

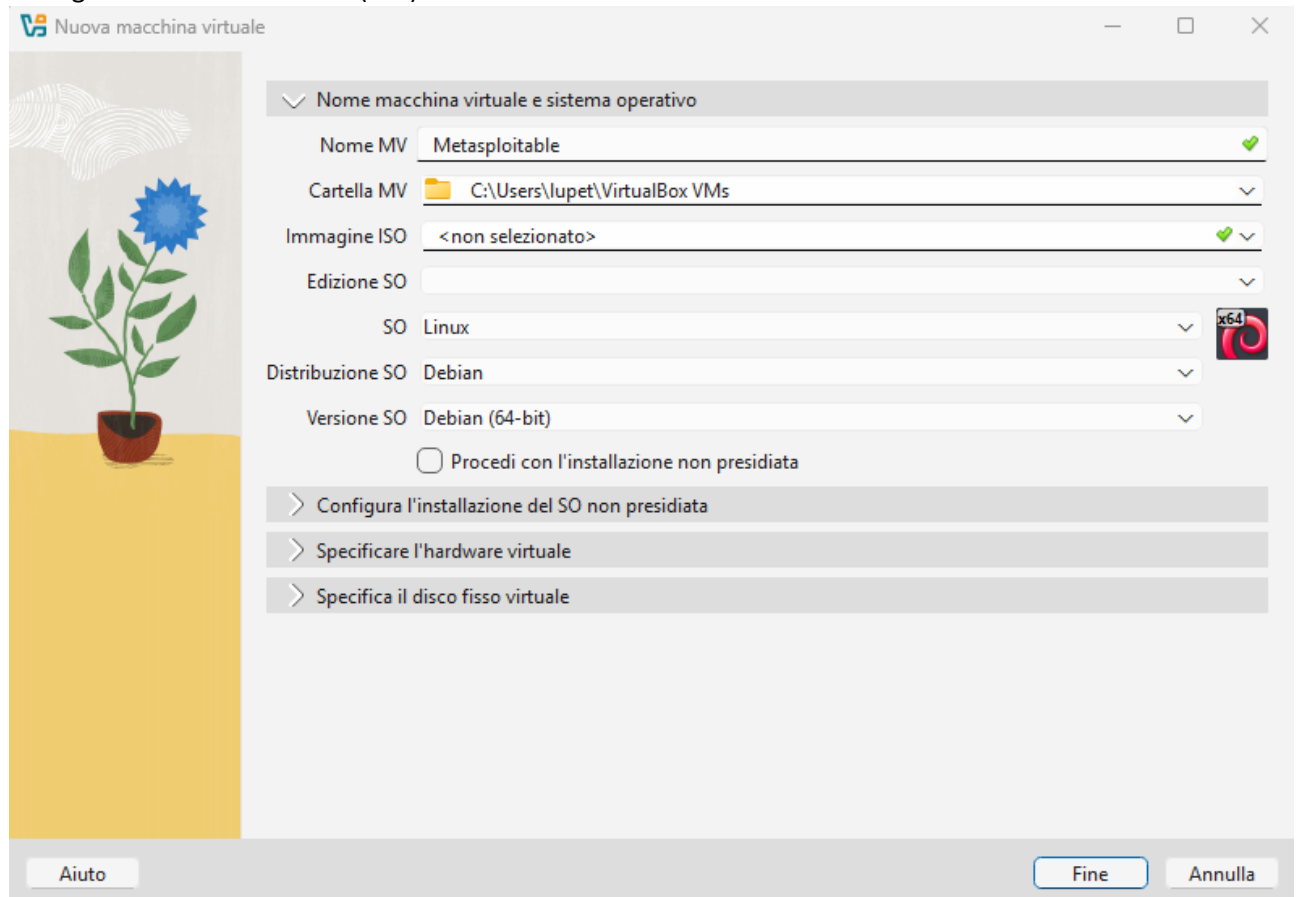
REPORT ORICCHIO ANTONIO

Macchine virtuali e Metasploitable

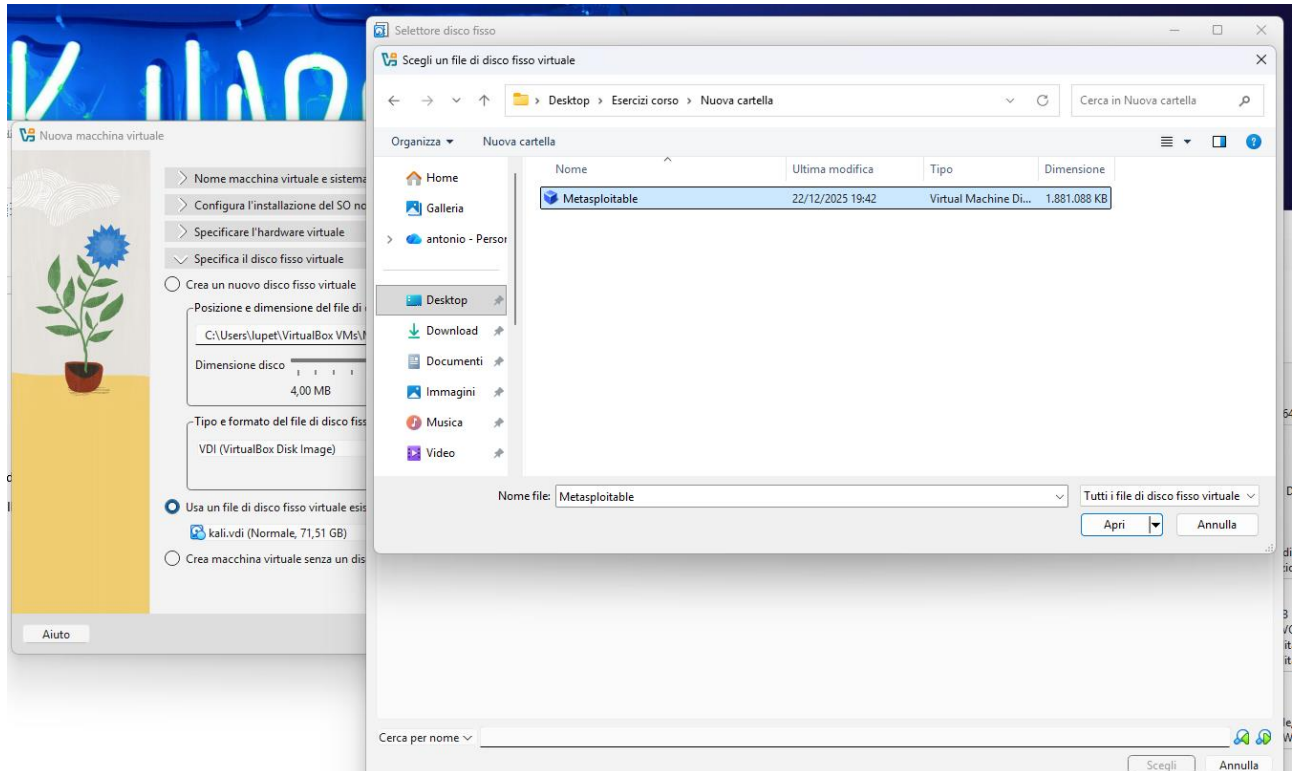
La consegna di oggi prevedeva le seguenti fasi:

