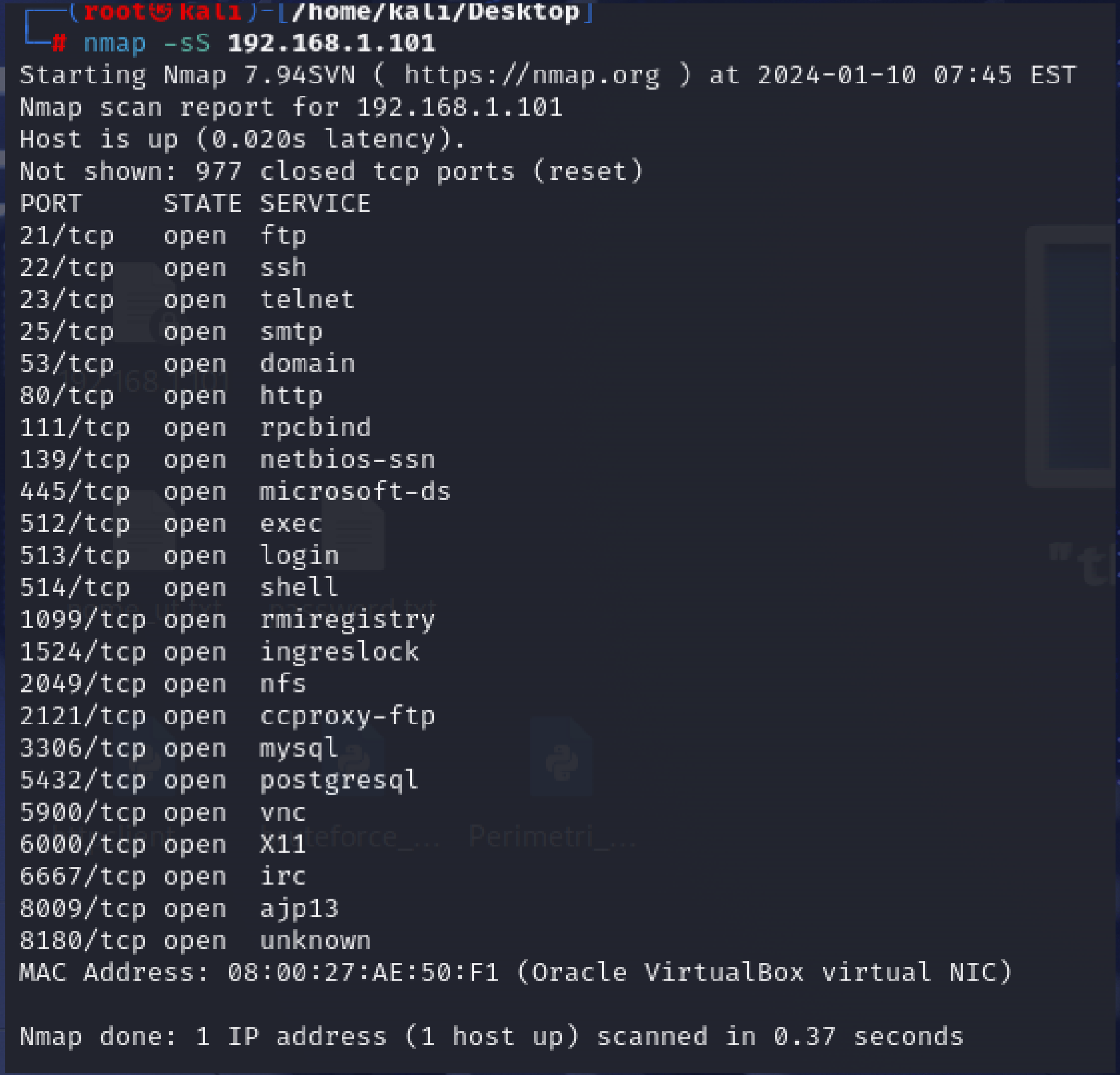


```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nmap -sT  192.168.1.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-10 08:00 EST
Nmap scan report for 192.168.1.101
Host is up (0.013s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  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:AE:50:F1 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.44 seconds
```

-sS=Syn Scan

Utilizzando solo il SYN, quindi invio del pacchetto, risulta una scansione poco invasiva e meno rumorosa.

