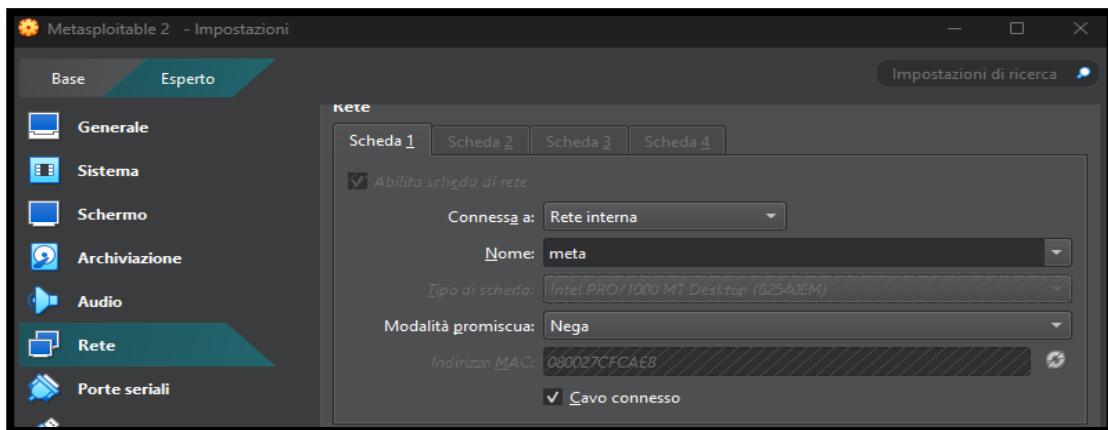


# Creazione policy Pfsense

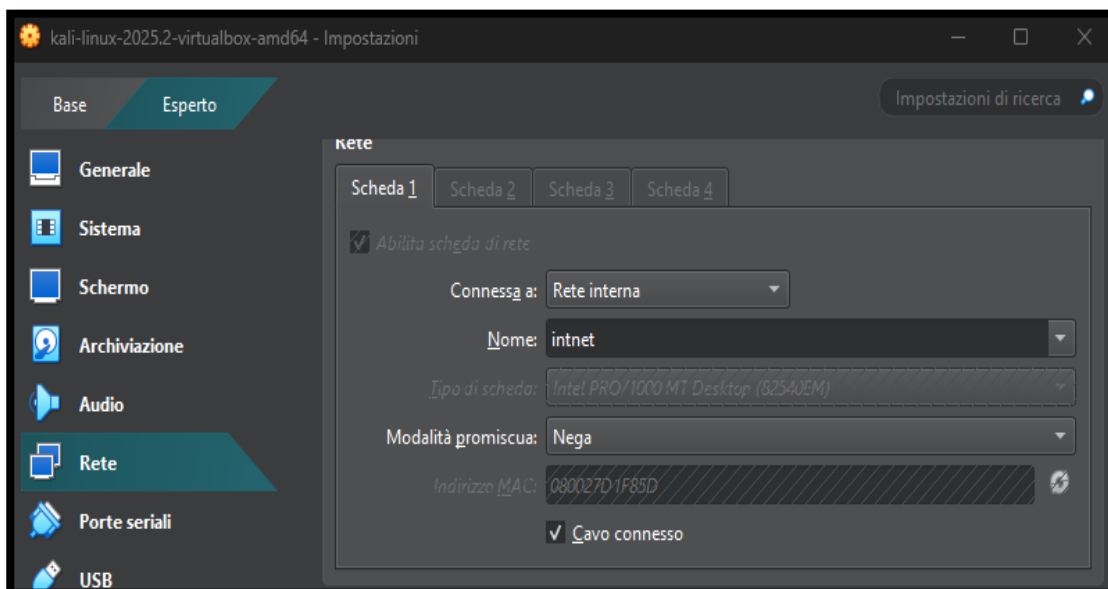
L'esercizio di oggi prevedeva l'uso del nostro laboratorio virtuale, con particolare attenzione al firewall Pfsense, la macchina con Kali Linux e la Metasploitable2.

Come prima cosa ho configurato le schede di rete delle varie macchine virtuali.

