

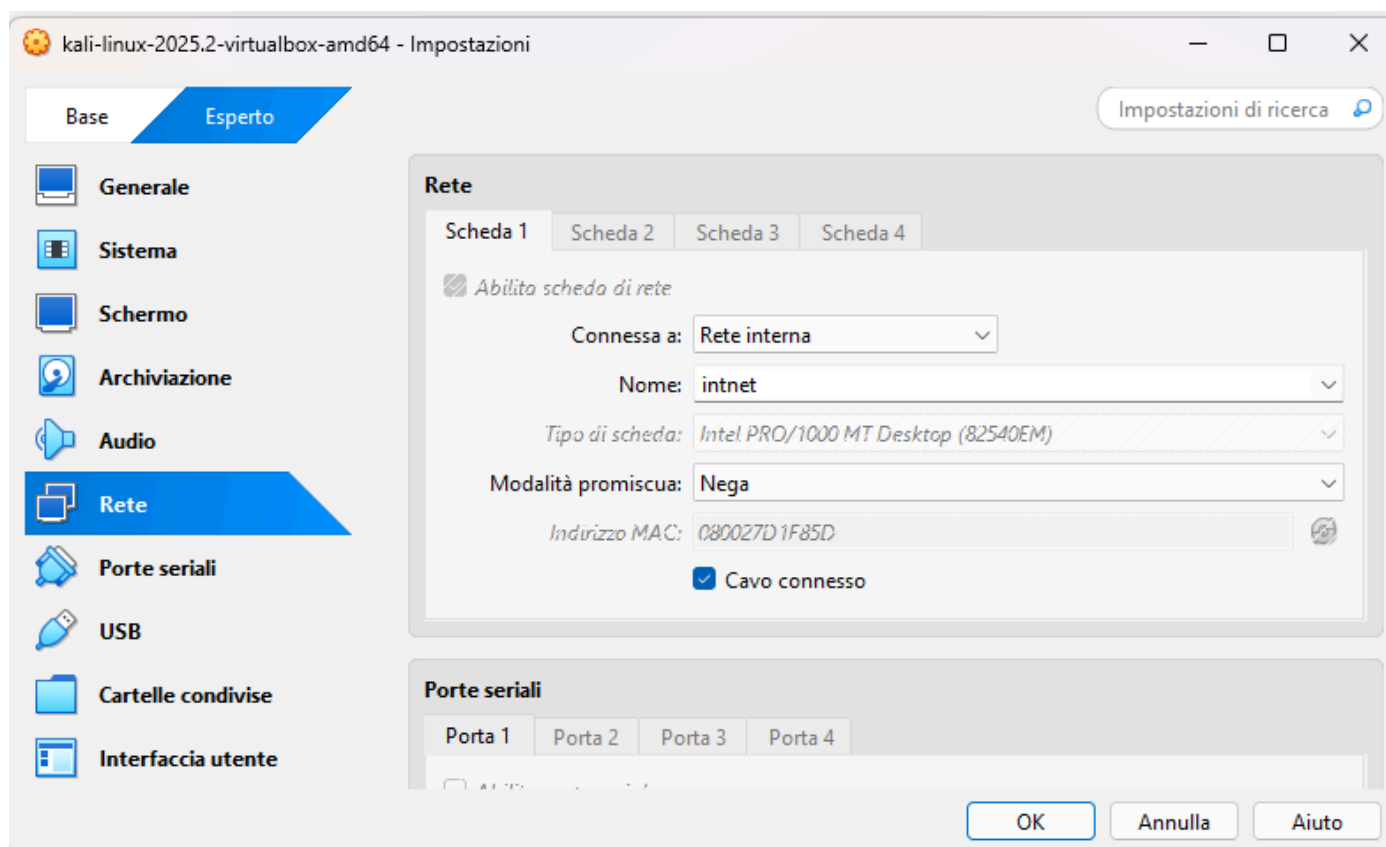
Creazione pratica di una regola Firewall

Traccia esercizio:

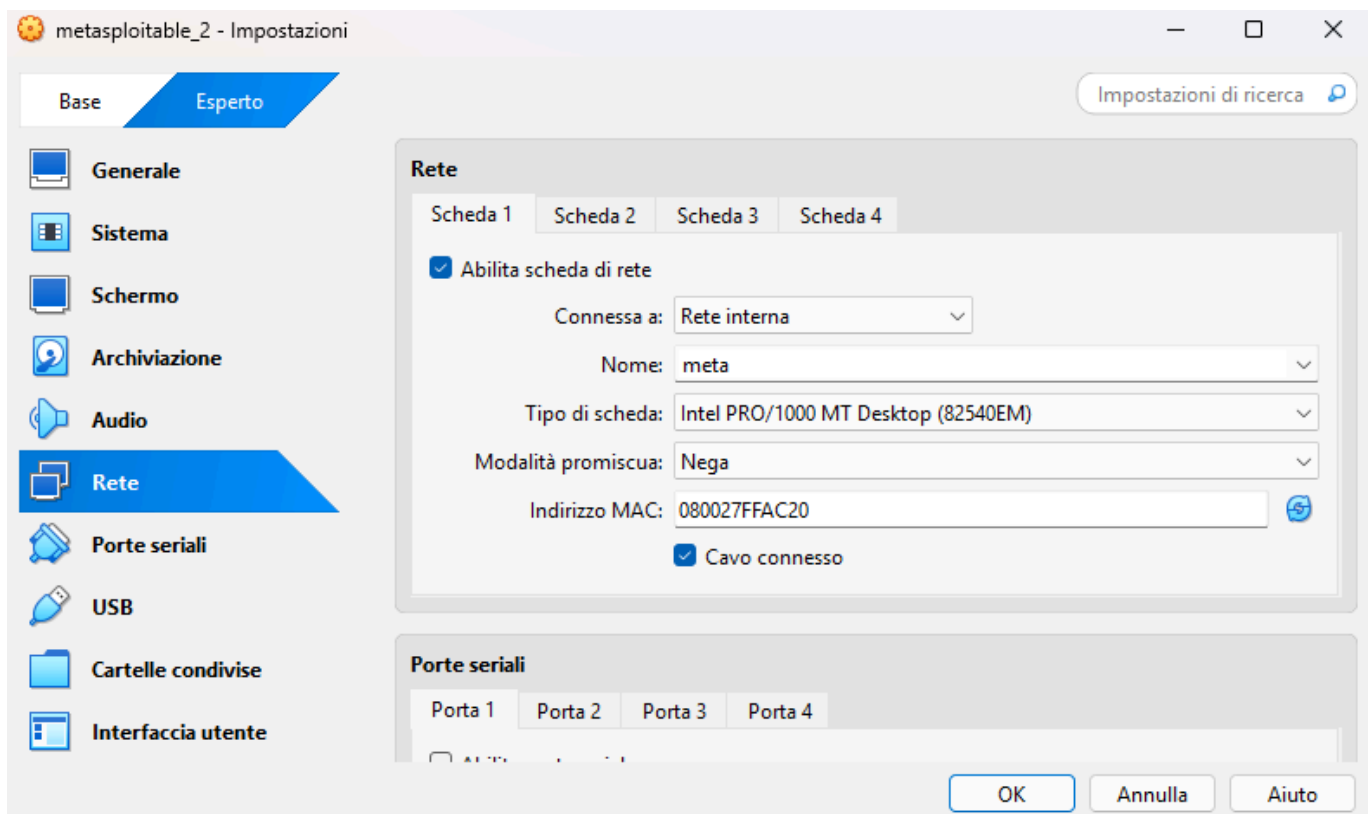
Sulla base di quanto visto, creare una regola firewall che blocchi l'accesso alla DVWA (su metasploitable) dalla macchina Kali Linux e ne impedisca di conseguenza lo scan. Un requisito fondamentale di questo esercizio è che le macchine Kali e Metasploitable siano su reti diverse, potete aggiungere una nuova interfaccia di rete a Pfsense in modo tale da gestire una ulteriore rete.