1. Installazione e configurazione di Metasploitable

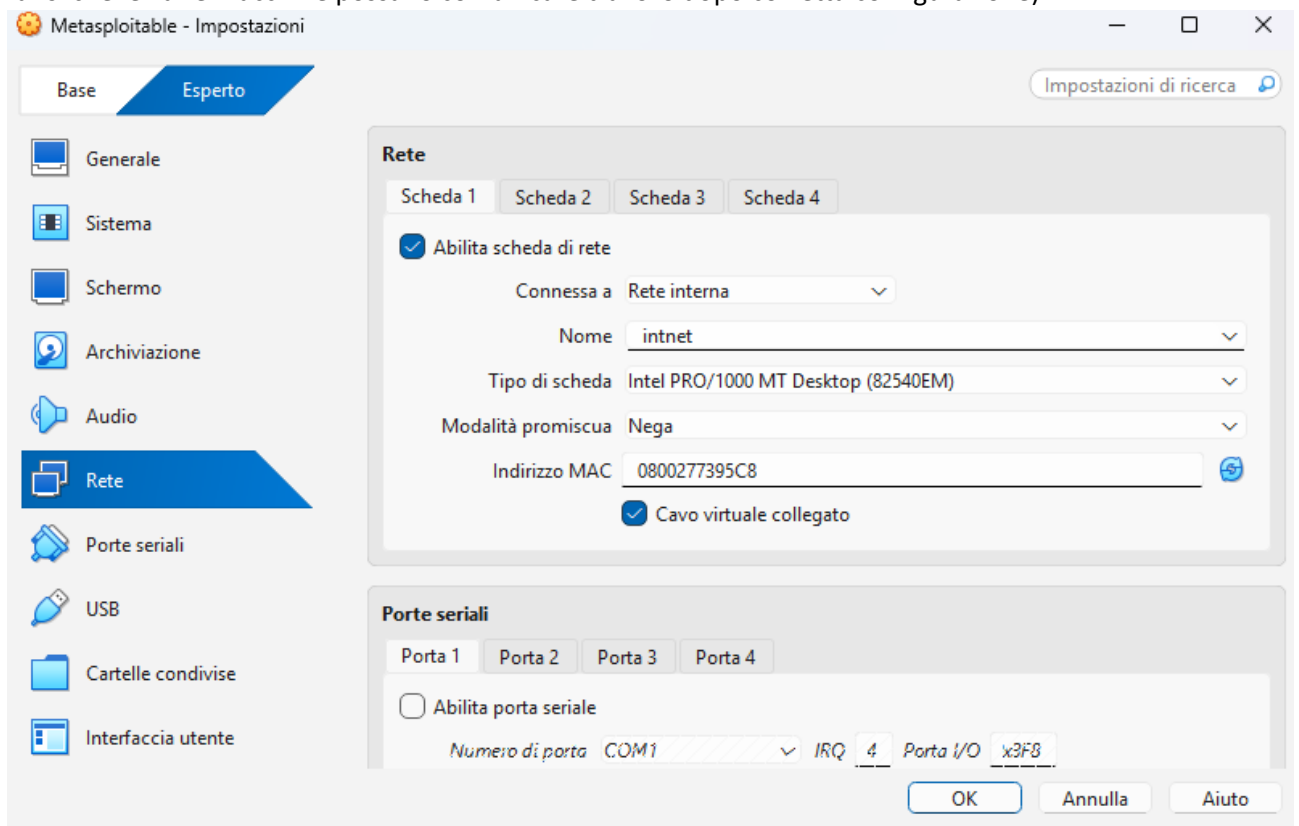
Scarichiamo il disco pre esistente e lo carichiamo su VirtualBox creando una nuova macchina configurata con Linux Debian(x64)



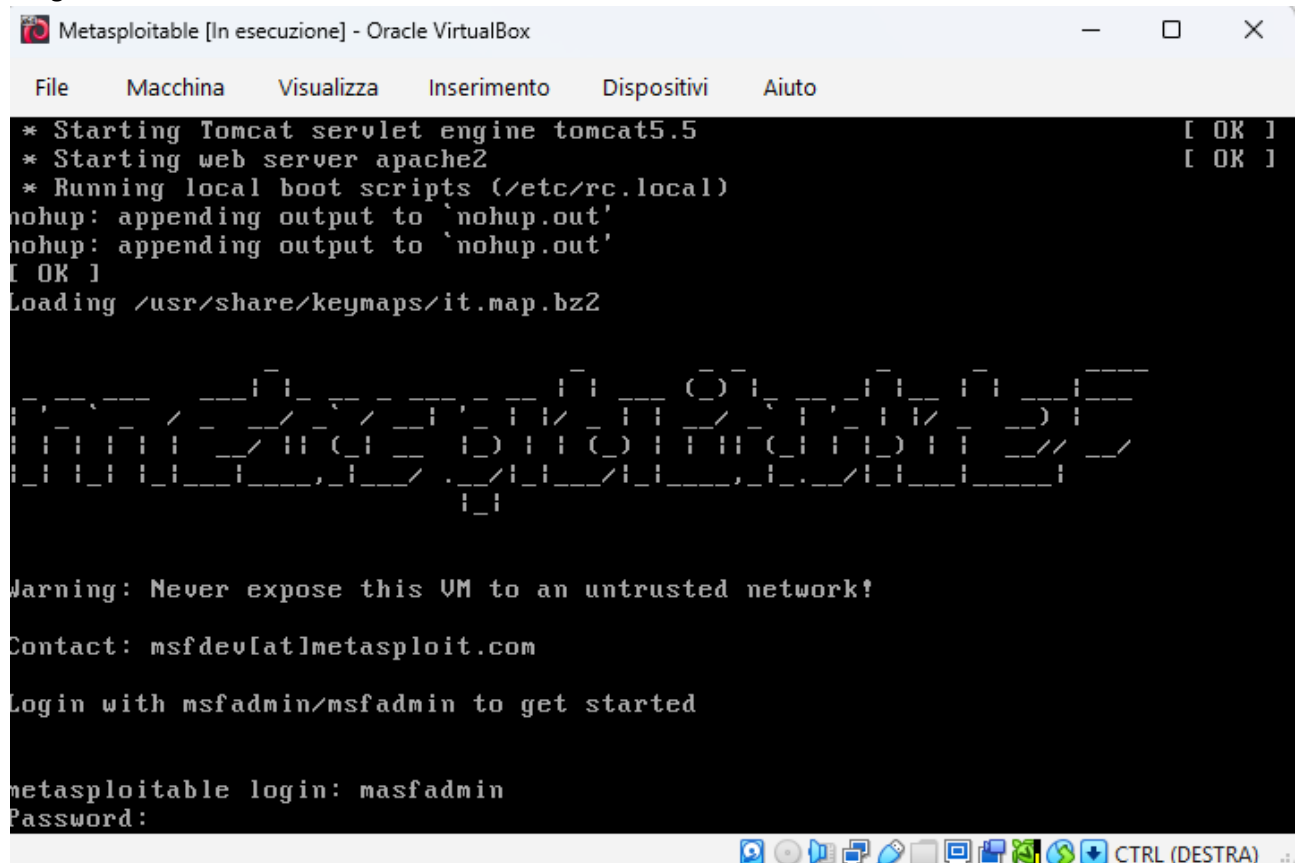
Successivamente configuriamo l'hardware e carichiamo il disco



Dopo aver caricato il disco configuriamo la rete della macchina e la mettiamo su rete interna (per far sì che le varie macchine possano comunicare tra loro dopo corretta configurazione)



Eseguiamo l'accesso usando msfadmin



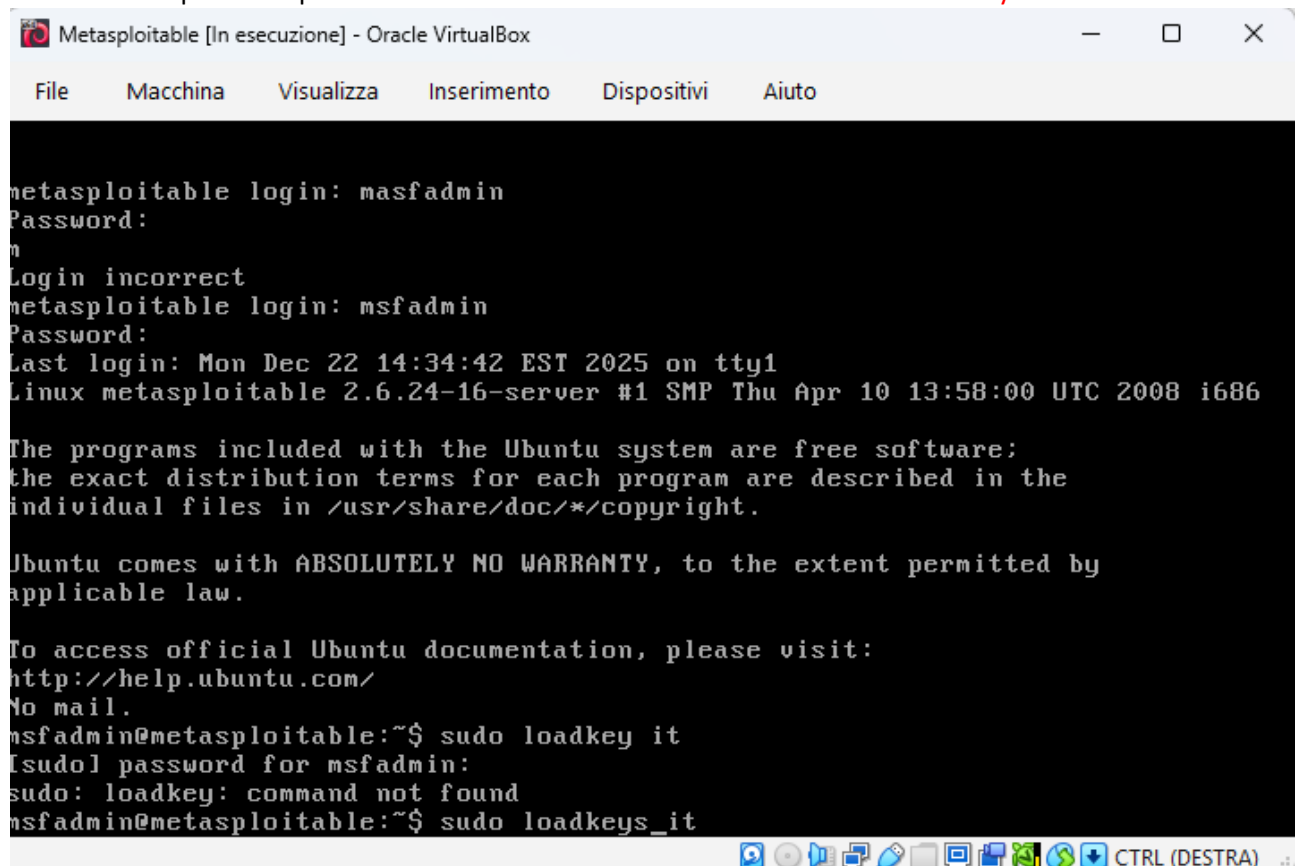
```
Metasploitable [In esecuzione] - Oracle VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

* Starting Tomcat servlet engine tomcat5.5 [ OK ]
* Starting web server apache2 [ OK ]
* Running local boot scripts (/etc/rc.local)
nohup: appending output to 'nohup.out'
nohup: appending output to 'nohup.out'
[ OK ]
Loading /usr/share/keymaps/it.map.bz2

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login: masfadmin
Password:
```

