Scansione Metasploitable

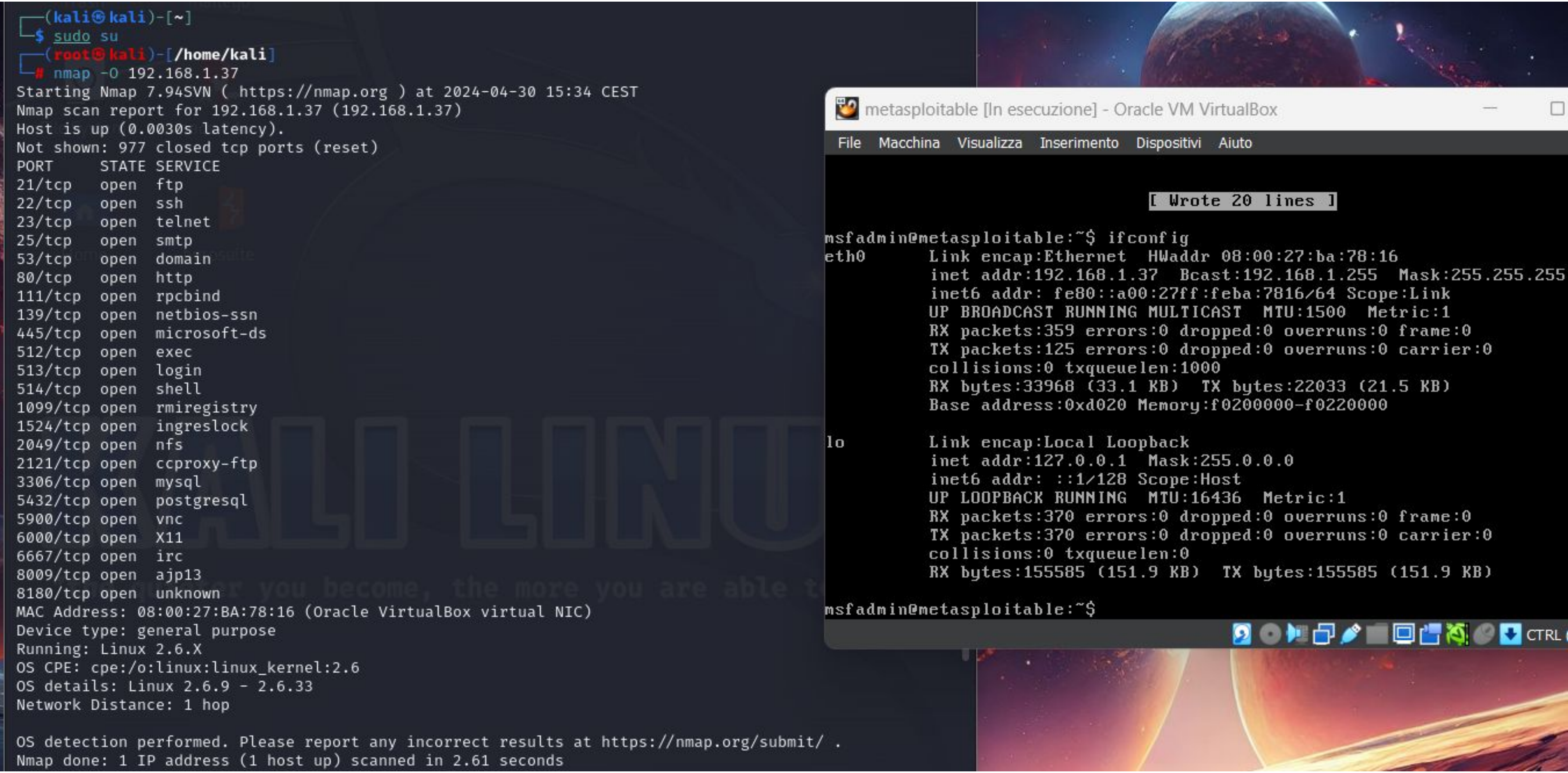
Come richiesto dalla traccia si prosegue con uno scanning di Metasploitable

-O (OS detection): Questa opzione consente a Nmap di tentare di determinare il sistema operativo del target analizzando i pacchetti di rete e le risposte dei servizi.Utilizza una serie di tecniche, come il rilevamento delle caratteristiche di implementazione del protocollo TCP/IP, per inferire il sistema operativo.È utile per comprendere la composizione e le vulnerabilità potenziali di una rete, permettendo di adottare misure di sicurezza adeguate.

-sS (TCP SYN scan): Questa opzione esegue una scansione SYN delle porte del target.
Invia un pacchetto SYN al target e analizza la risposta per determinare lo stato delle porte (aperte, chiuse o filtrate).
È una tecnica di scansione veloce e stealth, in quanto non completa la connessione TCP, ma analizza solo le risposte iniziali.

