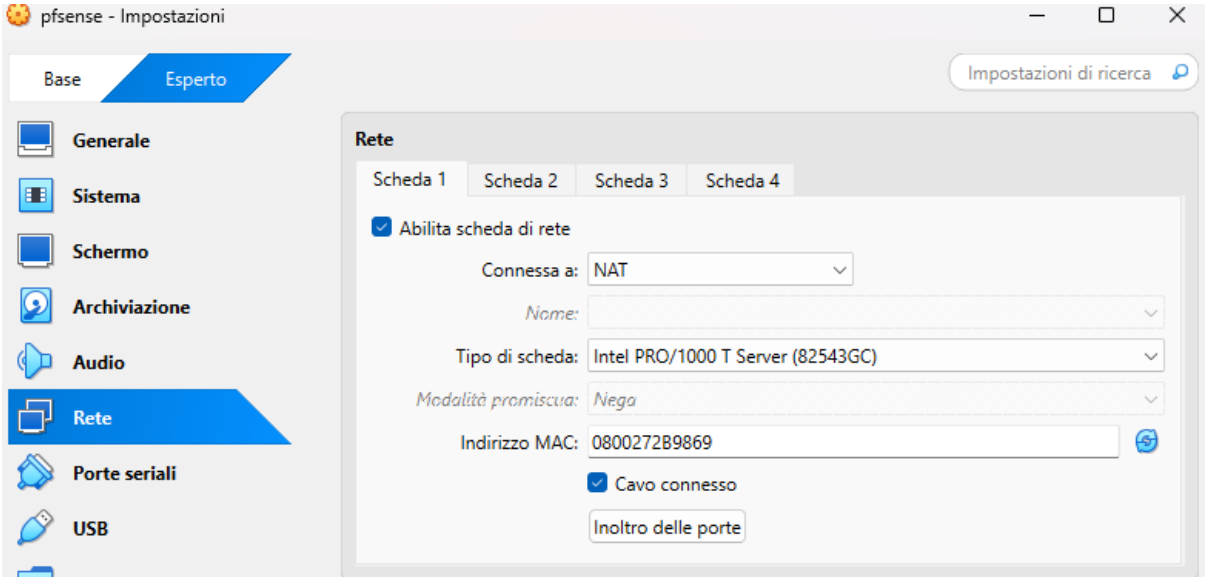
Report Esercizio 13/12/2024

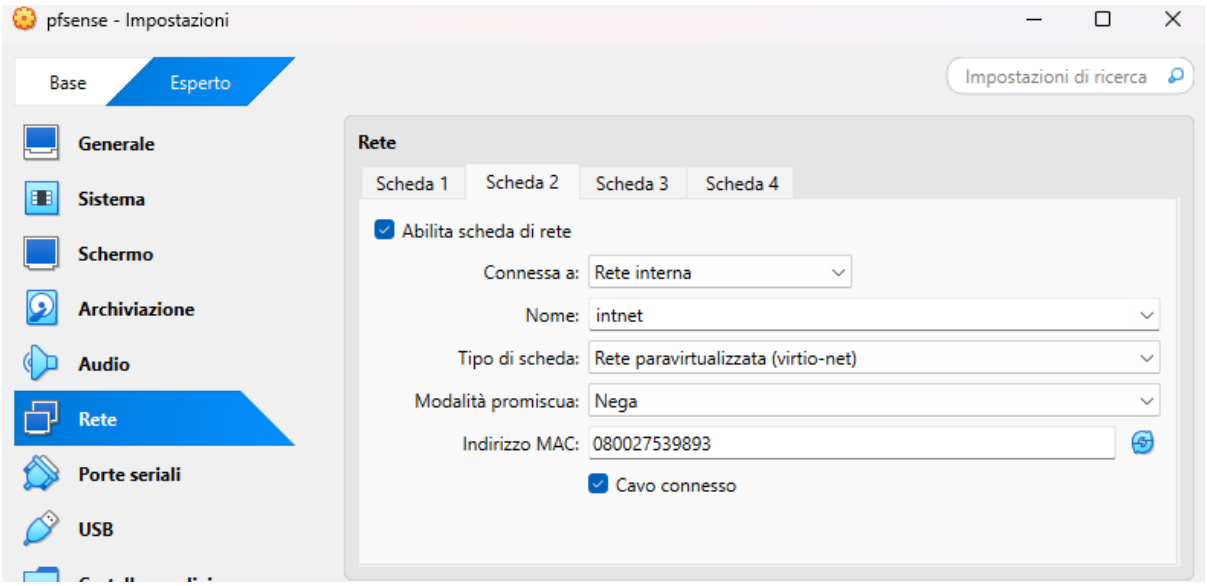
Progetto Firewall Leonardo Catalano

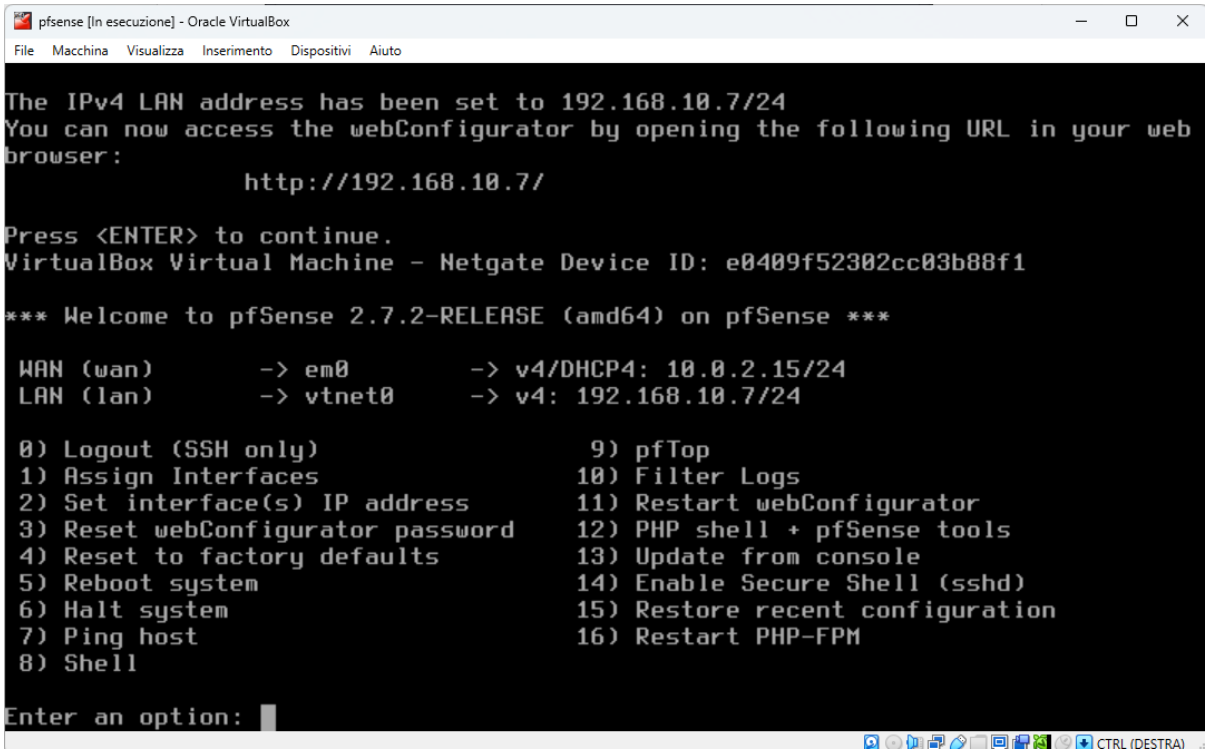
“La traccia di oggi ci chiede di creare una policy su pfsense facendo una nuova regola firewall, che blocchi l’accesso alla DVWA (su metasploitable) dalla macchina kali linux e ne impedisca lo scan.”
Bonus: “Creare una regola che impedisca da kali l’accesso a metasploitable tramite il protocollo telnet (porta 23)”.
Le reti kali e Metasploitable devono essere su reti diverse.

Allora prima di iniziare accendiamo le macchine.