Come inizio dato che la traccia richiede che Kali e Metasploitable siano su reti diverse bisogna impostare VirtualBox le reti come segue:

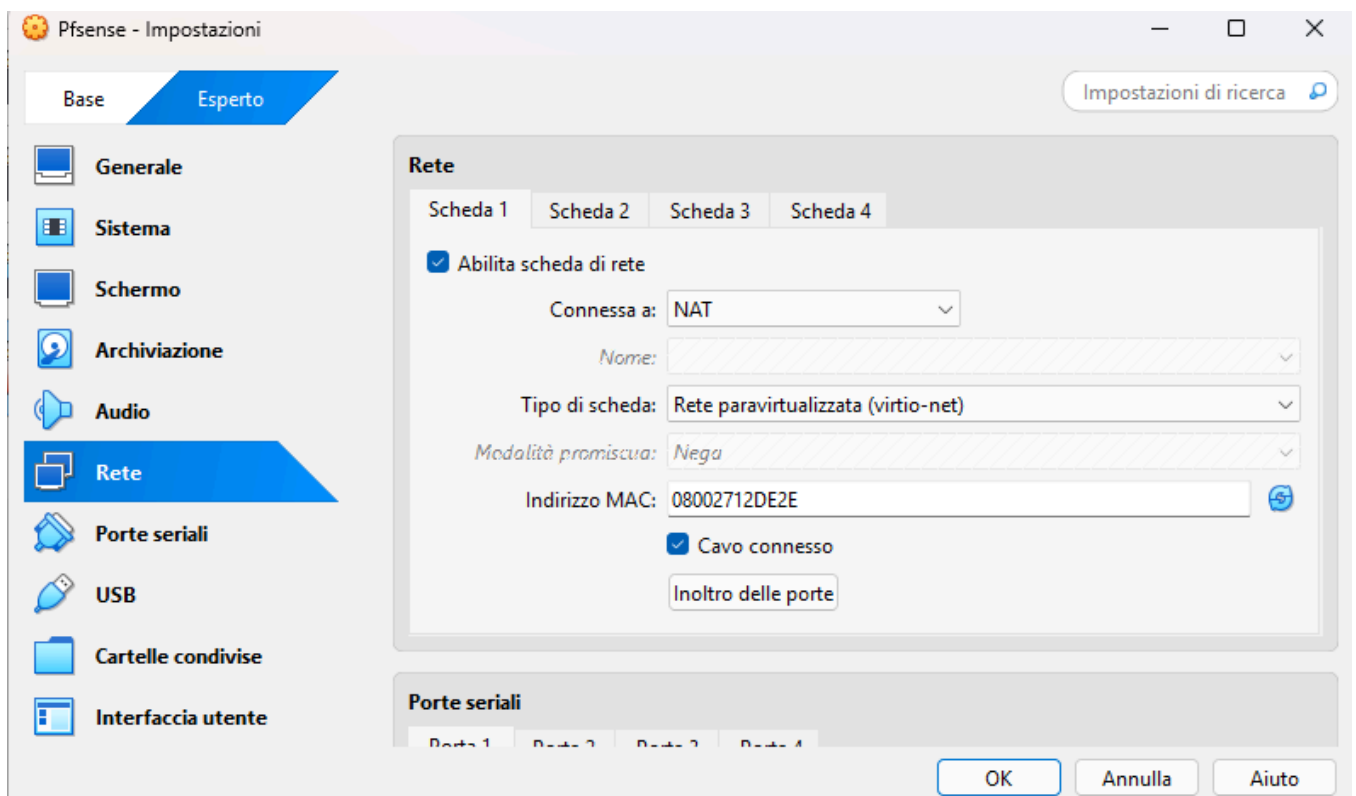
Rete interna kali linux (chiamata intnet):