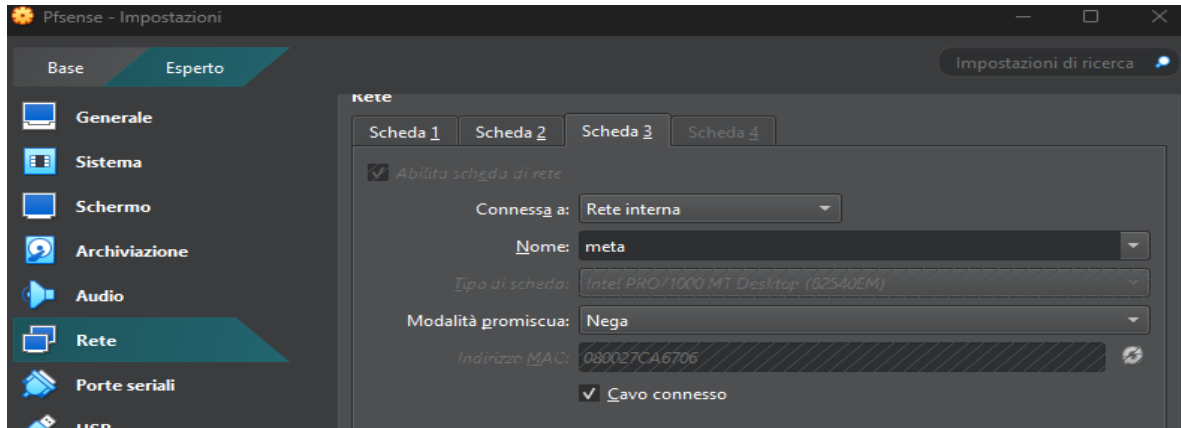
- Metasploitable2



- Kali



- Firewall Pfsense:



La traccia richiedeva anche che la Kali e la Metasploitable fossero in due reti diverse; perciò, ho settato la Kali con indirizzo IP **192.168.50.100** e la Metasploitable con indirizzo IP **192.168.51.100**.

## Obiettivo

Creare una regola firewall che blocchi l'accesso alla DVWA su Metasploitable dalla macchina Kali Linux

1. Come primo step ho aggiunto la nuova interfaccia Meta

Interfaces / **meta (em0)**

General Configuration

Enable ☒ Enable interface

Description

meta

Enter a description (name) for the interface here.

IPv4 Configuration Type

Static IPv4

IPv6 Configuration Type

None

MAC Address

xx:xx:xx:xx:xx:xx

This field can be used to modify ("spoof") the MAC address of this interface.  
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.

MTU

If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

MSS

If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.

Speed and Duplex

Default (no preference, typically autoselect)

Explicitly set speed and duplex mode for this interface.  
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

Static IPv4 Configuration

IPv4 Address

192.168.51.1

/ 24

IPv4 Upstream gateway

None

+ Add a new gateway

Ho settato l'IPv4 statico e come indirizzo ho messo il gateway 192.168.51.1 in modo che le macchine che usano la scheda di rete chiamata meta usino 192.168.51.1 come punto di uscita per quella rete.

2. Poi ho creato le regole firewall in modo da impedire la comunicazione http tra Kali e Metasploitable

Edit Firewall Rule

Action

Block

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

LAN

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

TCP

Choose which IP protocol this rule should match.

Source

Source

☐ Invert match

Address or Alias

192.168.50.100

/

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

Destination

☐ Invert match

Address or Alias

192.168.51.100

/

Destination Port Range

HTTP (80)

From

Custom

HTTP (80)

To

Custom

Ho impostato come azione quella di bloccare il traffico, scelto LAN come interfaccia da cui arrivano i pacchetti e imposto il protocollo su TCP perché blocca specificatamente l'accesso web alla DVWA mantenendo altri servizi funzionanti; infatti, se facessi una prova di ping tra Kali e Metasploitable risulterebbe eseguito con successo. Infine, imposto come IP sorgente l'IP della Kali, come IP destinazione quello di Metasploitable e il range delle porte su 80(porta http).

3. Come prova dell'effettivo funzionamento della regola, ho eseguito uno scan Nmap su porta 80 verso l'indirizzo IP 192.168.51.100(Metasploitable2).

```
(kali㉿kali)-[~]
└─$ nmap -p 80, 192.168.51.100
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-18 10:21 EDT
Nmap scan report for 192.168.51.100
Host is up (0.00085s latency).

PORT      STATE SERVICE
80/tcp    filtered http

Nmap done: 1 IP address (1 host up) scanned in 0.55 seconds
```

La risposta allo scan risulta corretta perché lo stato della porta 80 è filtrata, il che vuol dire che la regola impostata nel firewall funziona.