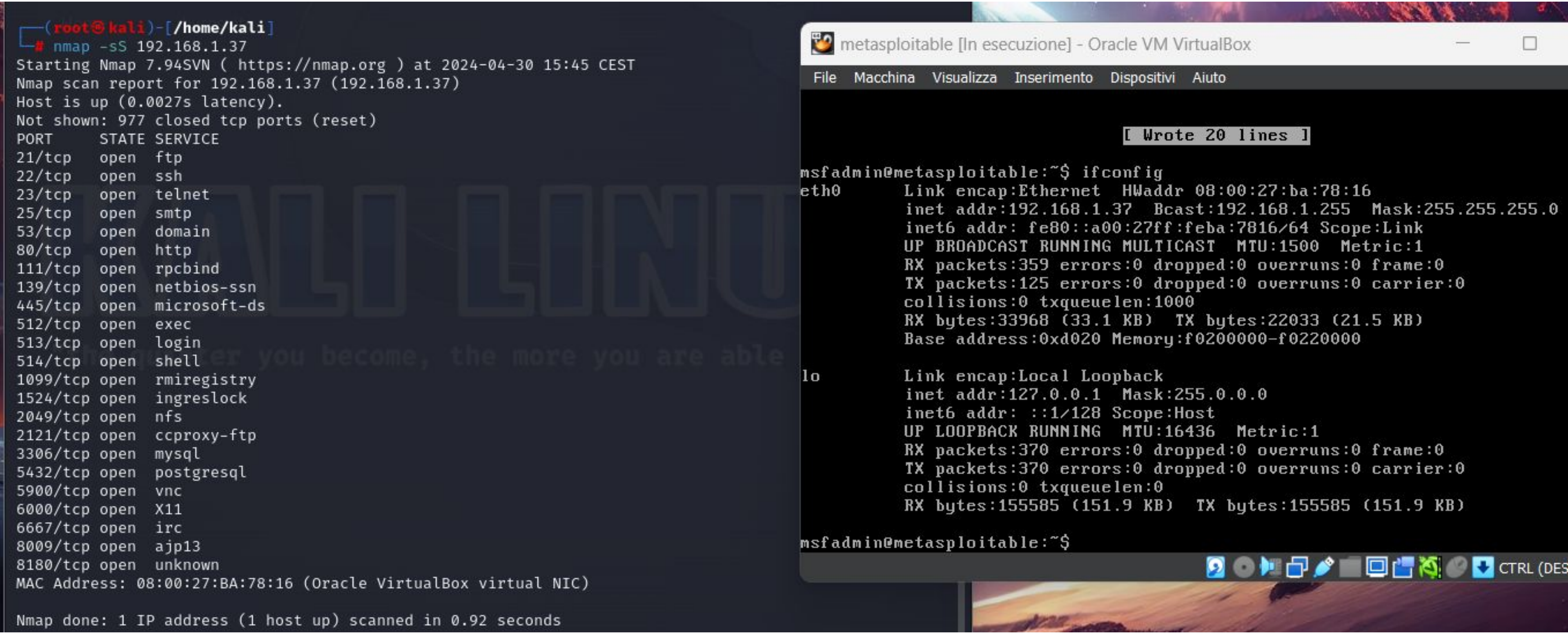
-sT (TCP connect scan): Questa opzione esegue una scansione di connessione TCP completa delle porte del target.
Nmap tenta di stabilire una connessione TCP completa con ciascuna porta del target per determinare lo stato delle porte.
È più rumoroso rispetto alla scansione SYN, poiché completa la connessione TCP con il target.

-sV (Service version detection): Questa opzione consente a Nmap di identificare le versioni dei servizi in esecuzione sul target.
Analizza le risposte dei servizi durante la scansione delle porte per identificare le versioni specifiche dei software
Fornisce informazioni utili per comprendere le configurazioni dei servizi e le vulnerabilità potenziali.