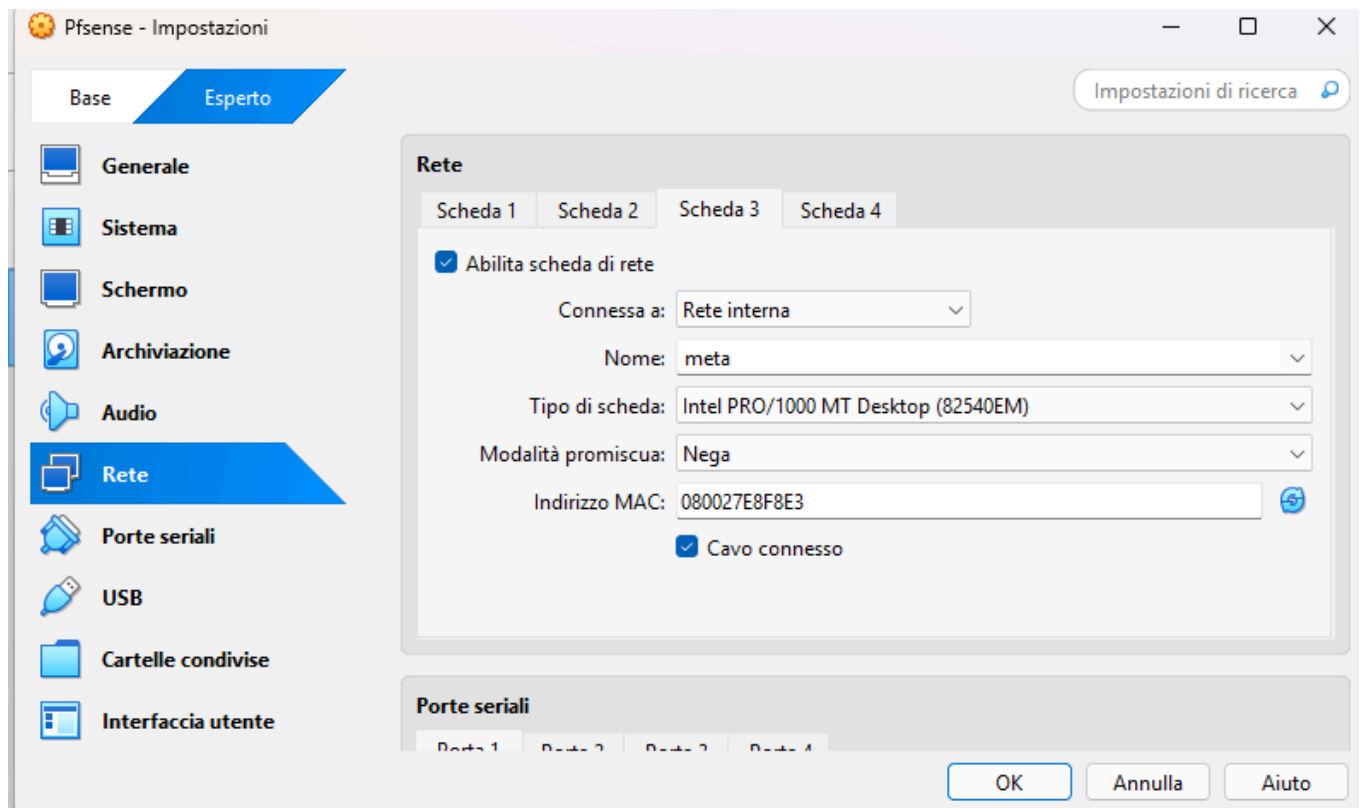