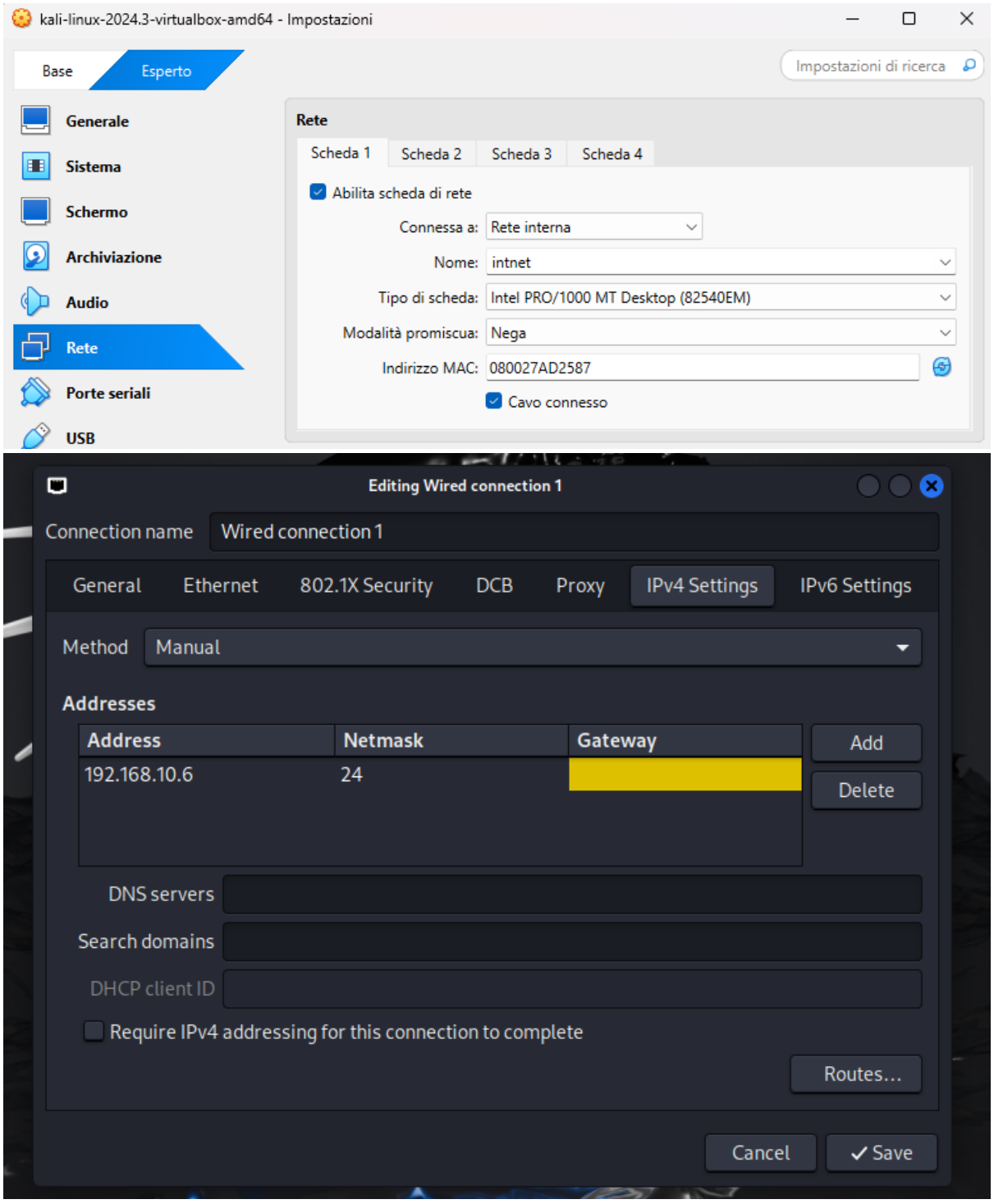
Pfsense: (Scheda 1 Nat – Scheda 2 Rete interna)


pfsense - Impostazioni
Base
Esperto
Impostazioni di ricerca
Generale
Sistema
Schermo
Archiviazione
Audio
Rete
Porte seriali
USB
Rete
Scheda 1
Scheda 2
Scheda 3
Scheda 4
Abilita scheda di rete
Connessa a:
NAT
Nome:
Tipo di scheda:
Intel PRO/1000 T Server (82543GC)
Modalità promiscua:
Nega
Indirizzo MAC:
080027B9869
Cavo connesso
Inoltro delle porte

