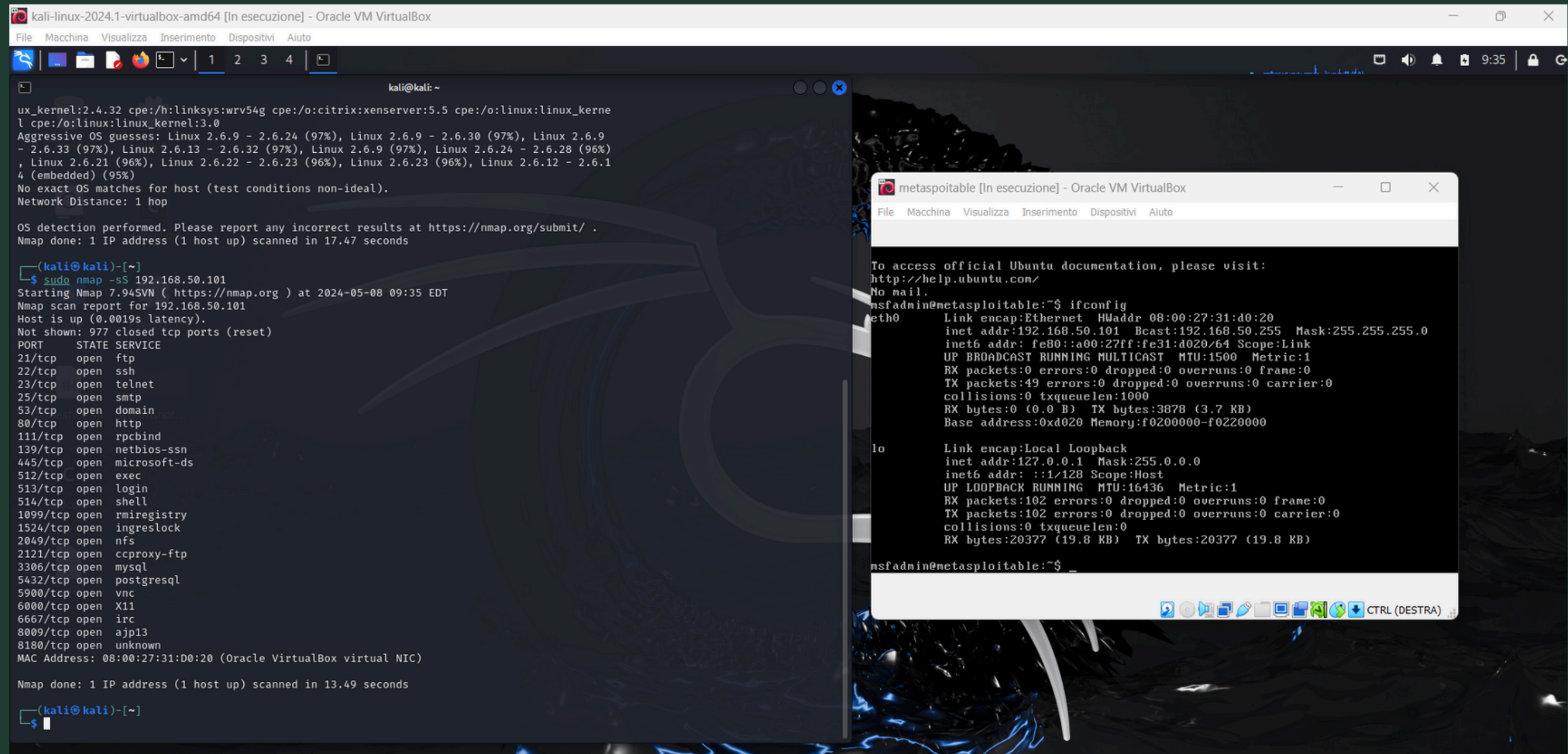
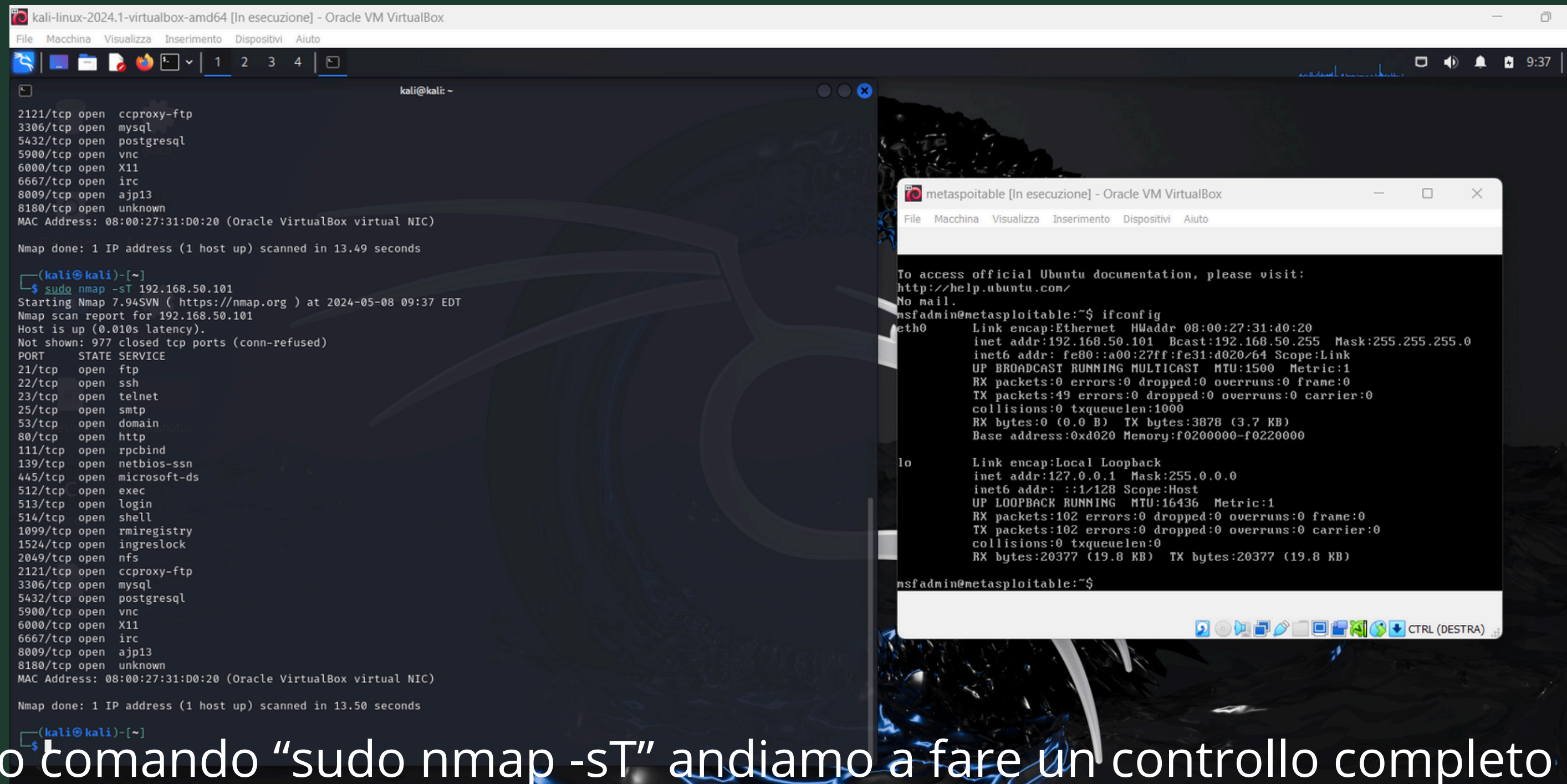