Adesso siamo pronti. Imposto la tastiera in italiano usando il comando **sudo loadkeys**



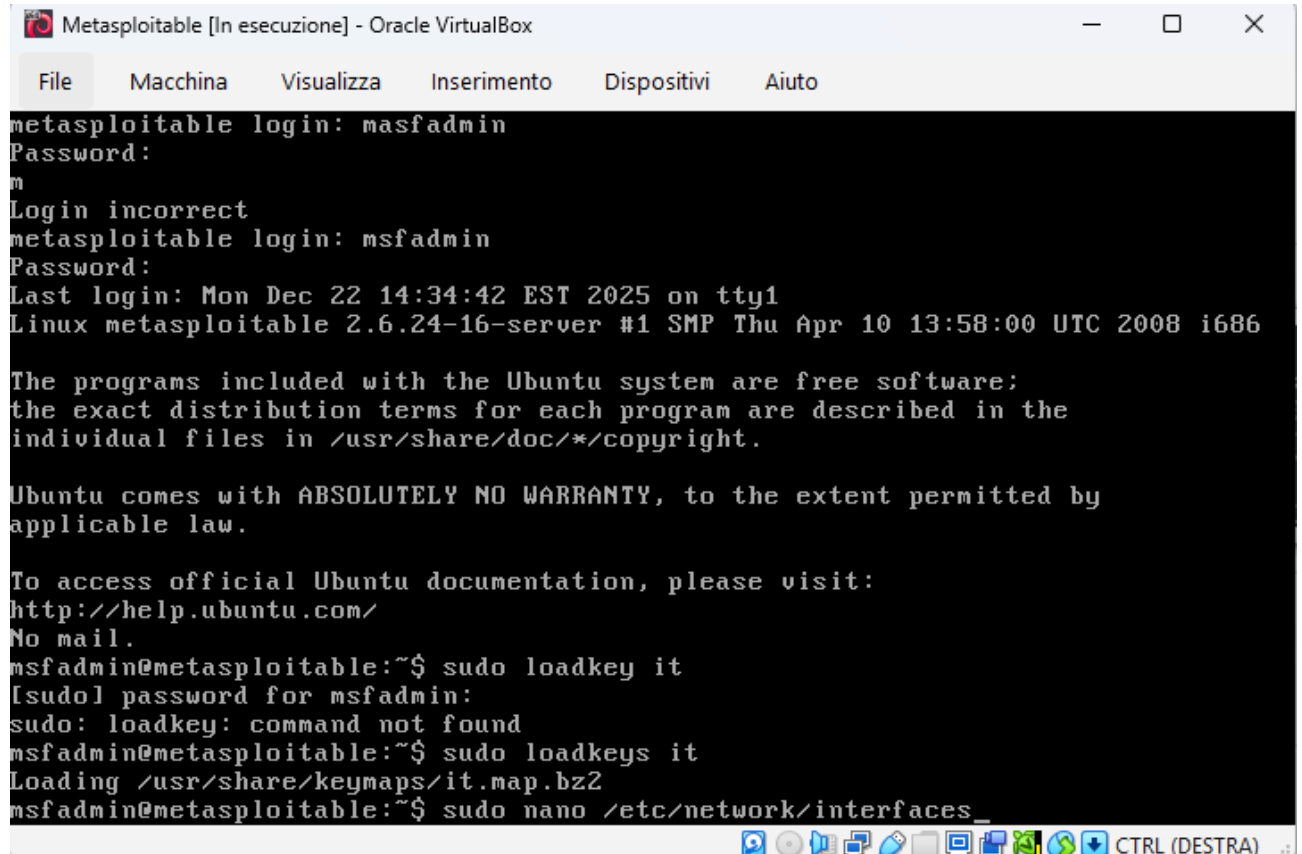
```
metasploitable login: masfadmin
Password:
Login incorrect
metasploitable login: msfadmin
Password:
Last login: Mon Dec 22 14:34:42 EST 2025 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ sudo loadkey it
[sudo] password for msfadmin:
sudo: loadkey: command not found
msfadmin@metasploitable:~$ sudo loadkeys_it
```

E procedo a con la configurazione della rete utilizzando `sudo nano /etc/network/interfaces`



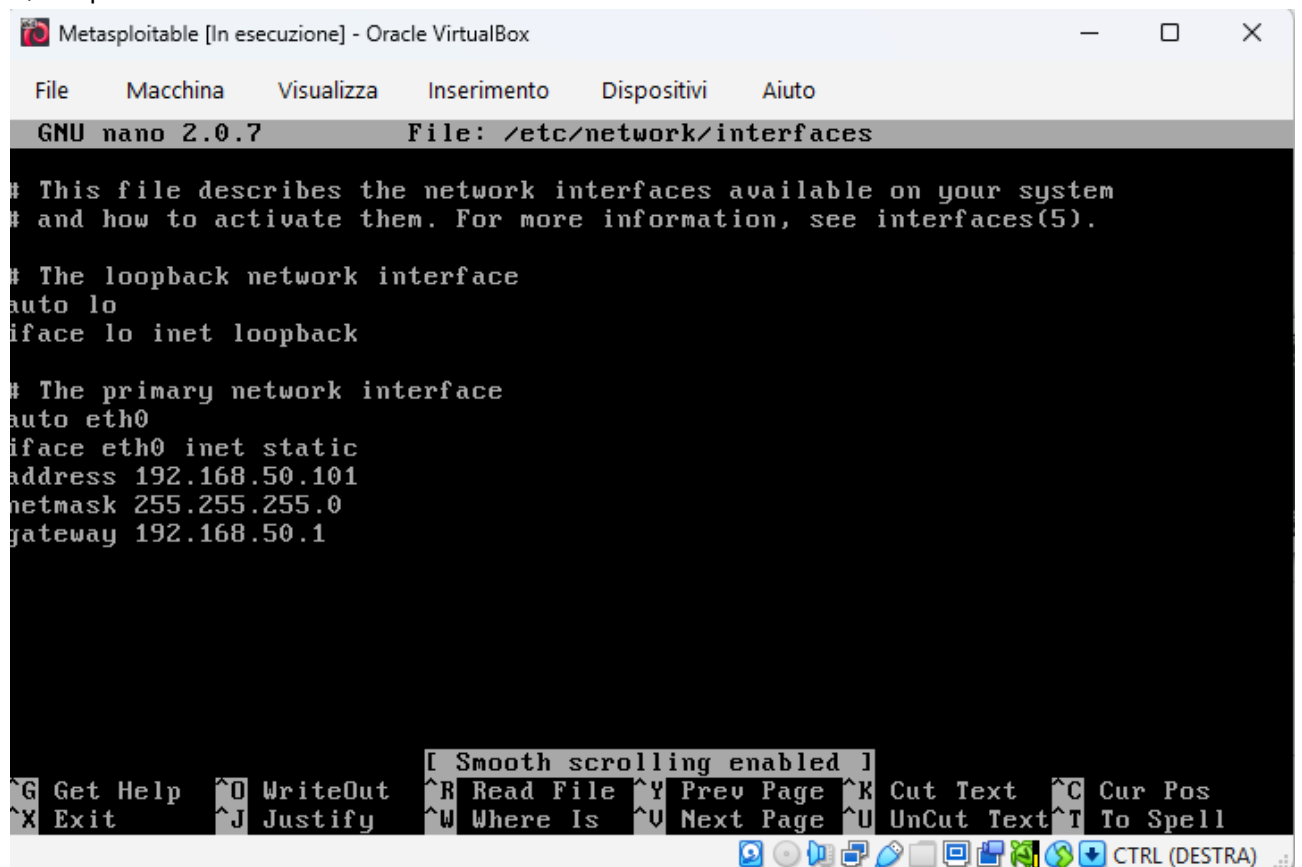
```
metasploitable login: masfadmin
Password:
Login incorrect
metasploitable login: msfadmin
Password:
Last login: Mon Dec 22 14:34:42 EST 2025 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ sudo loadkey it
[sudo] password for msfadmin:
sudo: loadkey: command not found
msfadmin@metasploitable:~$ sudo loadkeys it
Loading /usr/share/keymaps/it.map.bz2
msfadmin@metasploitable:~$ sudo nano /etc/network/interfaces_
```