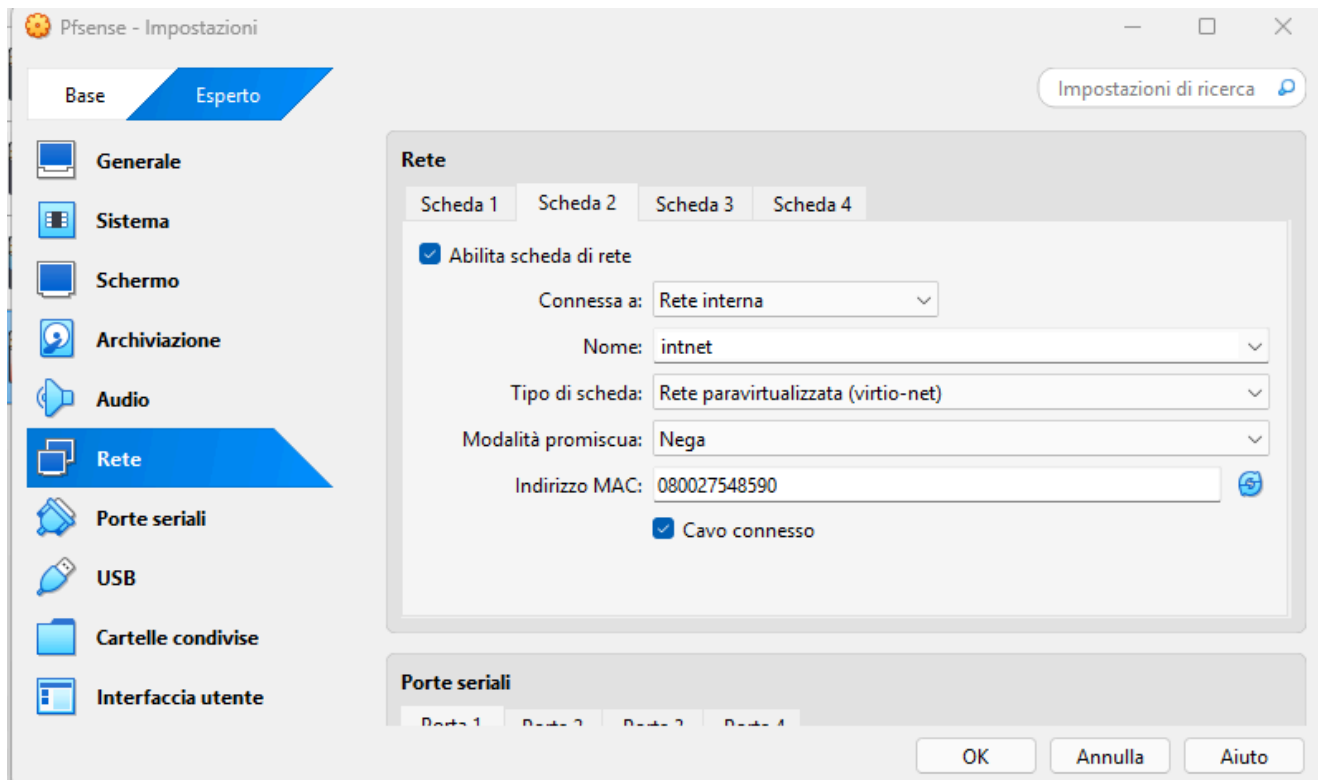


