ESAME S3

Creazione policy Pfsense

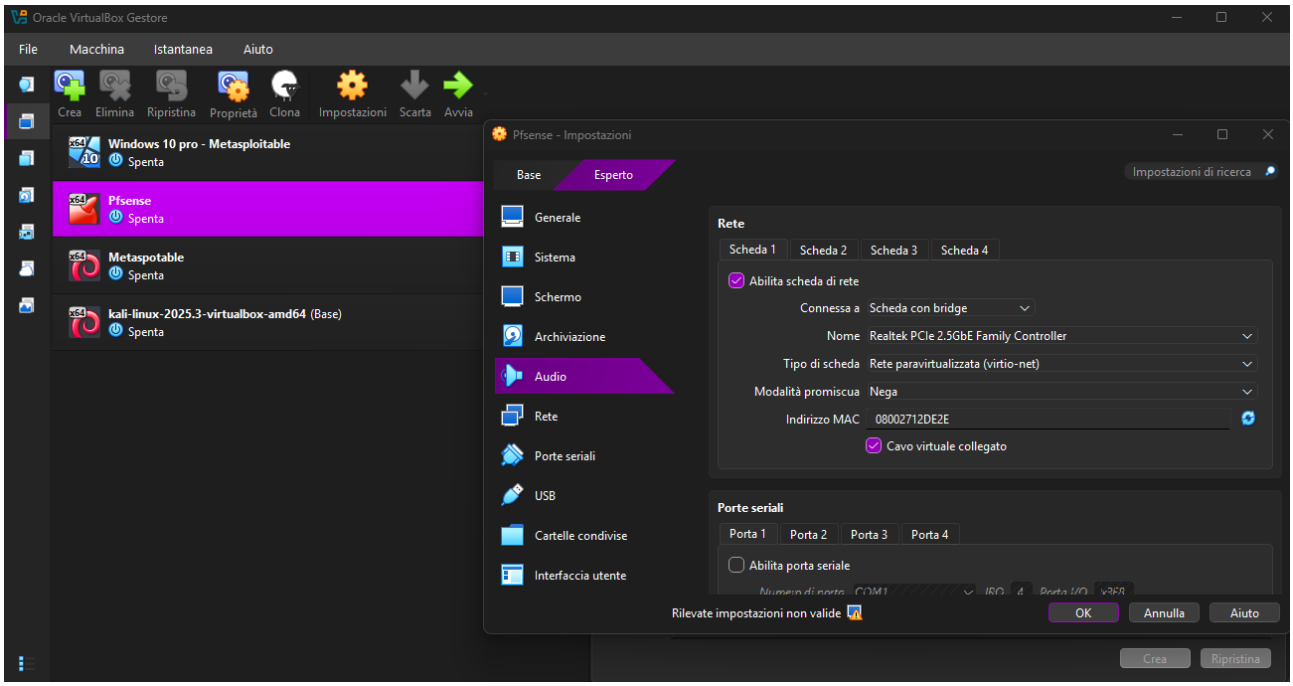
- CONFIGURAZIONE HARDWARE -

Per prima cosa configuro, all'interno di **Virtualbox**, l'hardware relativo alle schede di rete relative alle macchine che utilizzerò per l'esercitazione di oggi.