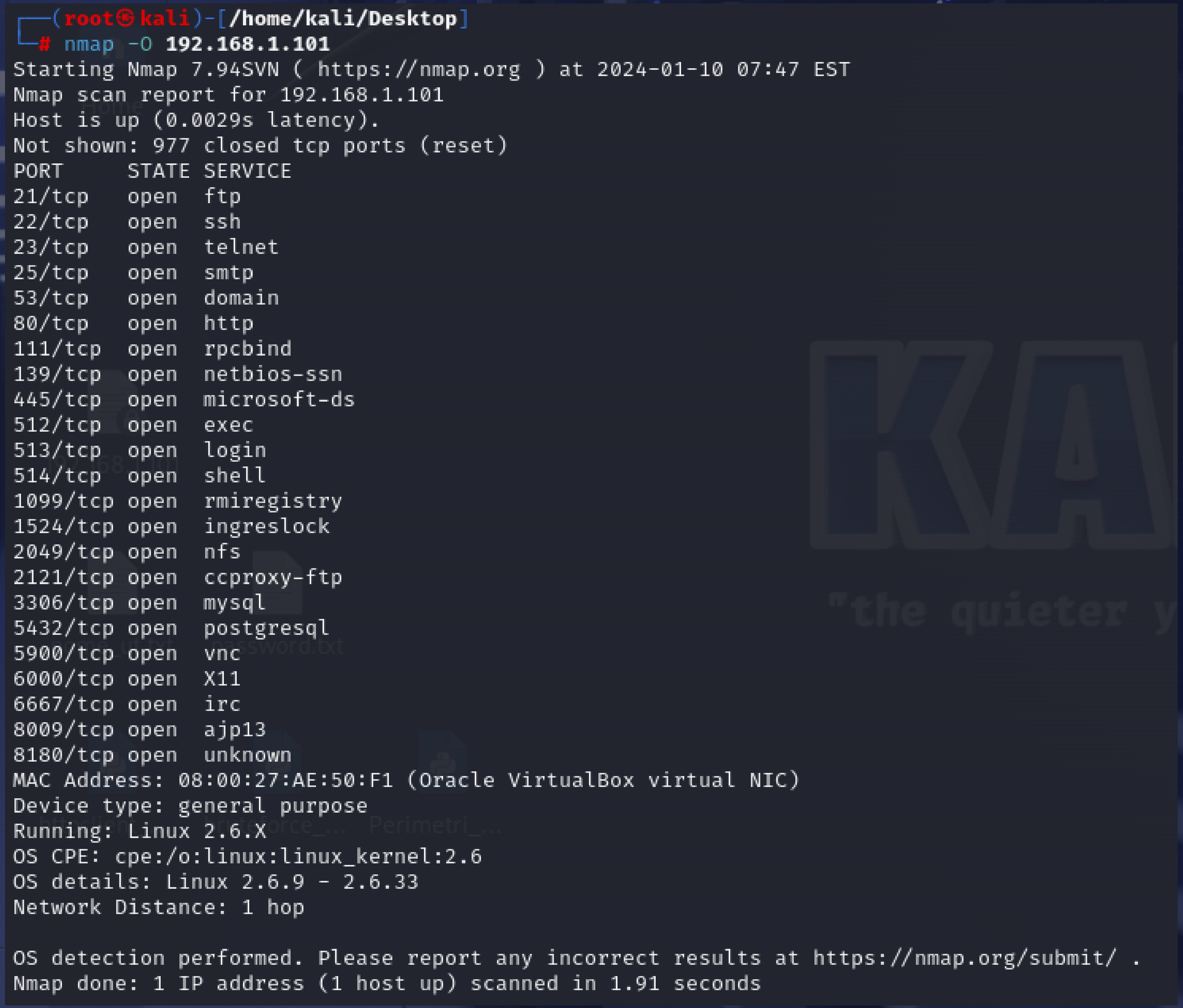


```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nmap -sS 192.168.1.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-10 07:45 EST
Nmap scan report for 192.168.1.101
Host is up (0.020s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   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:AE:50:F1 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.37 seconds
```

-o=OS fingerprint

Processo di identificazione del sistema operativo. Per poterlo fare bisogna agire sulle impostazioni del firewall di Windows e avviare la comunicazione con kali. Da li eseguire la scansione