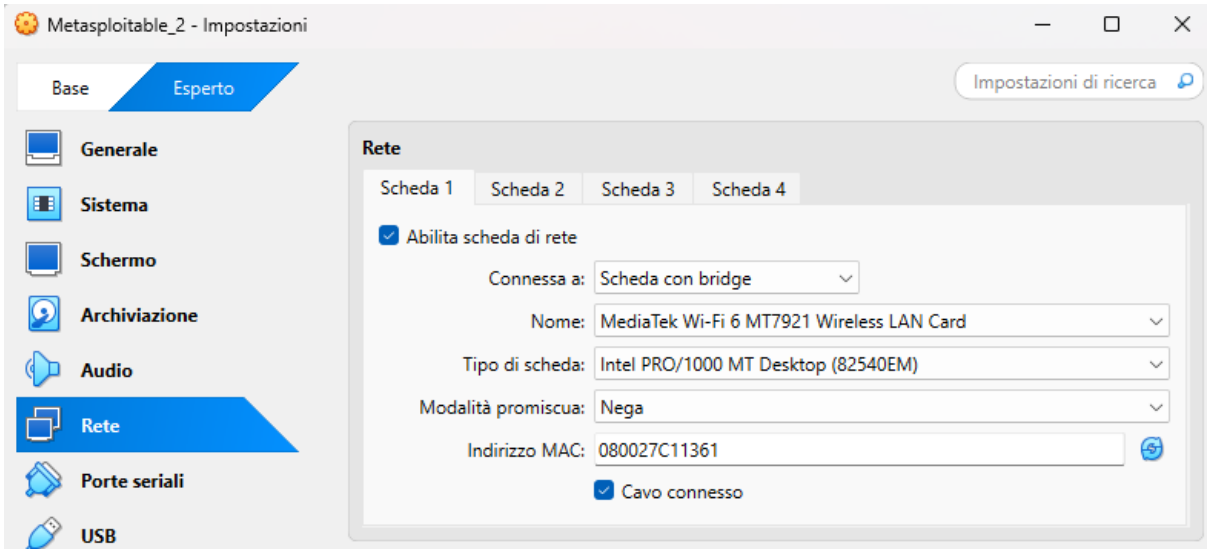

pfsense - Impostazioni
Base
Esperto
Impostazioni di ricerca
Generale
Sistema
Schermo
Archiviazione
Audio
Rete
Porte seriali
USB
Rete
Scheda 1
Scheda 2
Scheda 3
Scheda 4
Abilita scheda di rete
Connessa a:
Rete interna
Nome:
intnet
Tipo di scheda:
Rete paravirtualizzata (virtio-net)
Modalità promiscua:
Nega
Indirizzo MAC:
080027539893
Cavo connesso