Qui imposto i valori e salvo



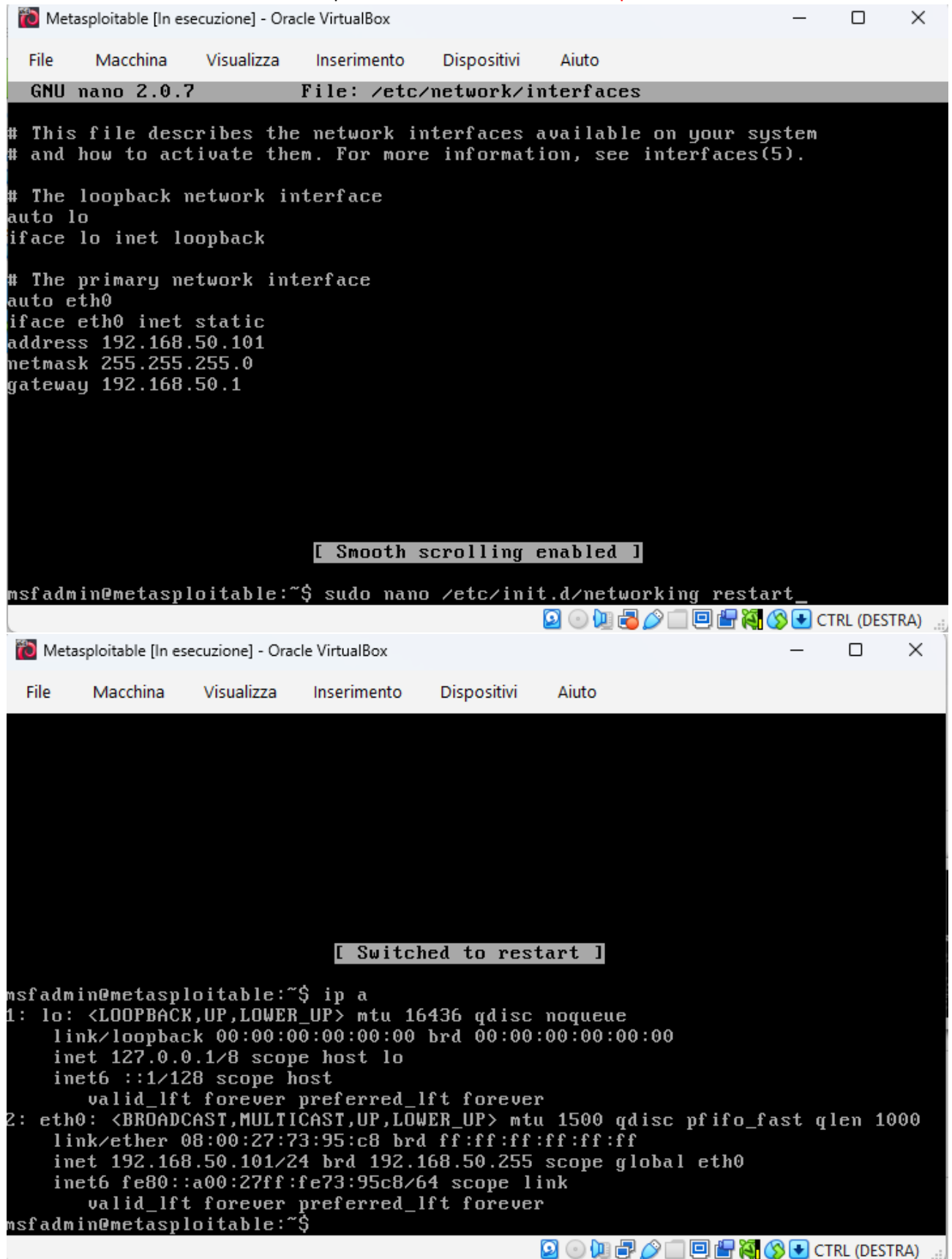
```
GNU nano 2.0.7 File: /etc/network/interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.50.101
netmask 255.255.255.0
gateway 192.168.50.1
```

Una volta salvato riavvio il network e procedo al controllo utilizzando **ip a**



```
Metasploitable [In esecuzione] - Oracle VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
GNU nano 2.0.7  File: /etc/network/interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.50.101
netmask 255.255.255.0
gateway 192.168.50.1

[ Smooth scrolling enabled ]

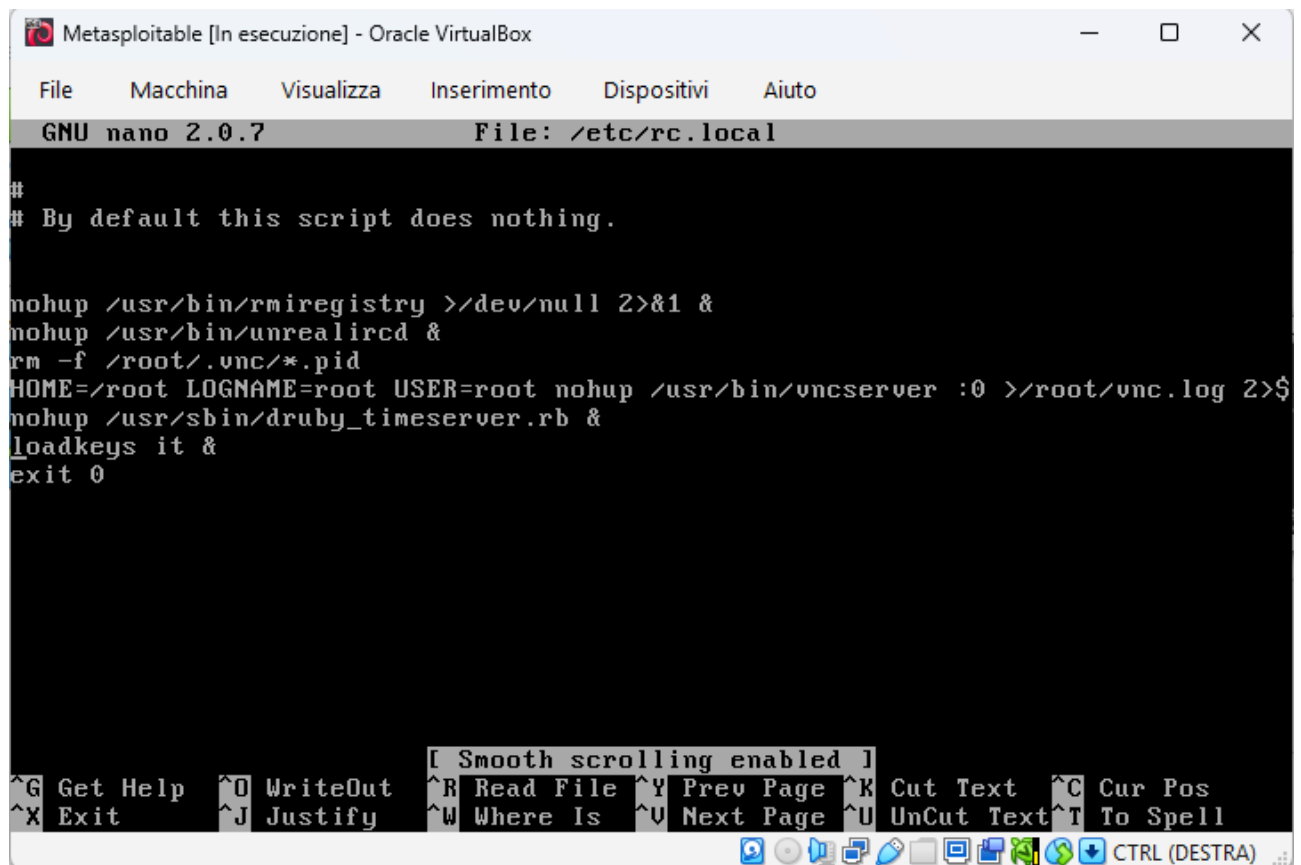
msfadmin@metasploitable:~$ sudo nano /etc/init.d/networking restart_

Metasploitable [In esecuzione] - Oracle VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

[ Switched to restart ]

msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:73:95:c8 brd ff:ff:ff:ff:ff:ff
    inet 192.168.50.101/24 brd 192.168.50.255 scope global eth0
    inet6 fe80::a00:27ff:fe73:95c8/64 scope link
        valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$
```