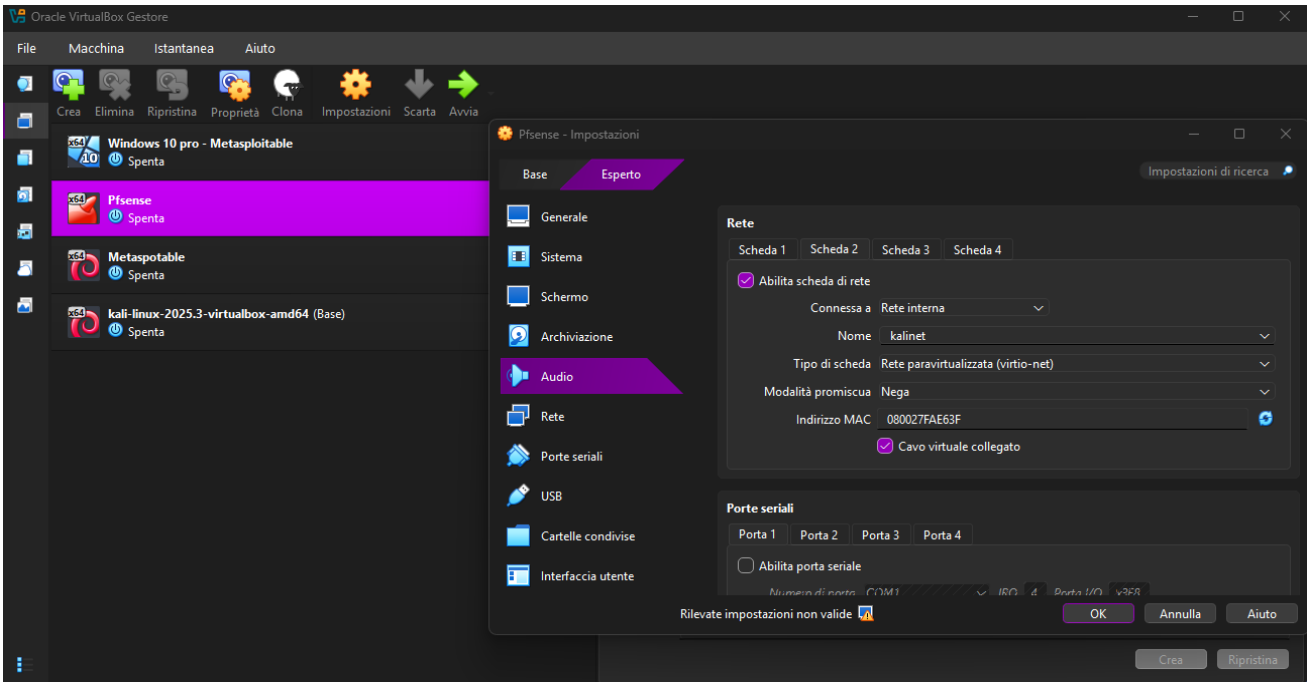
PfSense

Qui dovrò creare tre diverse interfacce di rete perché questa macchina fungerà da intermediario tra le altre due macchine appartenenti a reti diverse, pfSense sarà il nostro **firewall**.

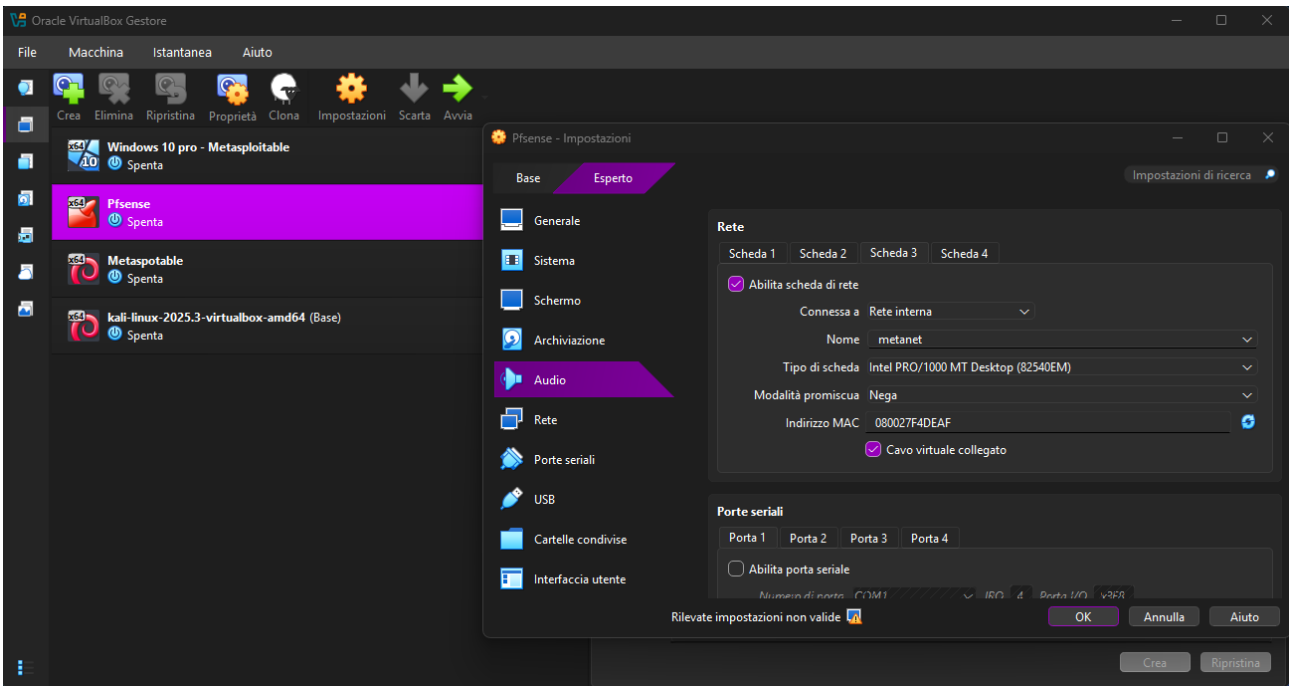
Setto la Scheda 1 in Bridge, connessa cioè alla **WAN** (Internet):