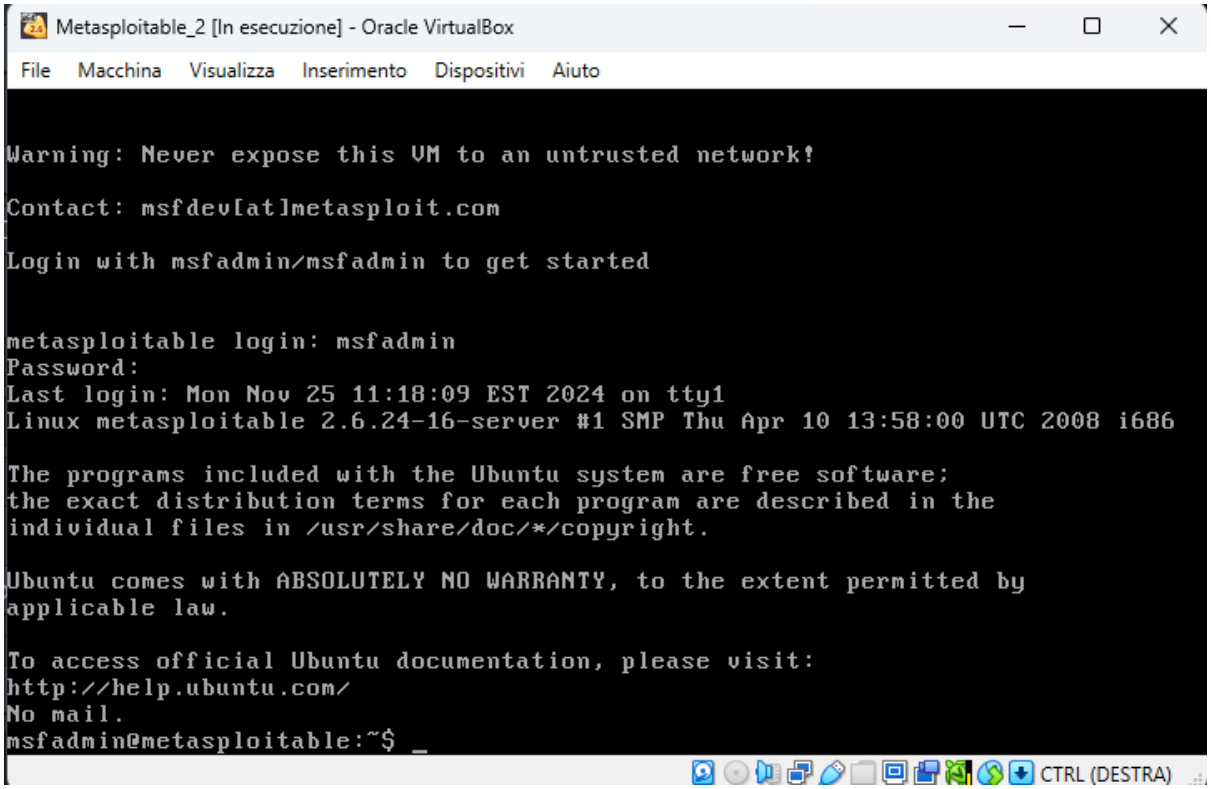


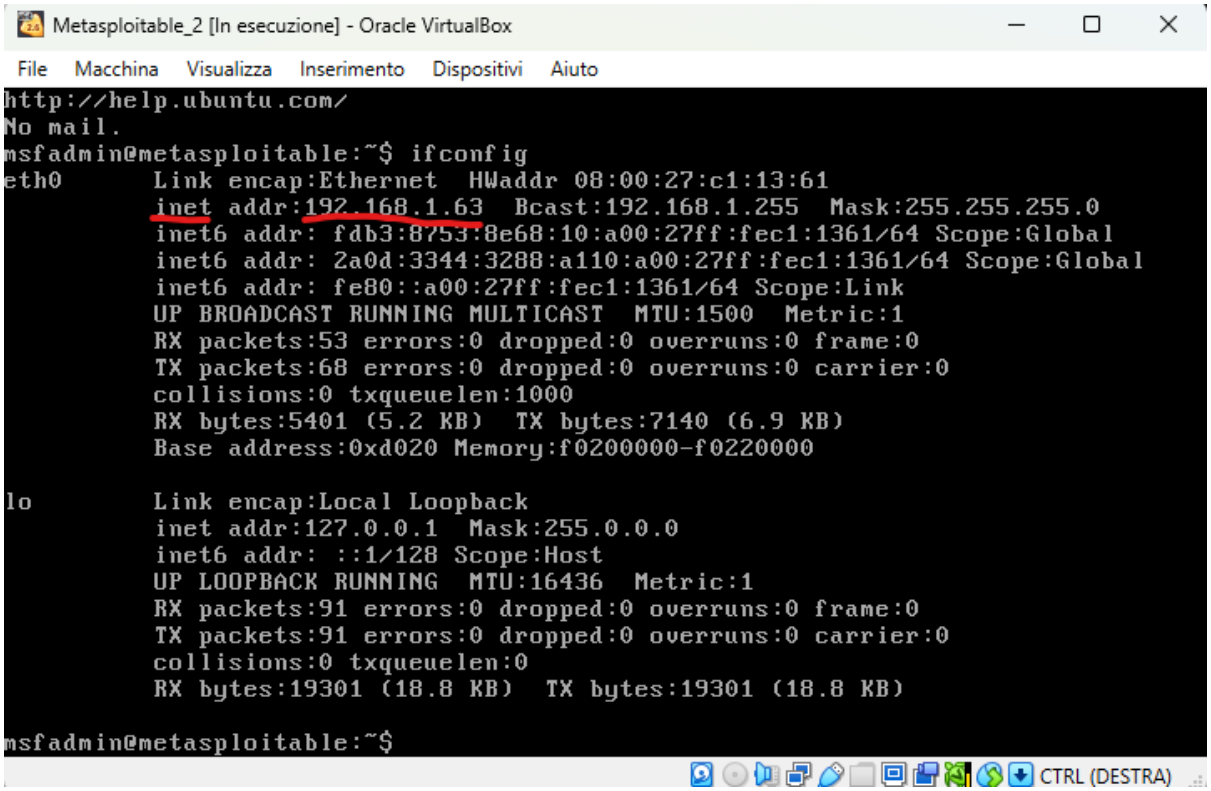
Kali: (Scheda 1 Rete locale)