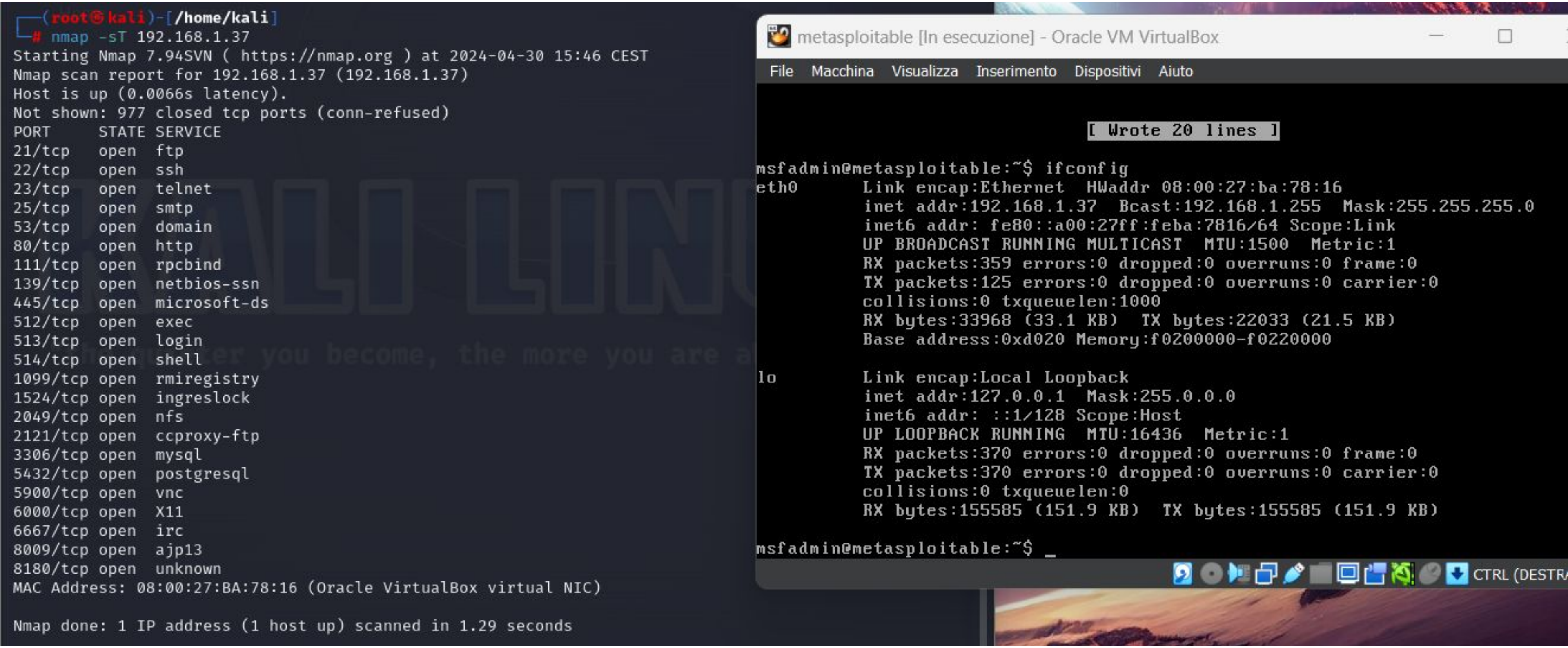
```
┌──(kali㉿kali)-[~]
└─$ sudo su
┌──(root㉿kali)-[/home/kali]
└─# nmap -O 192.168.1.37
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-30 15:34 CEST
Nmap scan report for 192.168.1.37 (192.168.1.37)
Host is up (0.0030s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   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:BA:78:16 (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 2.61 seconds
```

```
                    [ Wrote 20 lines ]

msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:ba:78:16
          inet addr:192.168.1.37  Bcast:192.168.1.255  Mask:255.255.255
          inet6 addr: fe80::a00:27ff:feba:7816/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:359 errors:0 dropped:0 overruns:0 frame:0
          TX packets:125 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:33968 (33.1 KB)  TX bytes:22033 (21.5 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:370 errors:0 dropped:0 overruns:0 frame:0
          TX packets:370 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:155585 (151.9 KB)  TX bytes:155585 (151.9 KB)

msfadmin@metasploitable:~$
```