Collego la Scheda 2 alla **LAN** di Kali Linux e la chiamo “kalinet”

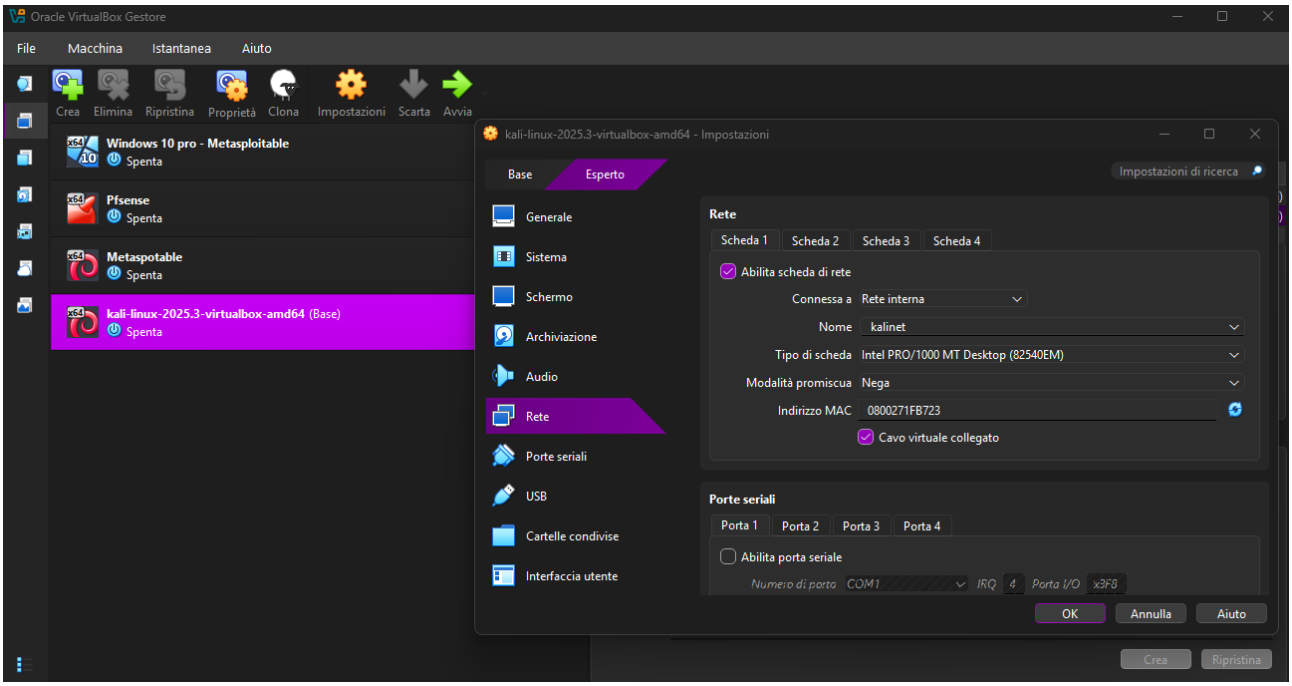


Collego la Scheda 2 alla **LAN** di Metasploitable e la chiamo “metanet”