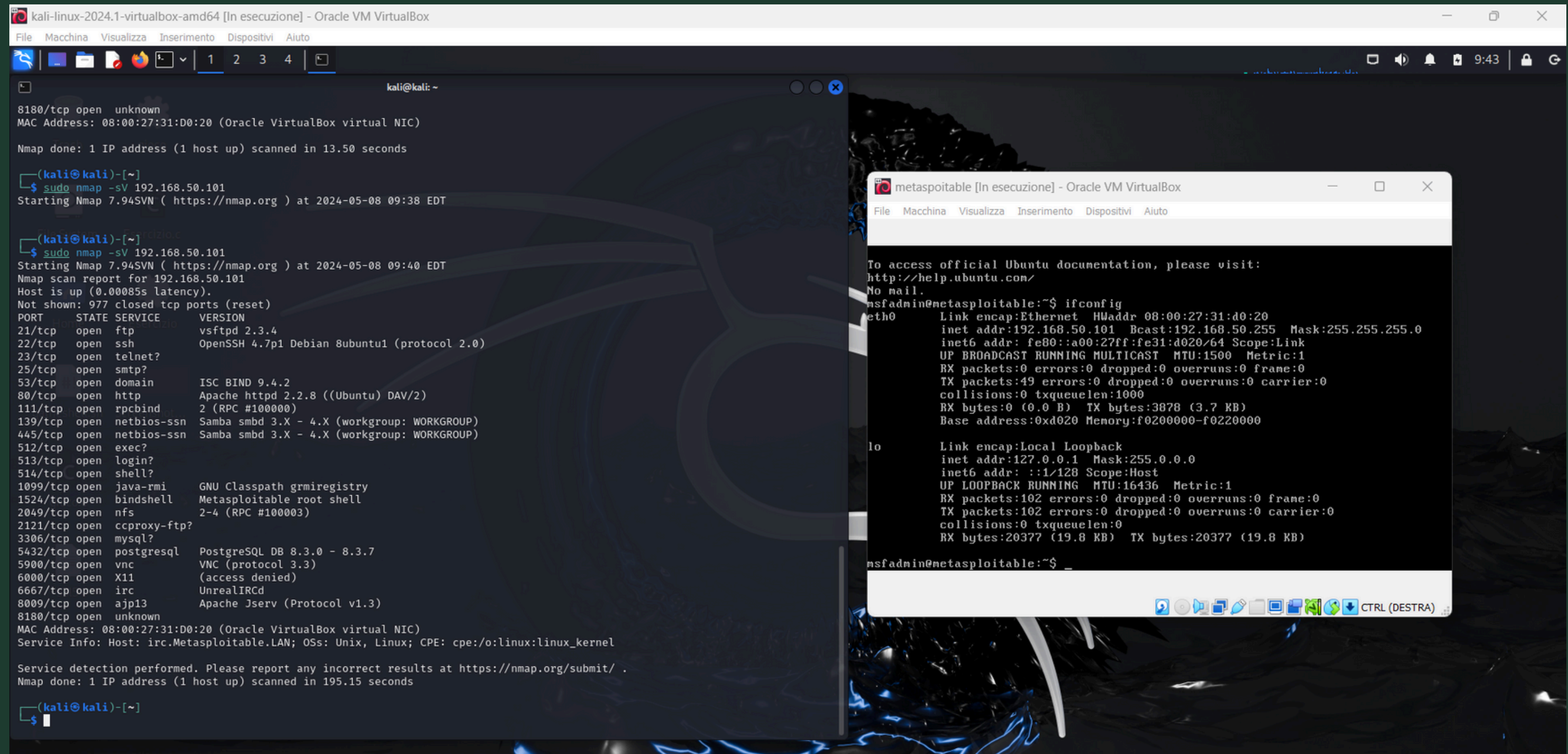
Con il primo comando “sudo nmap -o” andiamo a raccogliere le informazioni sul sistema operativo che ci interessa in questo caso di metasploitable