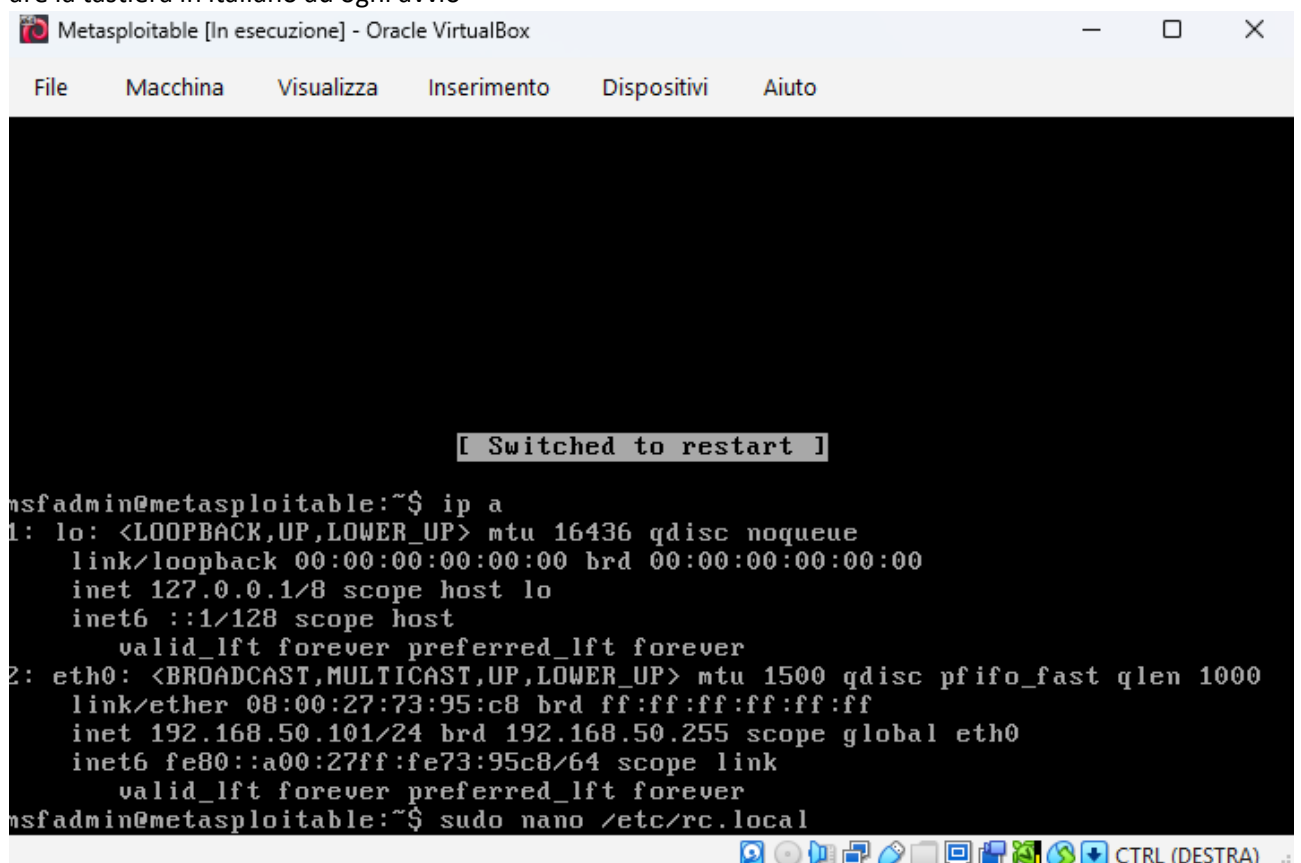
Adesso utilizzo il tip facoltativo per caricare la tastiera in italiano ad ogni avvio in automatico



```
#
# By default this script does nothing.

nohup /usr/bin/rmiregistry >/dev/null 2>&1 &
nohup /usr/bin/unrealircd &
rm -f /root/.vnc/*.pid
HOME=/root LOGNAME=root USER=root nohup /usr/bin/vncserver :0 >/root/vnc.log 2>$
nohup /usr/sbin/druby_timeserver.rb &
loadkeys it &
exit 0
```

are la tastiera in italiano ad ogni avvio

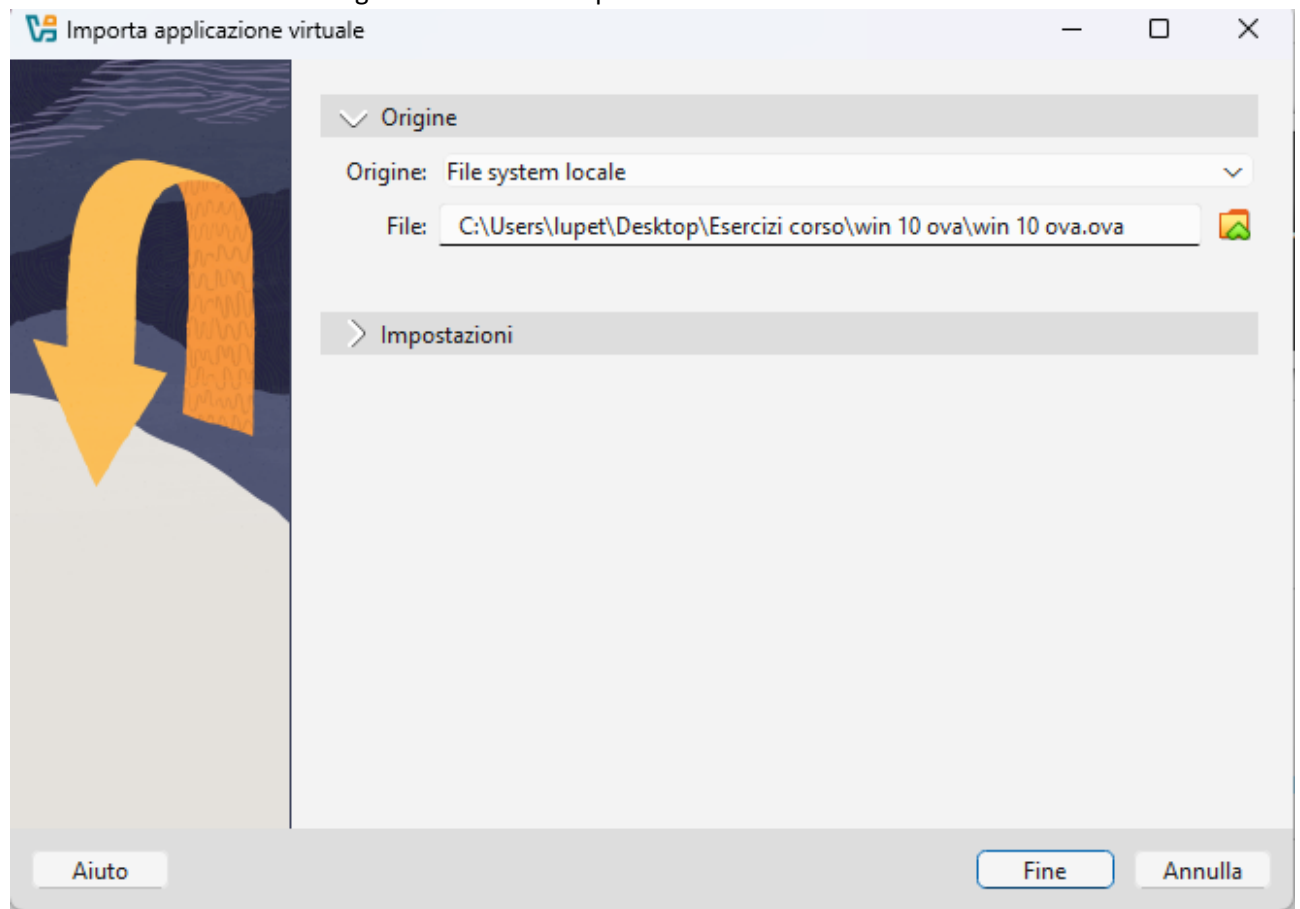


```
[ Switched to restart ]

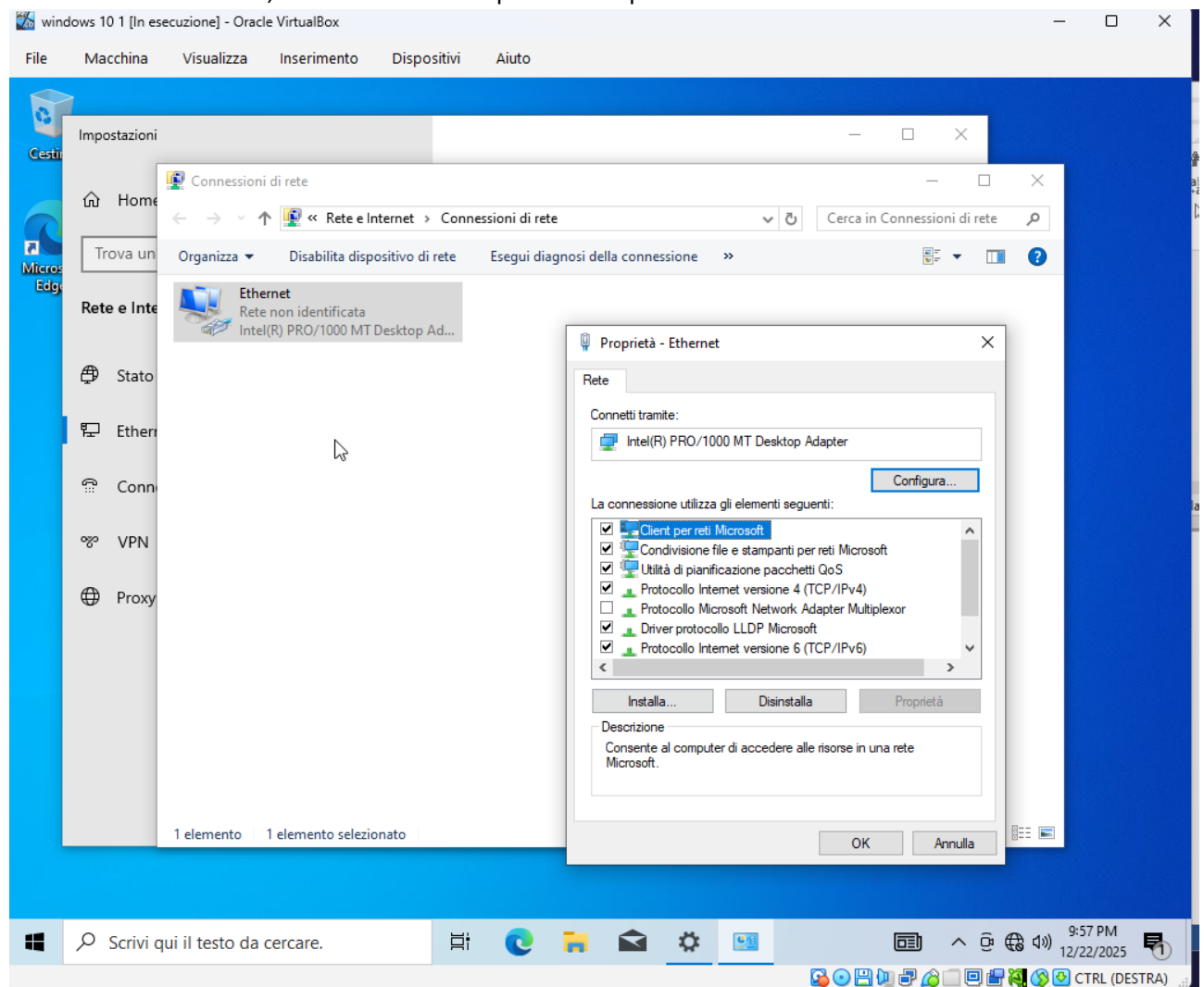
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:73:95:c8 brd ff:ff:ff:ff:ff:ff
    inet 192.168.50.101/24 brd 192.168.50.255 scope global eth0
    inet6 fe80::a00:27ff:fe73:95c8/64 scope link
        valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$ sudo nano /etc/rc.local
```