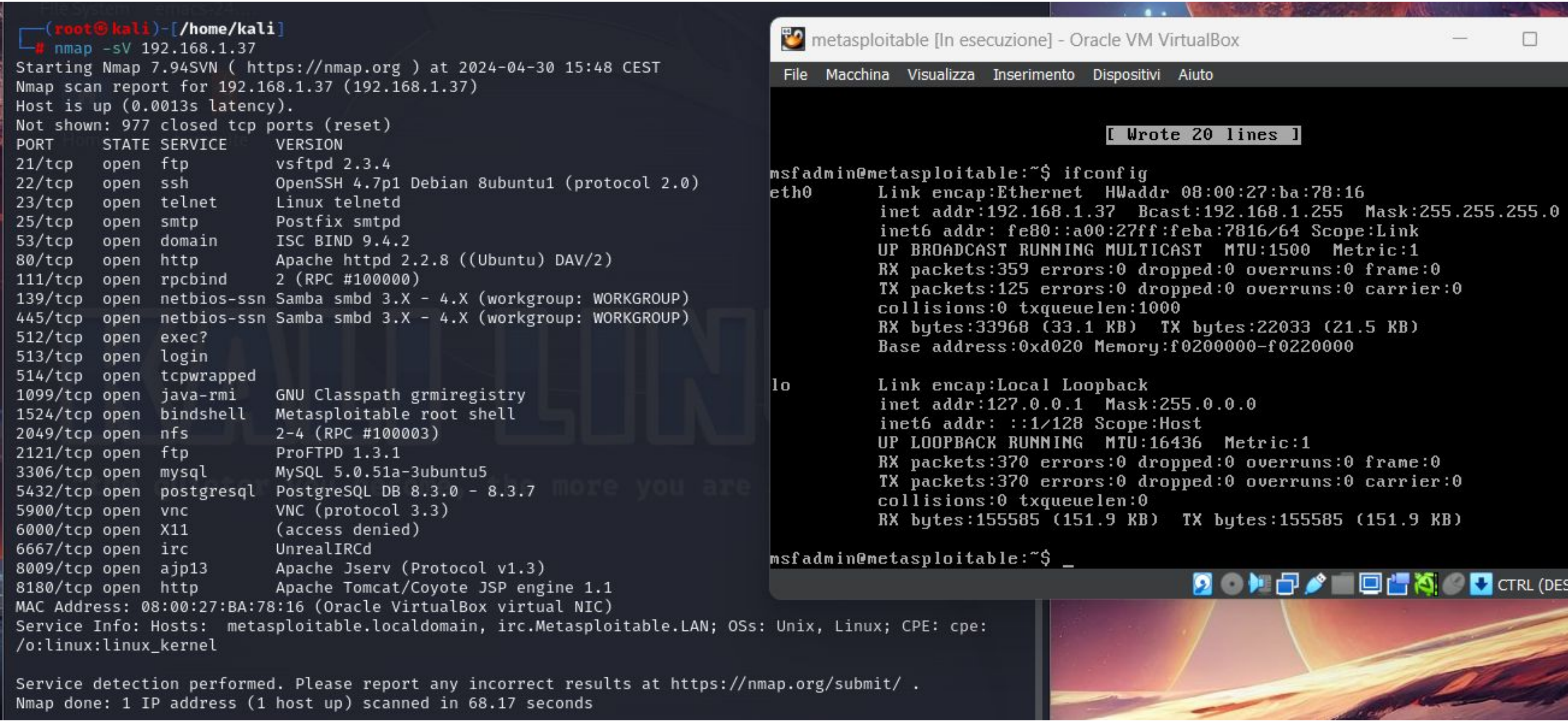
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS 192.168.1.37
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-30 15:45 CEST
Nmap scan report for 192.168.1.37 (192.168.1.37)
Host is up (0.0027s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  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:BA:78:16 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.92 seconds
```

```
                              [ Wrote 20 lines ]

msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:ba:78:16
          inet addr:192.168.1.37  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feba:7816/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:359 errors:0 dropped:0 overruns:0 frame:0
          TX packets:125 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:33968 (33.1 KB)  TX bytes:22033 (21.5 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:370 errors:0 dropped:0 overruns:0 frame:0
          TX packets:370 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:155585 (151.9 KB)  TX bytes:155585 (151.9 KB)

msfadmin@metasploitable:~$
```



```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sT 192.168.1.37
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-30 15:46 CEST
Nmap scan report for 192.168.1.37 (192.168.1.37)
Host is up (0.0066s 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:BA:78:16 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.29 seconds
```

```
                              [ Wrote 20 lines ]

msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:ba:78:16
          inet addr:192.168.1.37  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feba:7816/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:359 errors:0 dropped:0 overruns:0 frame:0
          TX packets:125 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:33968 (33.1 KB)  TX bytes:22033 (21.5 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:370 errors:0 dropped:0 overruns:0 frame:0
          TX packets:370 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:155585 (151.9 KB)  TX bytes:155585 (151.9 KB)

msfadmin@metasploitable:~$ _
```



```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.1.37
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-30 15:48 CEST
Nmap scan report for 192.168.1.37 (192.168.1.37)
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?
513/tcp  open  login
514/tcp  open  tcpwrapped
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:BA:78:16 (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 68.17 seconds
```

```
                                   [ Wrote 20 lines ]

msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:ba:78:16
          inet addr:192.168.1.37  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feba:7816/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:359 errors:0 dropped:0 overruns:0 frame:0
          TX packets:125 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:33968 (33.1 KB)  TX bytes:22033 (21.5 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:370 errors:0 dropped:0 overruns:0 frame:0
          TX packets:370 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:155585 (151.9 KB)  TX bytes:155585 (151.9 KB)

msfadmin@metasploitable:~$ _
```