Con il secondo comando “sudo nmap -sS” andiamo a mandare dei pacchetti syn solo per vedere la macchina ci risponde



Con il terzo comando “sudo nmap -sT” andiamo a fare un controllo completo sul protocollo TCP



Con il quarto comando “sudo nmap -sV” andiamo a vedere quali sono le porte aperte

```
kali@kali: ~  
zsh: corrupt history file /home/kali/.zsh_history  
(kali@kali)-[~]  
$ sudo nmap -O 192.168.50.102  
[sudo] password for kali:  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 10:54 EDT  
Nmap scan report for 192.168.50.102  
Host is up (0.0013s latency).  
All 1000 scanned ports on 192.168.50.102 are in ignored states.  
Not shown: 1000 filtered tcp ports (no-response)  
MAC Address: 08:00:27:7F:8C:F6 (Oracle VirtualBox virtual NIC)  
Too many fingerprints match this host to give specific OS details  
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 46.31 seconds  
(kali@kali)-[~]  
$
```

In questo caso con “sudo nmap -o” andiamo a raccogliere le informazioni sul sistema operativo che ci interessa in questo caso windows 7 e si può vedere che non ci da alcun risultato perché c’è il firewall che blocca il comando.


```
(kali㉿kali)-[~]  
$ sudo nmap -O 192.168.50.102  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 11:01 EDT  
Nmap scan report for 192.168.50.102  
Host is up (0.00097s 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  wsapi  
49152/tcp  open  unknown  
49153/tcp  open  unknown  
49154/tcp  open  unknown  
49155/tcp  open  unknown  
49156/tcp  open  unknown  
49157/tcp  open  unknown  
MAC Address: 08:00:27:7F:8C:F6 (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 16.42 seconds
```

Ora, avendo disabilitato il firewall e ripetendo il comando, notiamo che ci da le informazioni sul sistema operativo