2. Installazione e configurazione di Windows 10 tramite file.ova

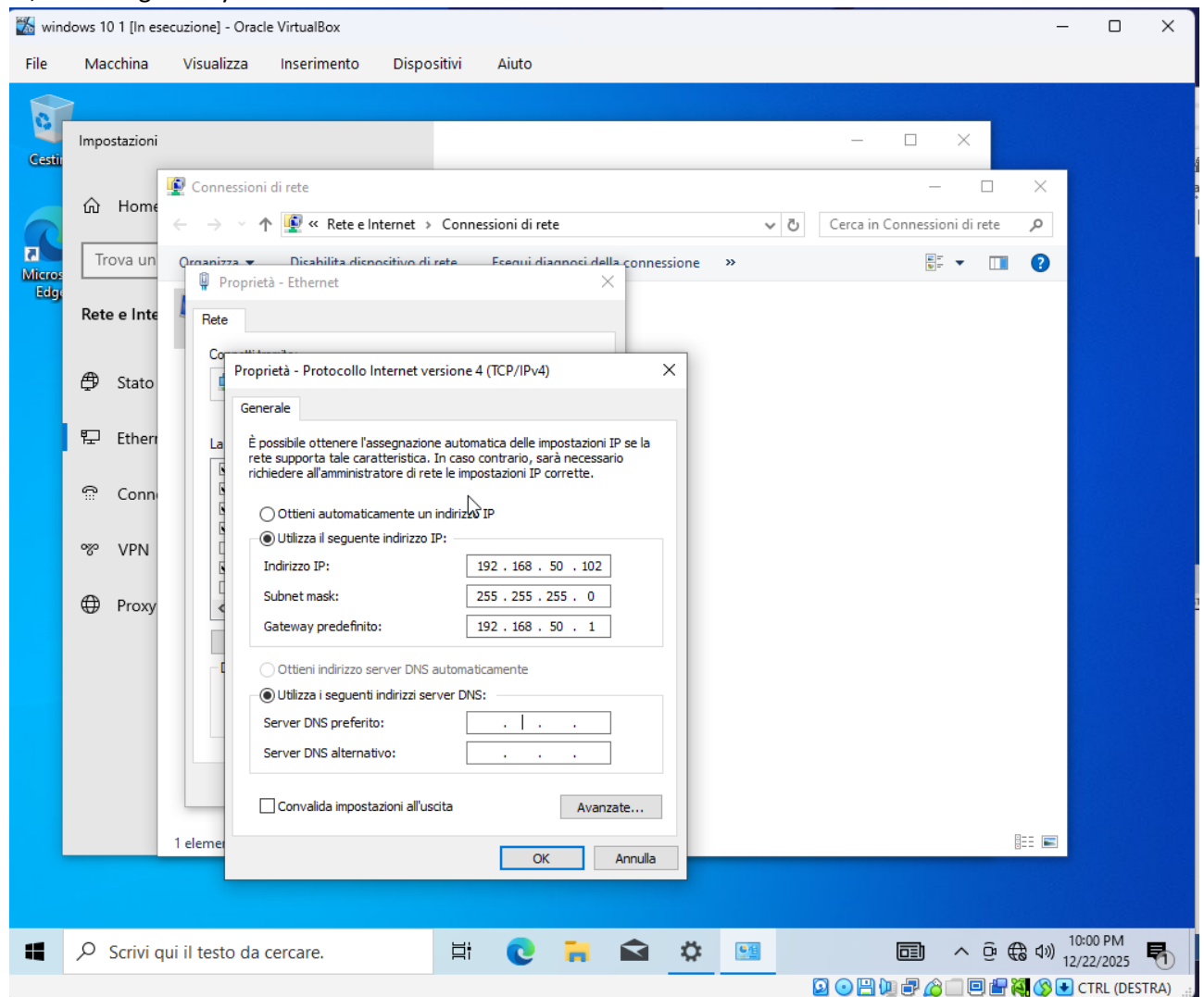
Come primo step recupero il file .ova dalla directory e lo importo tramite l'apposita interfaccia di VB e mi assicuro che sia collegata su rete interna prima di avviarla