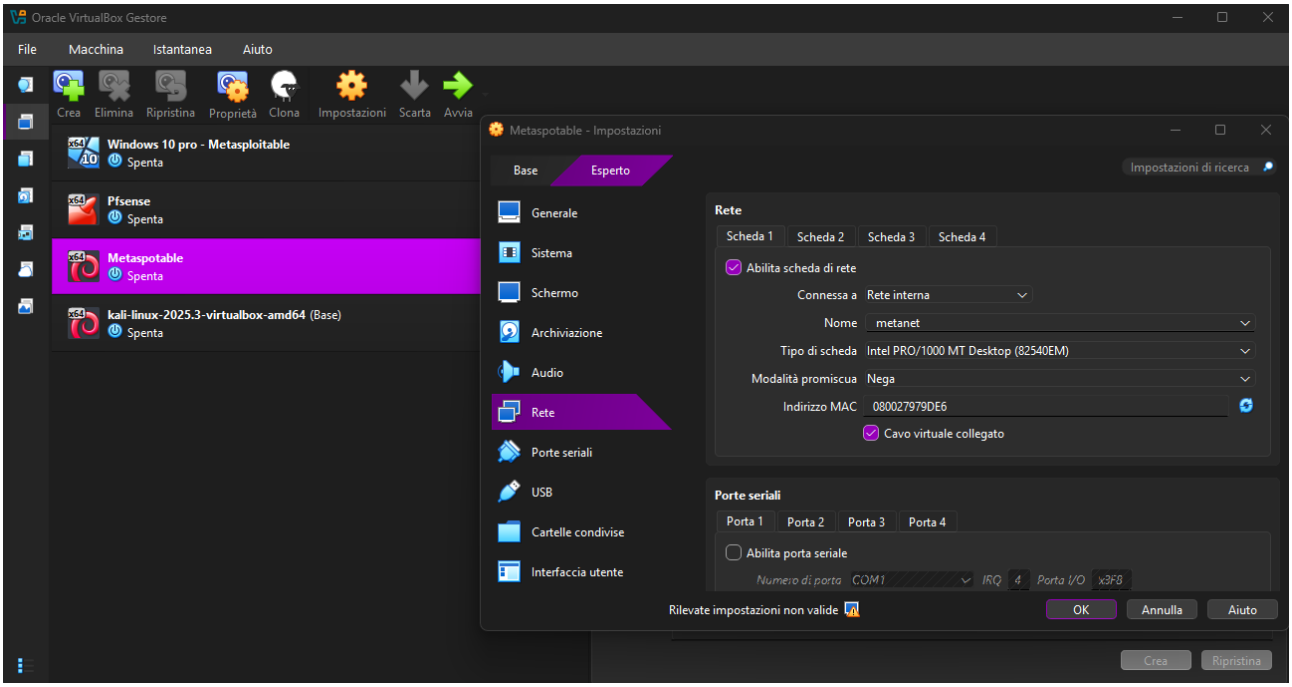
Kali

Per Kali andrò ad impostare la scheda 1 in locale e mi accerto di dare lo stesso nome a questa scheda di rete per simulare una connessione con la macchina pfSense (in questo caso “**kalinet**”)



Metasploitable

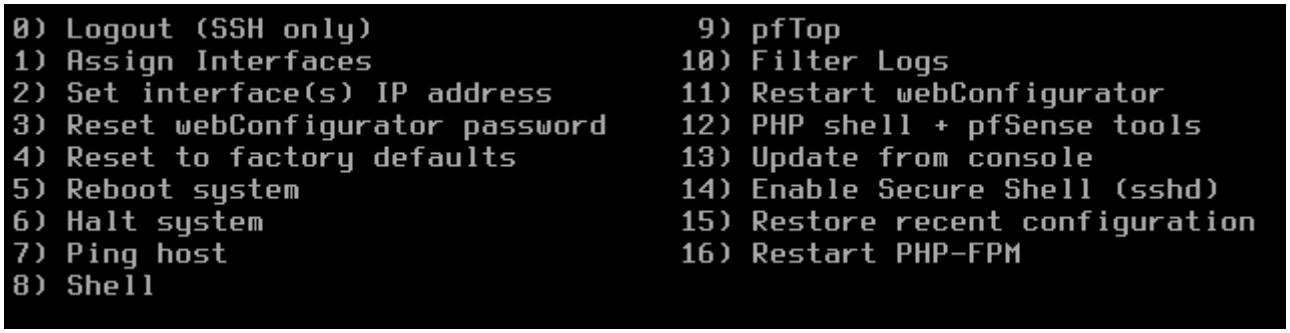
Per Metasploitable andrò ad eseguire lo stesso procedimento ma stando attento questa volta ad inserire il nome che ho assegnato a questa Lan (in questo caso “**metanet**”)



- CONFIGURAZIONE SOFTWARE -

Possiamo adesso accendere la macchina **pfSense** e configurare le nostre reti.
La configurazione è molto semplice in quanto consiste in una serie di domande guidate per poter settare al meglio le nostre LAN.

