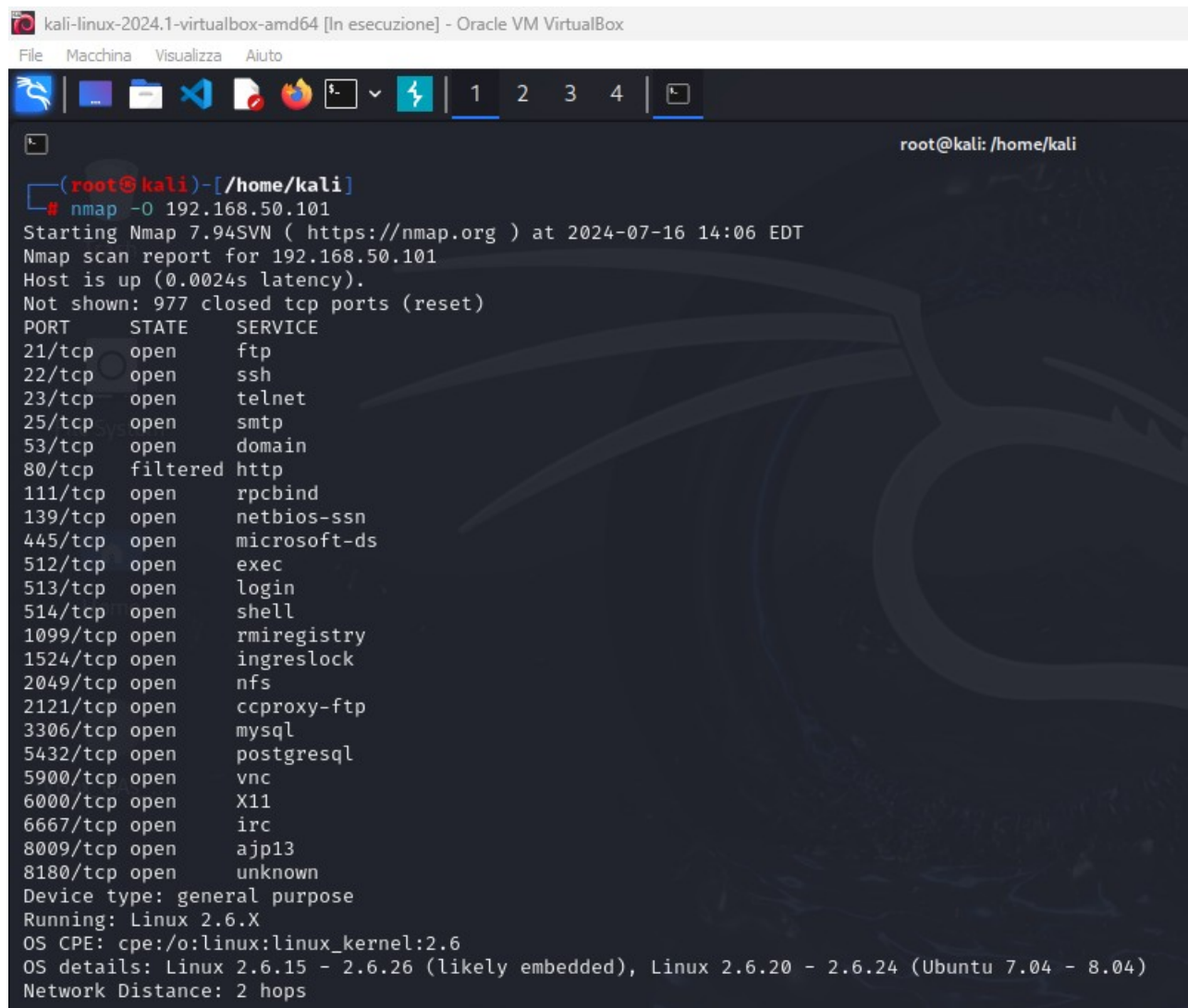


Ho eseguito i vari scan con i comandi proposti sulla macchina metasploitable2. Propongo gli screenshot.