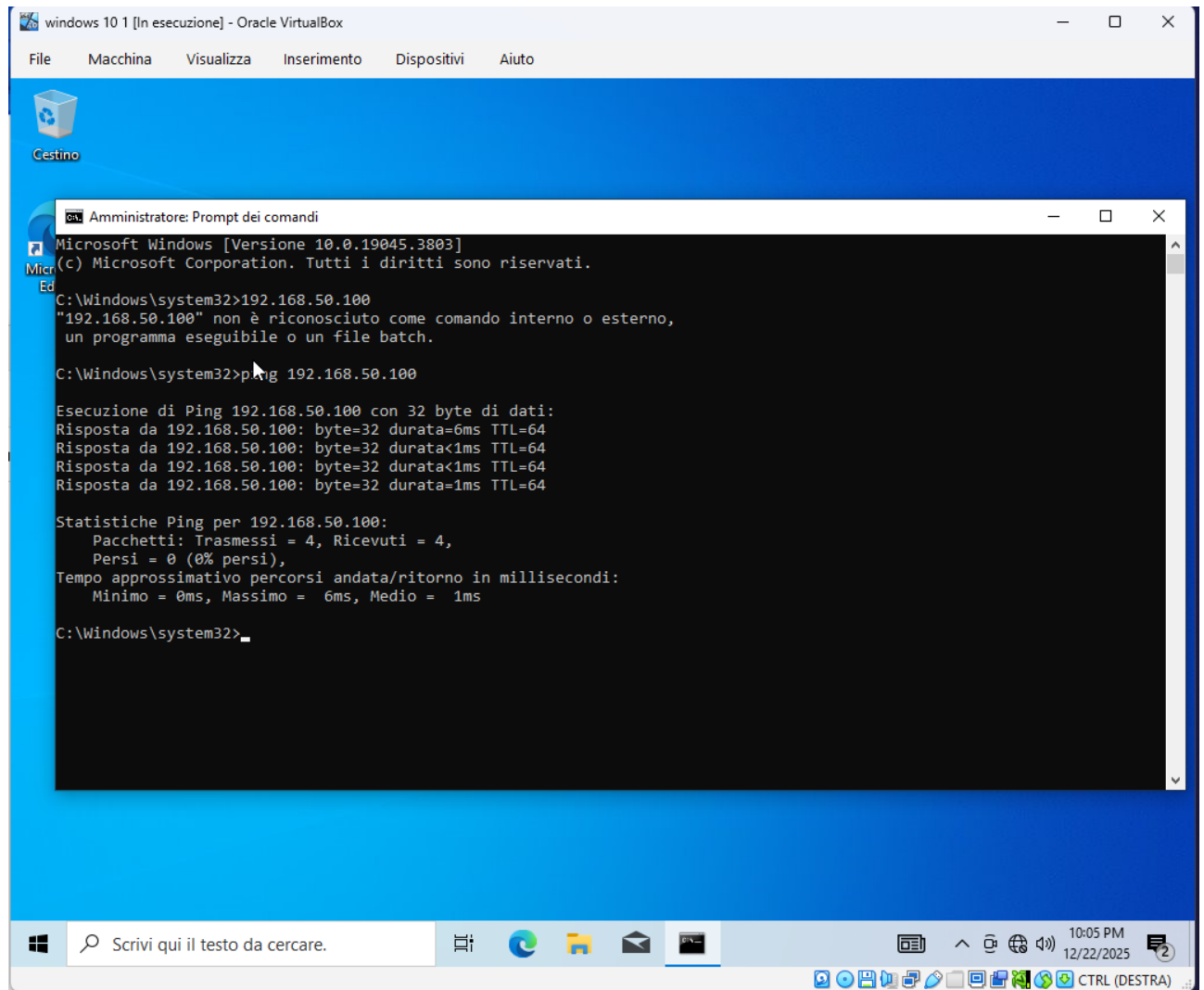
Una volta avviata la macchina virtuale apro subito le impostazioni dirette e vado a configurare la scheda di rete ethernet, disabilitando come prima cosa ipv6



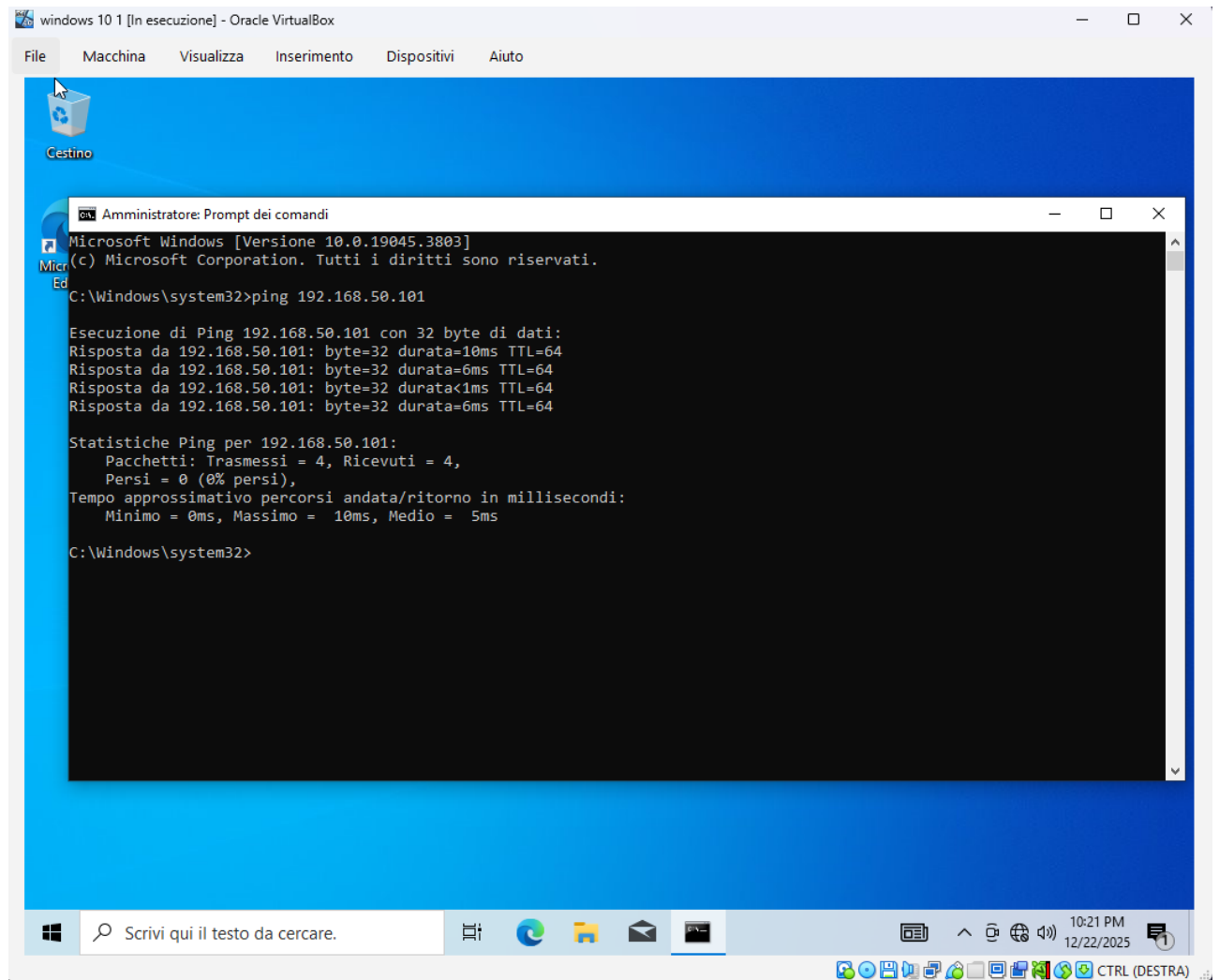
Dopo di che andando su protocollo internet versione 4 vado a inserire manualmente l'indirizzo IP, subnet e gateway



Riavvio la macchina e controllo se comunica con kali aprendo il prompt dei comandi ed utilizzando il comando **ping**



3. Le macchine virtuali devono essere in grado di comunicare tra loro su rete interna in windows abbiamo già controllato adesso vediamo gli altri 2 sistemi operativi.



Questo è il ping all'altra macchina da windows

kali (Controllo corretta comunicazione) [In esecuzione] - Oracle VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

kali@kali: ~

Sessione Azioni Modifica Visualizza Aiuto

```
(kali@kali)-[~]
$ ping 192.168.50.101
PING 192.168.50.101 (192.168.50.101) 56(84) bytes of data.
64 bytes from 192.168.50.101: icmp_seq=1 ttl=64 time=5.51 ms
64 bytes from 192.168.50.101: icmp_seq=2 ttl=64 time=0.617 ms
64 bytes from 192.168.50.101: icmp_seq=3 ttl=64 time=3.83 ms
64 bytes from 192.168.50.101: icmp_seq=4 ttl=64 time=0.958 ms
64 bytes from 192.168.50.101: icmp_seq=5 ttl=64 time=6.77 ms
64 bytes from 192.168.50.101: icmp_seq=6 ttl=64 time=0.928 ms
^C
--- 192.168.50.101 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5156ms
rtt min/avg/max/mdev = 0.617/3.101/6.769/2.424 ms

(kali@kali)-[~]
$
```