Rete interna metasploitable (chiamata meta):



Le 3 Reti impostazione di Psense: (1 NAT, 2 intnet kali, 3 meta metasploitable)

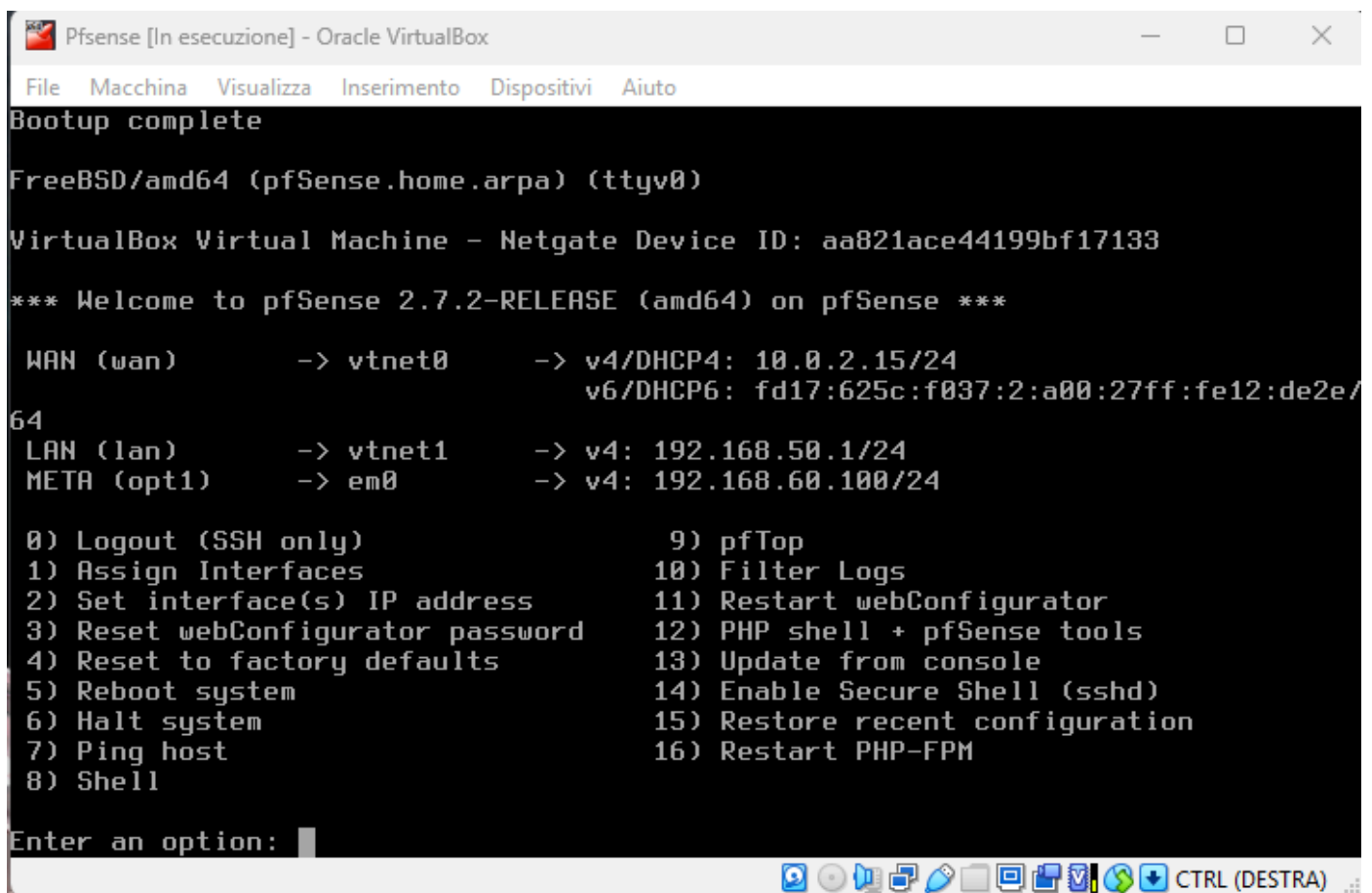




In seguito per avere effettivamente delle reti diverse si è dovuto impostare sulle macchine Kali e Metasploitable degli indirizzi IP in modo che appartenessero a reti diverse, dall'immagine sotto si può vedere il risultato su Pfsense:

Kali Linux ha indirizzo statico 192.168.50.100

Metasploitable ha indirizzo statico 192.168.60.100



```
Pfsense [In esecuzione] - Oracle VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
Bootup complete
FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)
VirtualBox Virtual Machine - Netgate Device ID: aa821ace44199bf17133
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> vtnet0      -> v4/DHCP4: 10.0.2.15/24
                                   v6/DHCP6: fd17:625c:f037:2:a00:27ff:fe12:de2e/
64
LAN (lan)      -> vtnet1      -> v4: 192.168.50.1/24
META (opt1)    -> em0        -> v4: 192.168.60.100/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults    13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell

Enter an option: 
```

Il passo successivo è stato tramite Pfsense (firewall software) l'aggiunta della rete Meta nel firewall stesso in modo da poter essere gestita:

| Interface | Network port |
|-----------|----------------------------|
| WAN | vtnet0 (08:00:27:12:de:2e) |
| LAN | vtnet1 (08:00:27:54:85:90) |
| Meta | em0 (08:00:27:e8:f8:e3) |

Una volta superato questo passaggio è stata creata una regola per permettere alla rete META di comunicare, impostando Meta subnet come source ed any come destination (questo passaggio è necessario altrimenti la rete META rimarrebbe completamente isolata):

Firewall / Rules / Edit

Edit Firewall Rule

Action

Pass

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled

☐ Disable this rule

Set this option to disable this rule without removing it from the list.

Interface

META

Choose the interface from which packets must come to match this rule.

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

Any

Choose which IP protocol this rule should match.