Metasploitable 2: (Scheda 1 Scheda con bridge)

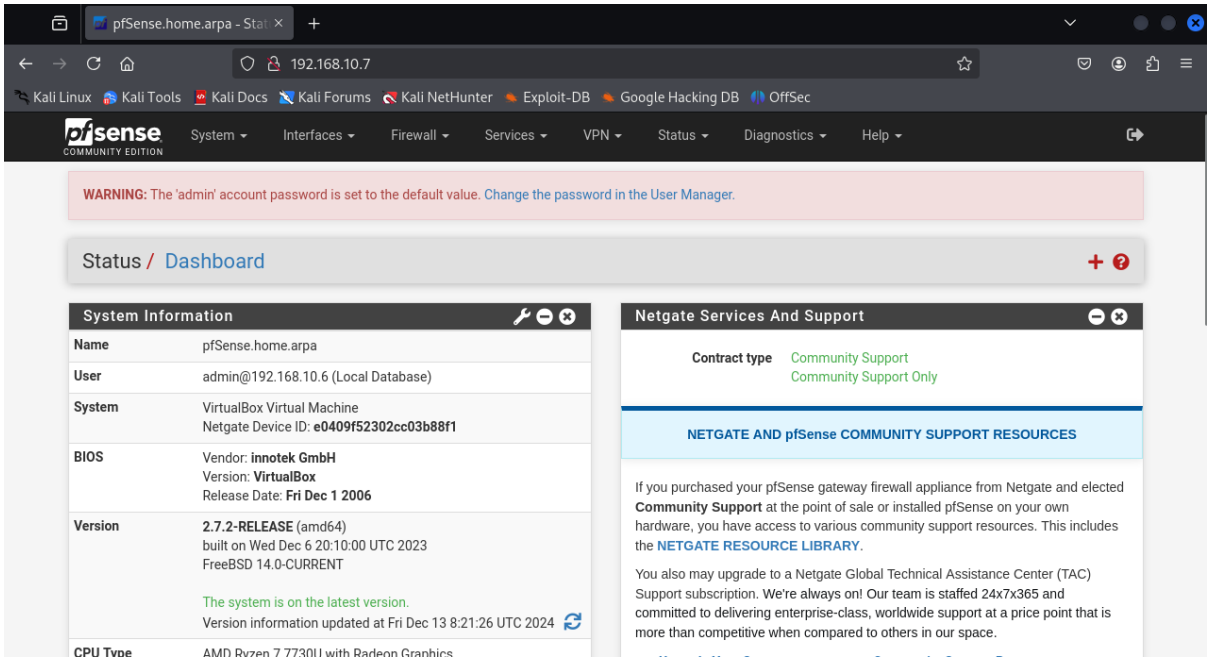

Metasploitable_2 - Impostazioni
Base
Esperto
Impostazioni di ricerca
Generale
Sistema
Schermo
Archiviazione
Audio
Rete
Porte seriali
USB
Rete
Scheda 1
Scheda 2
Scheda 3
Scheda 4
Abilita scheda di rete
Connessa a:
Scheda con bridge
Nome:
MediaTek Wi-Fi 6 MT7921 Wireless LAN Card
Tipo di scheda:
Intel PRO/1000 MT Desktop (82540EM)
Modalità promiscua:
Nega
Indirizzo MAC:
080027C11361
Cavo connesso


Metasploitable_2 [In esecuzione] - Oracle VirtualBox
File
Macchina
Visualizza
Inserimento
Dispositivi
Aiuto
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
metasploitable login: msfadmin
Password:
Last login: Mon Nov 25 11:18:09 EST 2024 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:~$ _
CTRL (DESTRA)