Nella schermata iniziale vedremo una serie di opzioni che potremo selezionare digitando il numero corrispondente:



A noi interessano le opzioni 1 e 2:

- in “**Assign Interfaces**” andremo ad assegnare le interfacce che noi utilizzeremo; nel nostro caso dovremo creare una interfaccia **WAN** (pfSense), una interfaccia **LAN** (Kali) e una **OPT1** (Metasploitable).
- In “**Set interfaces**” invece configureremo singolarmente le nostre interfacce assegnando gli indirizzi IP che andremo ad utilizzare:
  WAN → 192.168.1.140/24
  LAN → Con DHCP attivo con IPv4 che va da 192.168.50.10 a 192.168.50.100 (Kali)
  OPT1 →Con DHCP attivo con IPv4 che va da 192.168.60.10 a 192.168.60.100 (Metasploitable)

Quando assegniamo le interfacce di rete ci verrà chiesto se impostare o meno le VLAN, non servono per il completamento del nostro test quindi risponderemo /n.

Alla fine della configurazione avremo schermata simile a questa:

- Kali linux -

Una volta avviata Kali entriamo nel nostro browser ed accediamo al sito di gestione di pfSense immettendo come URL l'indirizzo IPv4 che abbiamo impostato poco fa per WAN:

http://192.168.1.140

Dopo aver eseguito l'accesso possiamo andare alla pagina in cui potremo andare a gestire le regole sulle quali si baserà il nostro firewall:

Firewall → Rules → LAN

Da questa schermata clicchiamo su **Add** per aggiungere una nuova regola al firewall.

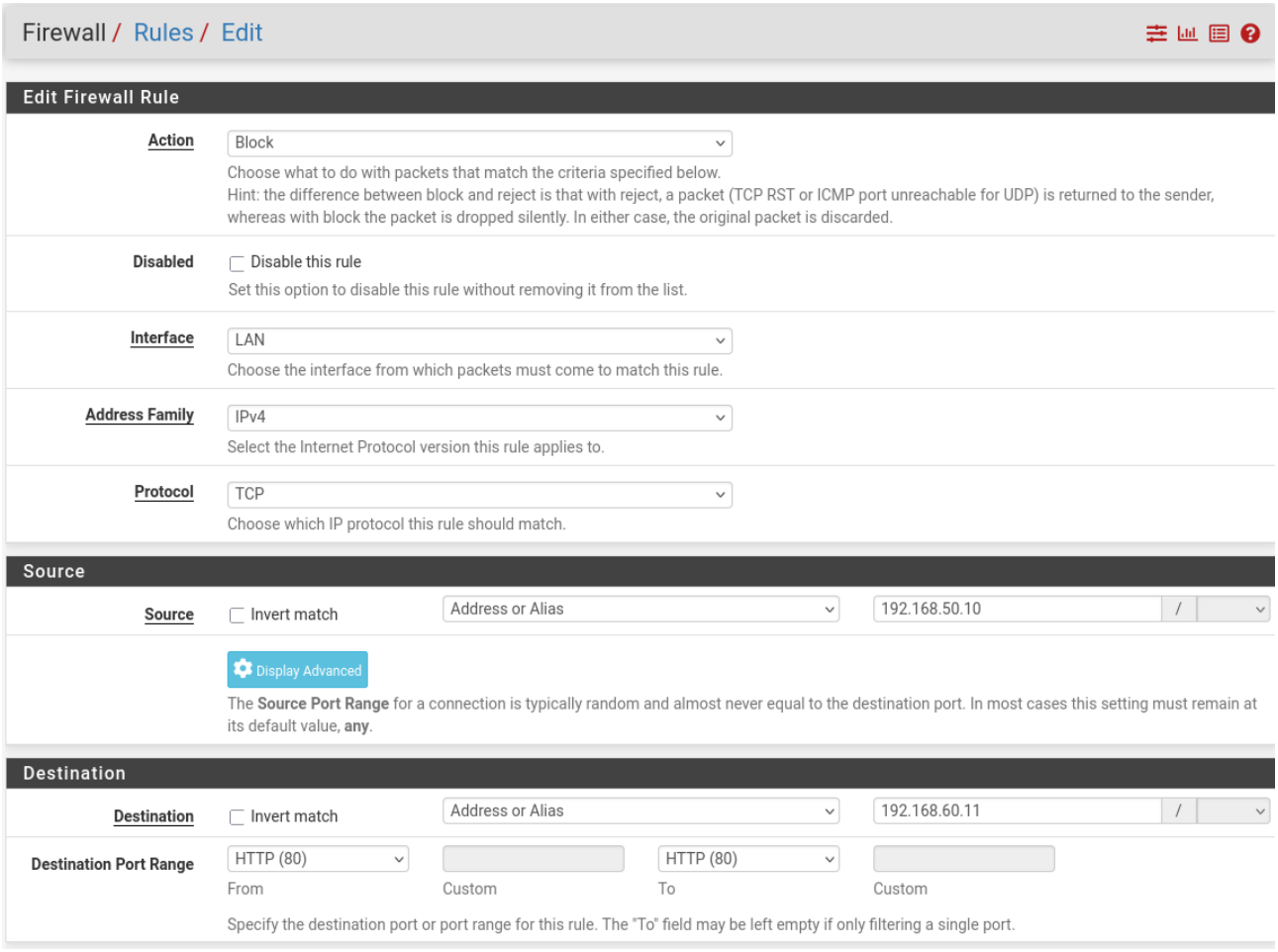
Adesso possiamo compilare un form in cui specifichiamo vari dettagli sulla regola che stiamo impostando:

- Action: Block, perchè vogliamo bloccare (silenziosamente) ogni tentativo di comunicazione di Kali alla Metasploitable.

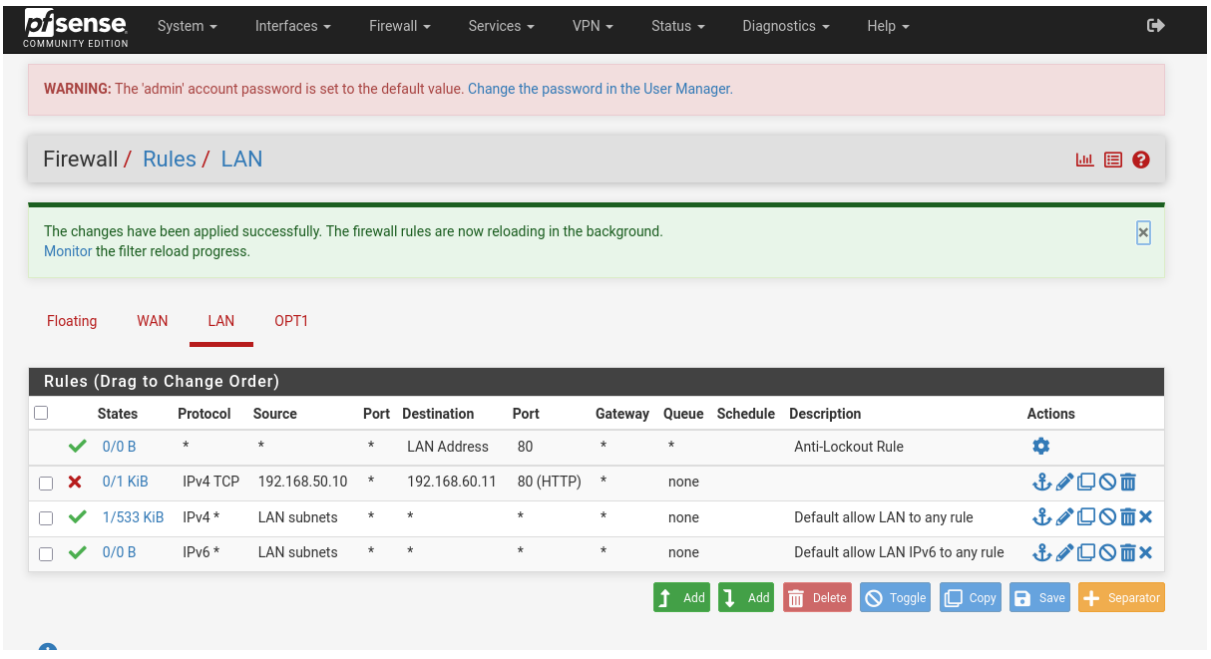
- Protocol: lasciamo solo il TCP (Cosi da non bloccare anche il ping ICMP).