Source

Source

☐ Invert match

META subnets

Source Address

/

Destination

Destination

☐ Invert match

Any

Destination Address

/

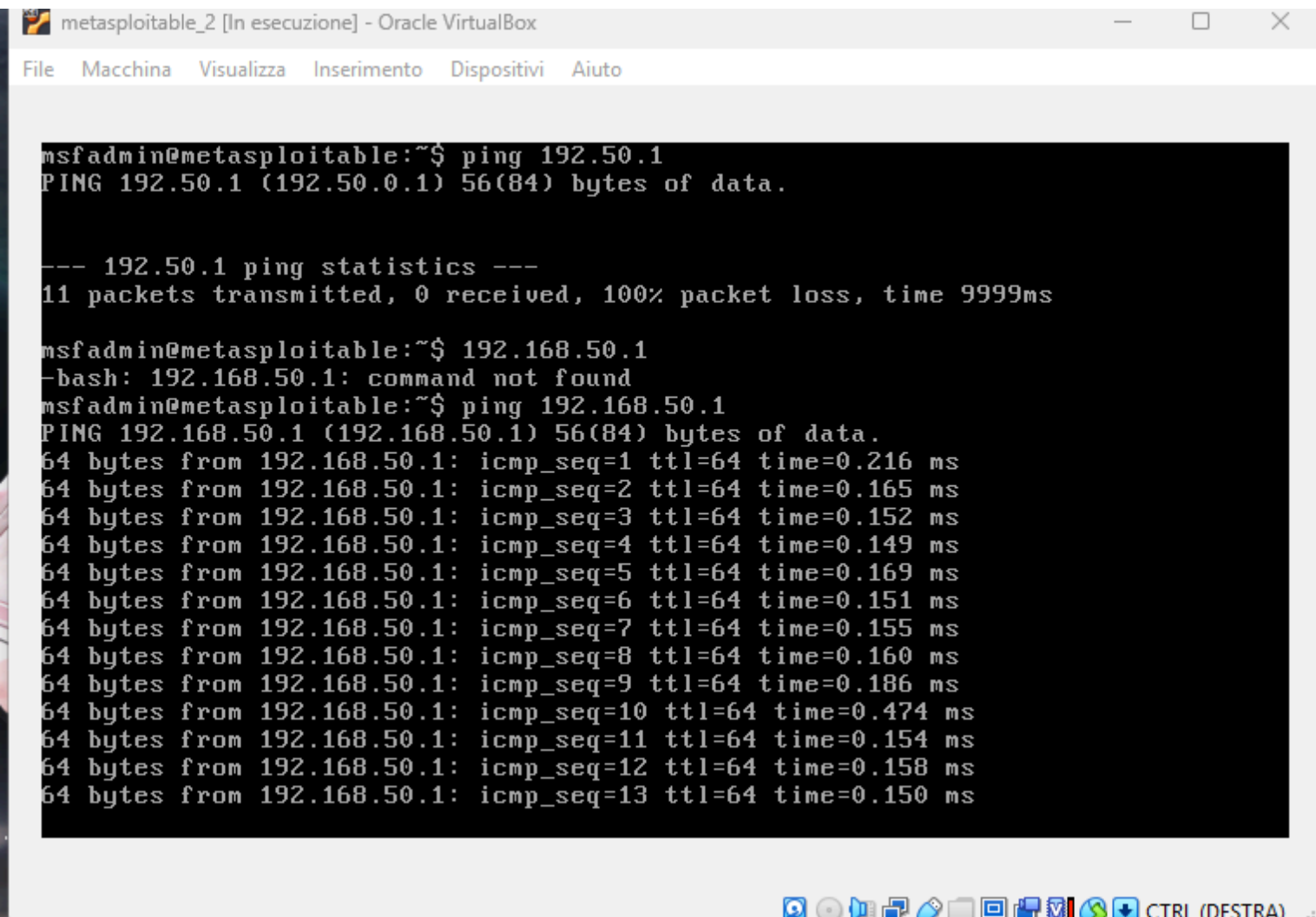
Extra Options

Log

☐ Log packets that are handled by this rule

Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status](#), [System Logs](#), [Settings](#) page).