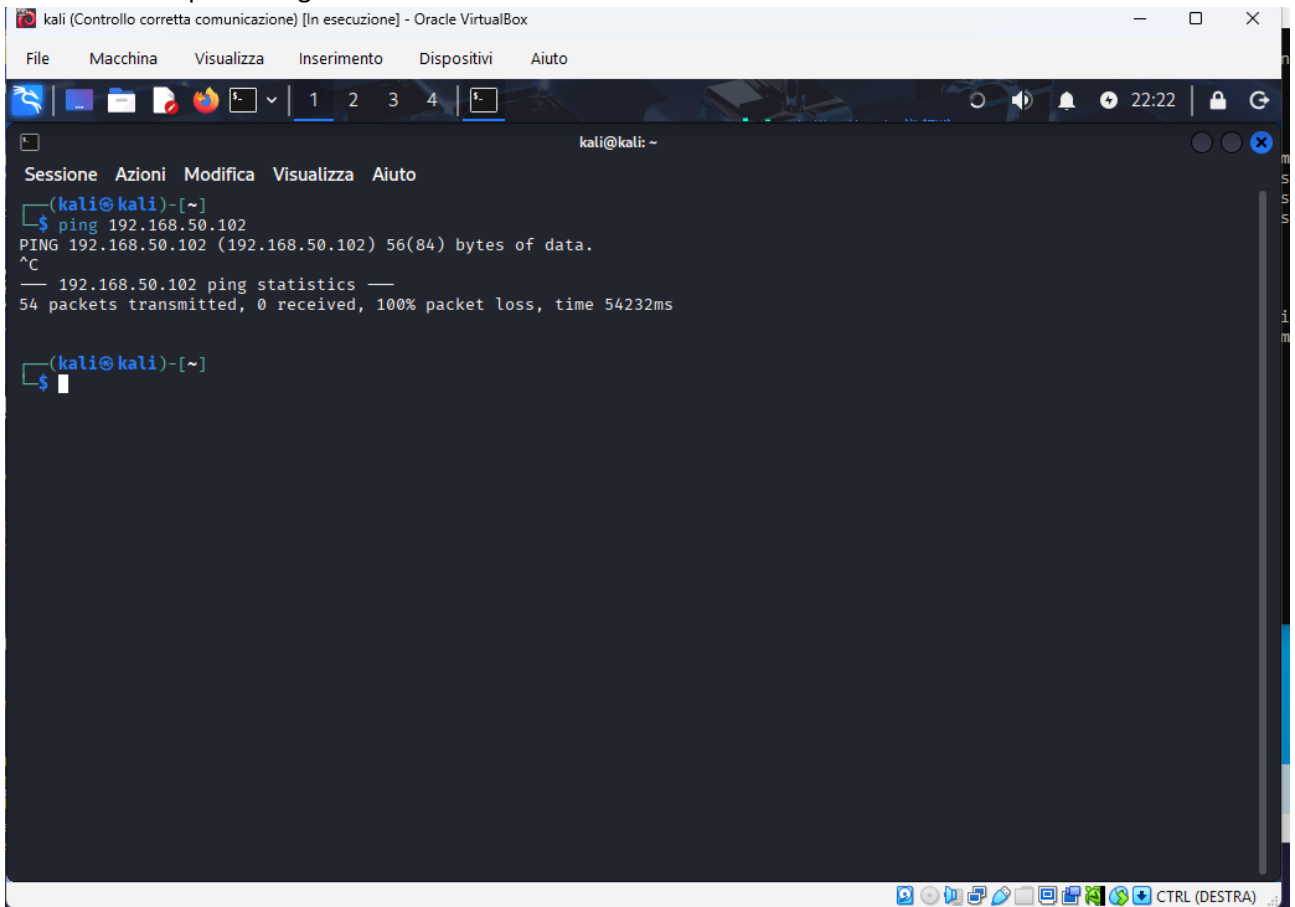
Metasploitable [In esecuzione] - Oracle VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

```
msfadmin@metasploitable:~$ ping 192.168.50.100
PING 192.168.50.100 (192.168.50.100) 56(84) bytes of data.
64 bytes from 192.168.50.100: icmp_seq=1 ttl=64 time=0.914 ms
64 bytes from 192.168.50.100: icmp_seq=2 ttl=64 time=0.601 ms
64 bytes from 192.168.50.100: icmp_seq=3 ttl=64 time=0.552 ms
64 bytes from 192.168.50.100: icmp_seq=4 ttl=64 time=0.588 ms
64 bytes from 192.168.50.100: icmp_seq=5 ttl=64 time=0.602 ms
64 bytes from 192.168.50.100: icmp_seq=6 ttl=64 time=0.571 ms
64 bytes from 192.168.50.100: icmp_seq=7 ttl=64 time=0.555 ms
64 bytes from 192.168.50.100: icmp_seq=8 ttl=64 time=0.655 ms
64 bytes from 192.168.50.100: icmp_seq=9 ttl=64 time=0.608 ms
64 bytes from 192.168.50.100: icmp_seq=10 ttl=64 time=0.600 ms
64 bytes from 192.168.50.100: icmp_seq=11 ttl=64 time=0.510 ms
64 bytes from 192.168.50.100: icmp_seq=12 ttl=64 time=0.557 ms
64 bytes from 192.168.50.100: icmp_seq=13 ttl=64 time=0.569 ms
64 bytes from 192.168.50.100: icmp_seq=14 ttl=64 time=0.572 ms
64 bytes from 192.168.50.100: icmp_seq=15 ttl=64 time=0.559 ms
64 bytes from 192.168.50.100: icmp_seq=16 ttl=64 time=0.874 ms
64 bytes from 192.168.50.100: icmp_seq=17 ttl=64 time=0.521 ms
64 bytes from 192.168.50.100: icmp_seq=18 ttl=64 time=0.547 ms

--- 192.168.50.100 ping statistics ---
19 packets transmitted, 18 received, 5% packet loss, time 17997ms
rtt min/avg/max/mdev = 0.510/0.608/0.914/0.109 ms
msfadmin@metasploitable:~$
```

E ovviamente per questioni di firewall non è possibile pingare verso la macchina con windows ,
dimostrato da quanto segue

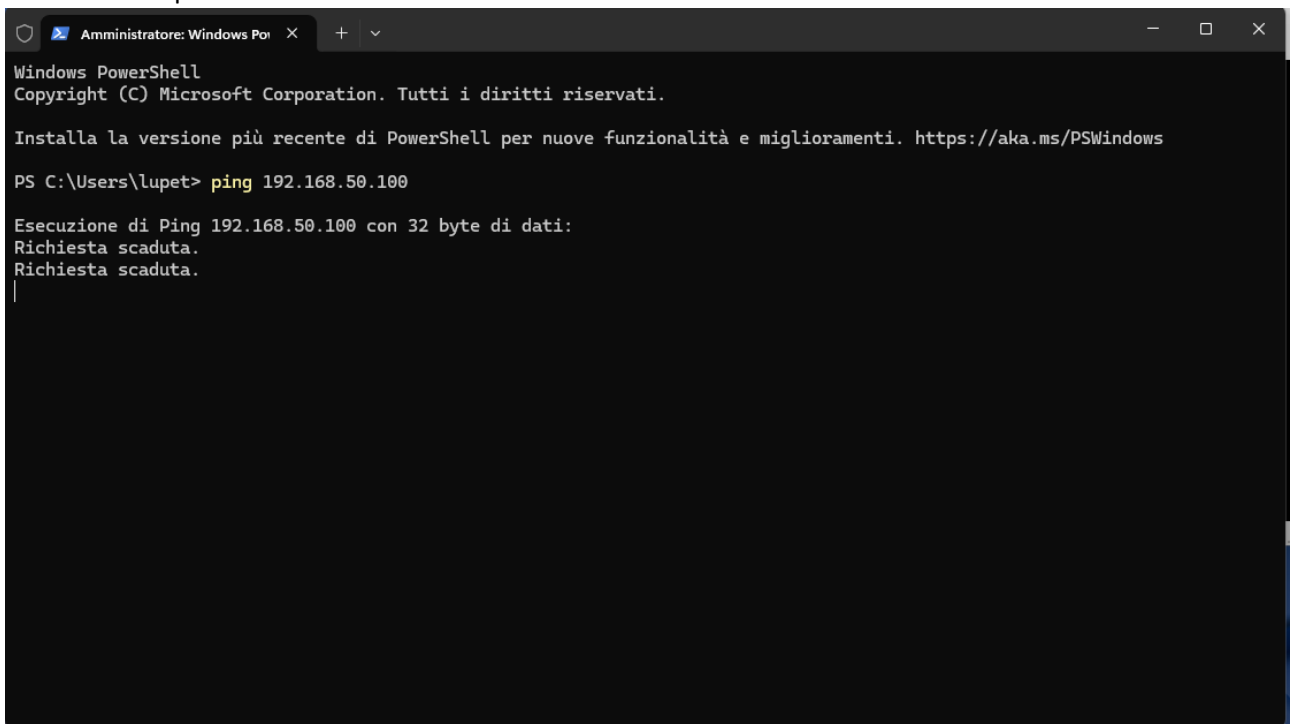


```
kali (Controllo corretta comunicazione) [In esecuzione] - Oracle VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
kali@kali: ~
Sessione  Azioni  Modifica  Visualizza  Aiuto
(kali@kali)-[~]
$ ping 192.168.50.102
PING 192.168.50.102 (192.168.50.102) 56(84) bytes of data.
^C
— 192.168.50.102 ping statistics —
54 packets transmitted, 0 received, 100% packet loss, time 54232ms

(kali@kali)-[~]
$
```

4. Il sistema host non deve comunicare con l'ambiente virtuale.

Ho provato a pingare tramite il cmd del sistema host verso i dispositivi virtuali e ovviamente non ho ricevuto esito positivo



```
Amministratore: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. Tutti i diritti riservati.

Installa la versione più recente di PowerShell per nuove funzionalità e miglioramenti. https://aka.ms/PSWindows
PS C:\Users\lupet> ping 192.168.50.100

Esecuzione di Ping 192.168.50.100 con 32 byte di dati:
Richiesta scaduta.
Richiesta scaduta.
|
```