- Source: seleziono "Address or Alias" ed inserirò l'IP del mio Kali 192.168.50.10

- Destination: seleziono anche qui “Address or Alias” ed inserirò l’IP del mio Metasploitable 192.168.60.11, infine blocchiamo solo la porta 80 (HTTP)



Cliccando su “**Save**” e successivamente su “**Apply changes**” abbiamo confermato la regola che impedisce a Kali di comunicare alla porta 80 con Metasploitable.

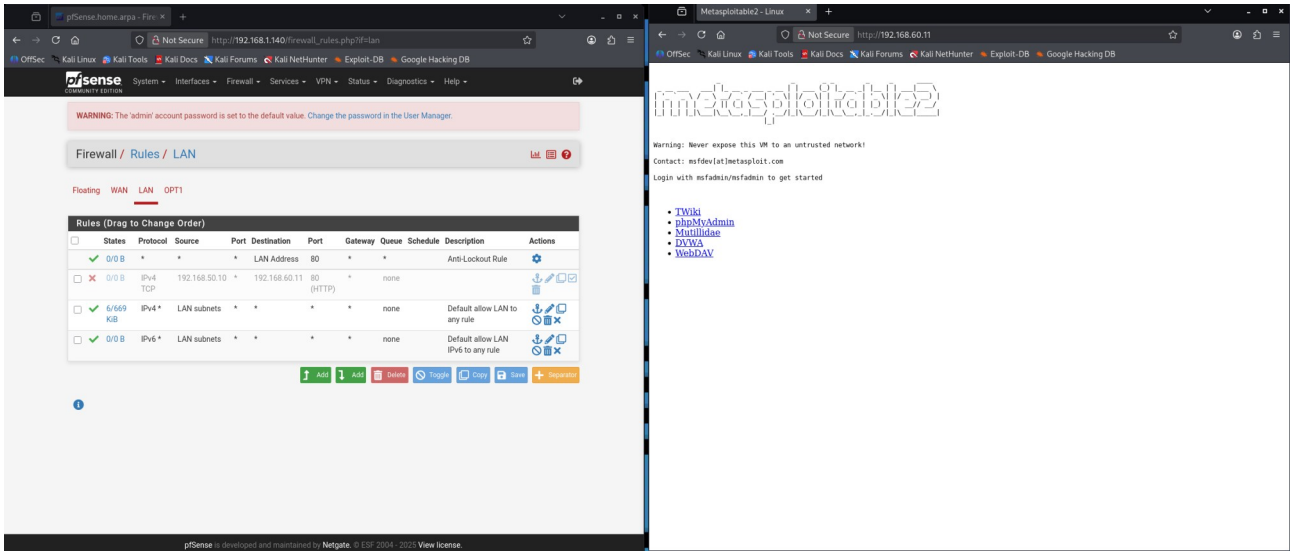


- Testing -

Adesso non ci resta altro che tentare di accedere alla macchina Metasploitable da Linux tramite browser per verificare che il nostro firewall è stato configurato correttamente.