Per verificare che la rete META fosse ora funzionante si è provato un ping dalla Metasploitable verso l'IP di Kali e come si può vedere ha funzionato correttamente:



```
metasploitable_2 [In esecuzione] - Oracle VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

msfadmin@metasploitable:~$ ping 192.50.1
PING 192.50.1 (192.50.0.1) 56(84) bytes of data.

--- 192.50.1 ping statistics ---
11 packets transmitted, 0 received, 100% packet loss, time 9999ms

msfadmin@metasploitable:~$ 192.168.50.1
-bash: 192.168.50.1: command not found
msfadmin@metasploitable:~$ ping 192.168.50.1
PING 192.168.50.1 (192.168.50.1) 56(84) bytes of data.
64 bytes from 192.168.50.1: icmp_seq=1 ttl=64 time=0.216 ms
64 bytes from 192.168.50.1: icmp_seq=2 ttl=64 time=0.165 ms
64 bytes from 192.168.50.1: icmp_seq=3 ttl=64 time=0.152 ms
64 bytes from 192.168.50.1: icmp_seq=4 ttl=64 time=0.149 ms
64 bytes from 192.168.50.1: icmp_seq=5 ttl=64 time=0.169 ms
64 bytes from 192.168.50.1: icmp_seq=6 ttl=64 time=0.151 ms
64 bytes from 192.168.50.1: icmp_seq=7 ttl=64 time=0.155 ms
64 bytes from 192.168.50.1: icmp_seq=8 ttl=64 time=0.160 ms
64 bytes from 192.168.50.1: icmp_seq=9 ttl=64 time=0.186 ms
64 bytes from 192.168.50.1: icmp_seq=10 ttl=64 time=0.474 ms
64 bytes from 192.168.50.1: icmp_seq=11 ttl=64 time=0.154 ms
64 bytes from 192.168.50.1: icmp_seq=12 ttl=64 time=0.158 ms
64 bytes from 192.168.50.1: icmp_seq=13 ttl=64 time=0.150 ms
```

Per arrivare alla richiesta dell'esercizio alla fine si è dovuta impostare una regola sulla LAN che bloccasse il traffico in uscita (con protocollo TCP) verso la Metasploitable (IP 192.168.60.100) sulla porta 80 (HTTP). Questo ha fatto sì che non fosse più possibile collegarsi tramite HTTP alla Metasploitable dalla Kali (mentre le altre porte rimangono aperte come evidenziato dal ping funzionante provato nuovamente dopo aver impostato la suddetta regola). Sotto aggiungo screen di questi passaggi:

Impostazione della regola: Action = Block (blocco della connessione)

Action

Choose what to do with packets that match the criteria specified below.

Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled ☐ Disable this rule

Set this option to disable this rule without removing it from the list.

Interface

Choose the interface from which packets must come to match this rule.

Address Family

Select the Internet Protocol version this rule applies to.

Protocol

Choose which IP protocol this rule should match.

Source ☐ Invert match /

 Display Advanced

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Destination ☐ Invert match /

Port Range
From To

Prova del ping da Metasploitable verso kali dopo impostazione della regola:

```
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=63 time=0.326 ms
64 bytes from 192.168.50.100: icmp_seq=2 ttl=63 time=0.427 ms
64 bytes from 192.168.50.100: icmp_seq=3 ttl=63 time=0.344 ms
64 bytes from 192.168.50.100: icmp_seq=4 ttl=63 time=0.345 ms
64 bytes from 192.168.50.100: icmp_seq=5 ttl=63 time=0.278 ms
64 bytes from 192.168.50.100: icmp_seq=6 ttl=63 time=0.324 ms
64 bytes from 192.168.50.100: icmp_seq=7 ttl=63 time=0.290 ms

--- 192.168.50.100 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 5999ms
rtt min/avg/max/mdev = 0.278/0.333/0.427/0.047 ms
msfadmin@metasploitable:~$
```

Prova di connessione dal browser di Kali Linux verso l'IP della Metasploitable (essendo la porta 80 HTTP bloccata non ci sarà nessuna risposta come rappresentato):