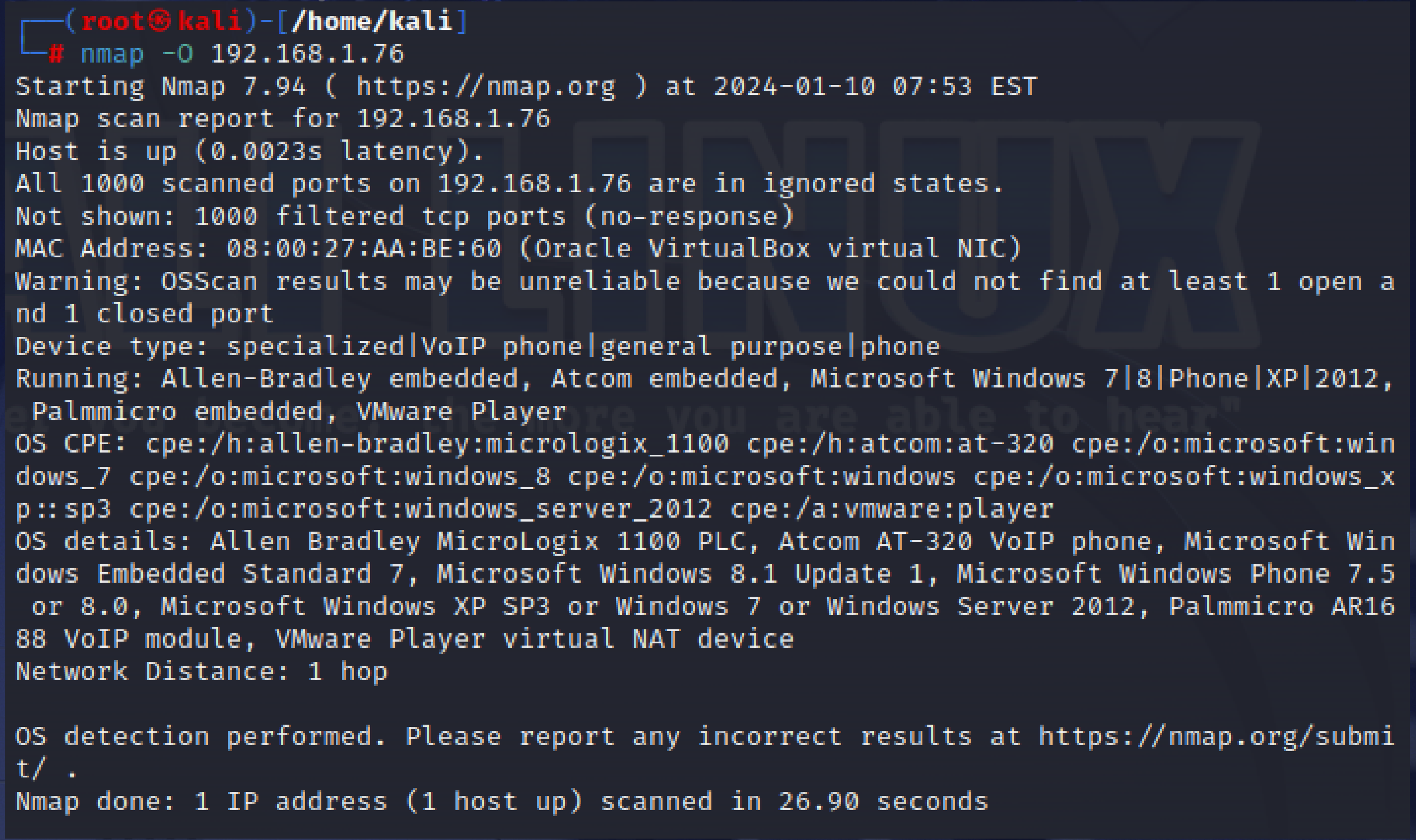
```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nmap -O 192.168.1.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-10 07:47 EST
Nmap scan report for 192.168.1.101
Host is up (0.0029s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   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:AE:50:F1 (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 1.91 seconds
```

TARGET: WINDOWS 7

-O=OS fingerprint

Scansione effettuata su windows 7
Per poterla fare bisogna agire sul Firewall,
modificando le Rules.



```
┌──(root㉿kali)-[/home/kali]
└─# nmap -O 192.168.1.76
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-10 07:53 EST
Nmap scan report for 192.168.1.76
Host is up (0.0023s latency).
All 1000 scanned ports on 192.168.1.76 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:AA:BE:60 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open a
nd 1 closed port
Device type: specialized|VoIP phone|general purpose|phone
Running: Allen-Bradley embedded, Atcom embedded, Microsoft Windows 7|8|Phone|XP|2012,
 Palmmicro embedded, VMware Player
OS CPE: cpe:/h:allen-bradley:micrologix_1100 cpe:/h:atcom:at-320 cpe:/o:microsoft:win
dows_7 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_x
p::sp3 cpe:/o:microsoft:windows_server_2012 cpe:/a:vmware:player
OS details: Allen Bradley MicroLogix 1100 PLC, Atcom AT-320 VoIP phone, Microsoft Win
dows Embedded Standard 7, Microsoft Windows 8.1 Update 1, Microsoft Windows Phone 7.5
 or 8.0, Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012, Palmmicro AR16
88 VoIP module, VMware Player virtual NAT device
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submi
t/ .
Nmap done: 1 IP address (1 host up) scanned in 26.90 seconds
```