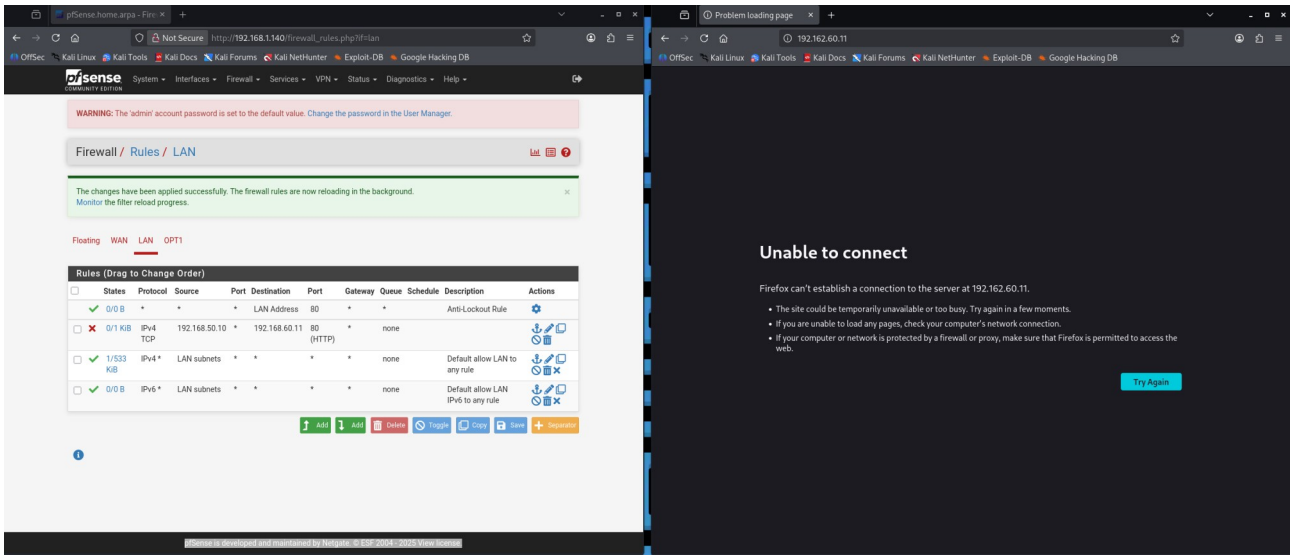
Disattivo temporaneamente la regola di blocco su pfSense e provo ad accedere alla macchina Metasploitable tramite il suo indirizzo:

http://192.168.60.5.



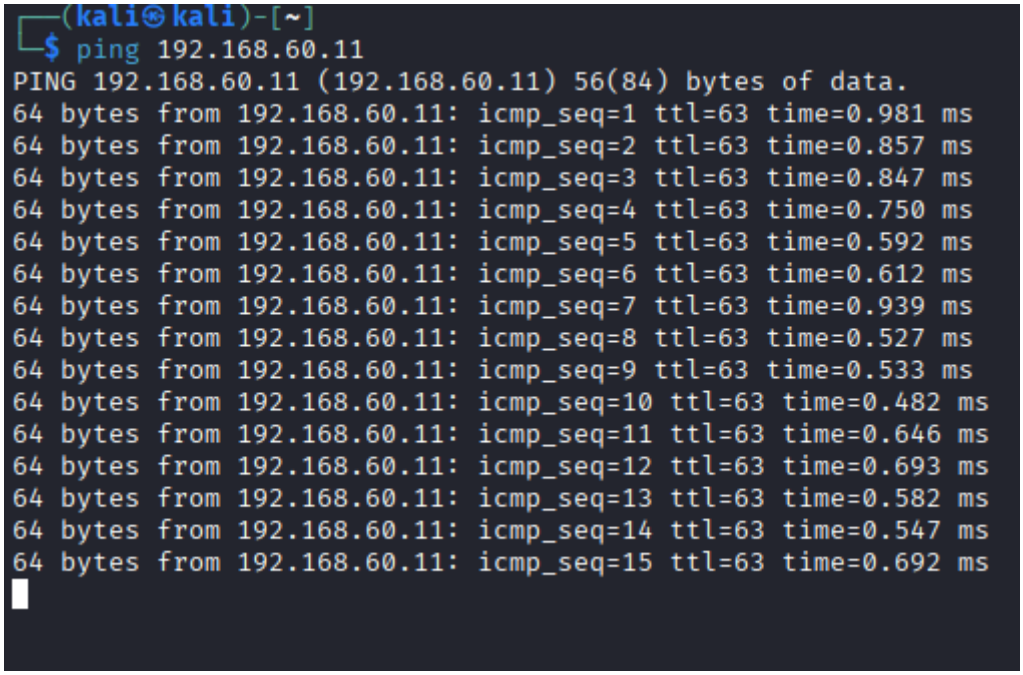
Riusciamo a connetterci tranquillamente.

Riattivo la regola di blocco e riprovo ad accedere a http://192.168.60.5.



Non riusciamo a connetterci, la connessione va in Time Out.

Se effettuiamo il ping da Kali a Metasploitable otteniamo risposta poiché noi abbiamo bloccato solo il **TCP** della porta 80 e non l'**ICMP**



Nicolò Calì