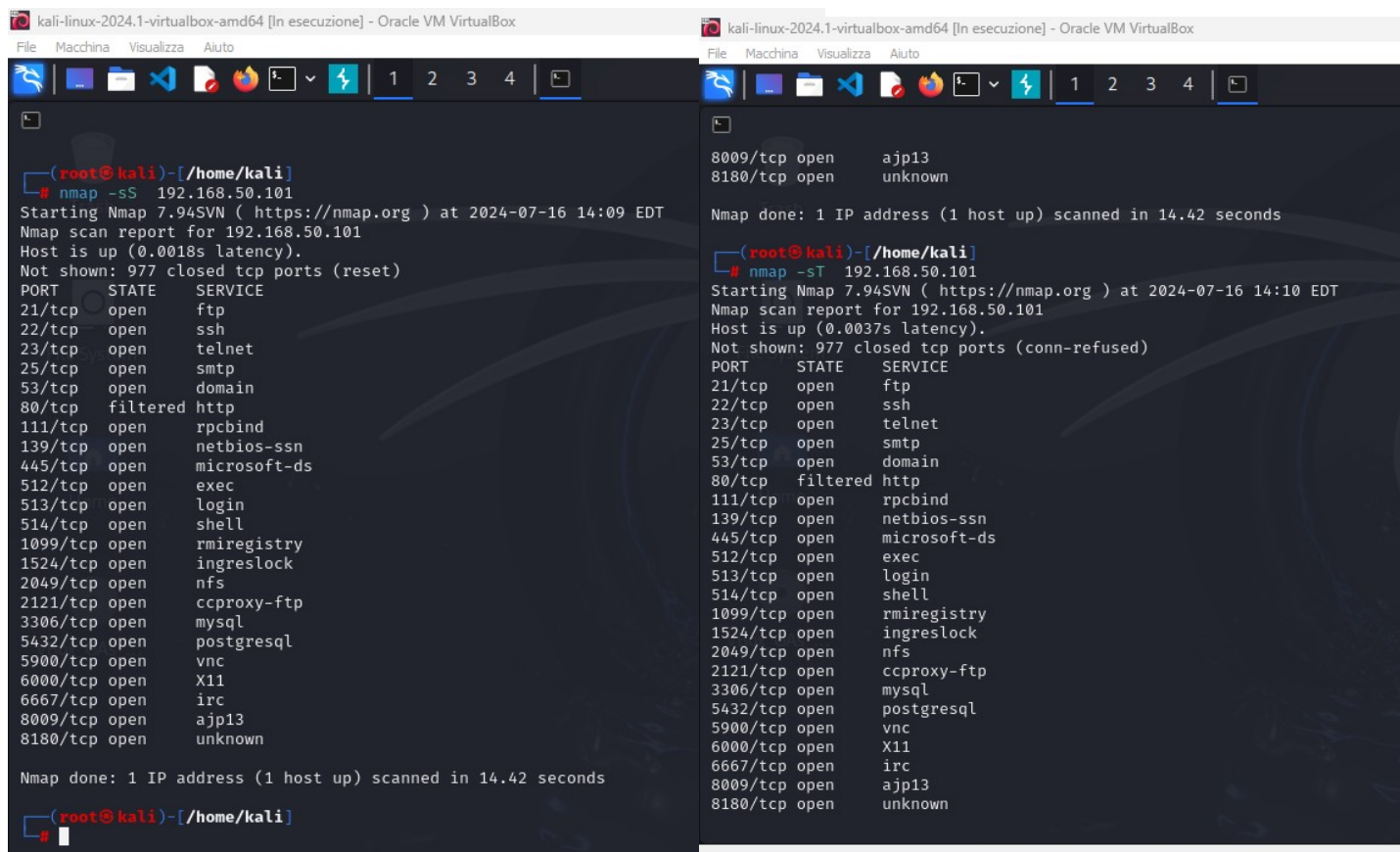


```
kali-linux-2024.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Aiuto
root@kali: /home/kali

(root@kali)~[/home/kali]
# nmap -O 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-16 14:06 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0024s 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    filtered  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
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.15 - 2.6.26 (likely embedded), Linux 2.6.20 - 2.6.24 (Ubuntu 7.04 - 8.04)
Network Distance: 2 hops
```

Questo scan ci dà info sul OS, come vediamo in basso nello screenshot.

Poi ho eseguito gli scan syn e tcp. La differenza è visibile con dei tool come wireshark che ci permettono di osservare più da vicino le request del client e la response del server così da accorgerci che la connessione tcp viene completata mentre quella syn chiusa da nmap con un pacchetto rst (reset).



Il comando -sV invece ci da qualche info più consistente fornendo le versioni dei servizi che girano