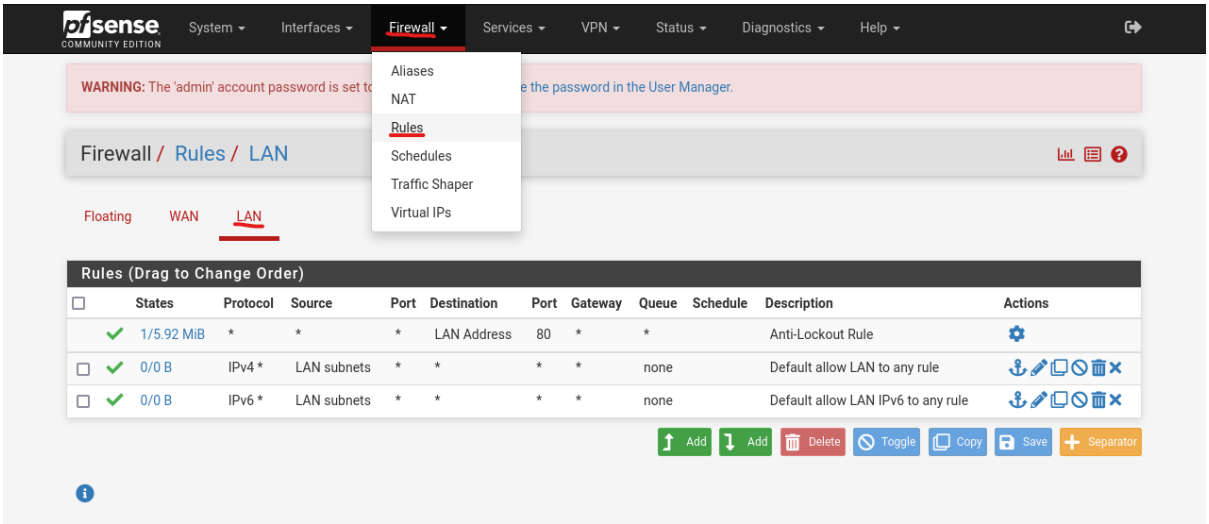
(Ho messo la scheda in bridge perchè senò se mettevo in rete locale mi dava l'indirizzo con ipv6.)

Poi si accede con il browser su kali all'interfaccia di configurazione di pfsense.



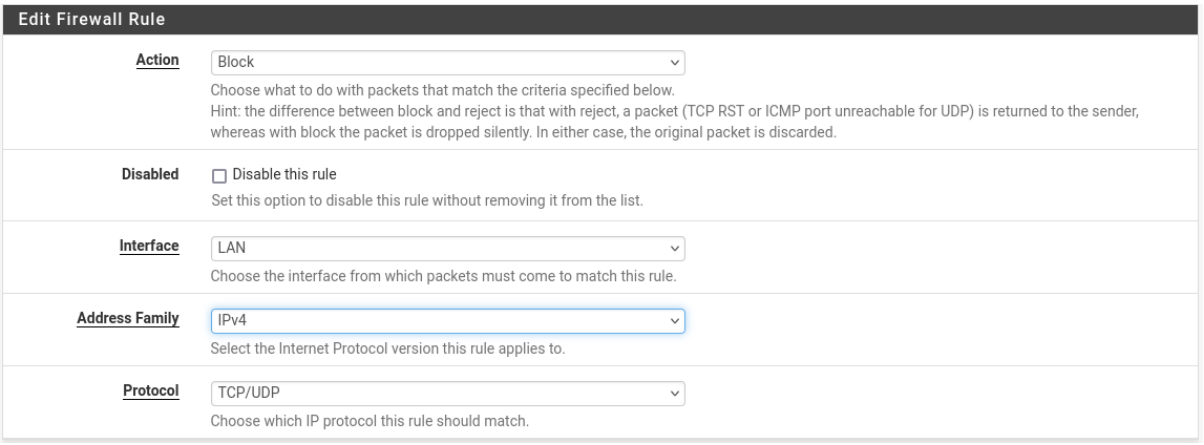
E si comincia la procedura di policy.

Per creare una nuova regola firewall bisogna andare su :
Firewall->Rules-> Sezione Lan e clicchiamo su Add.

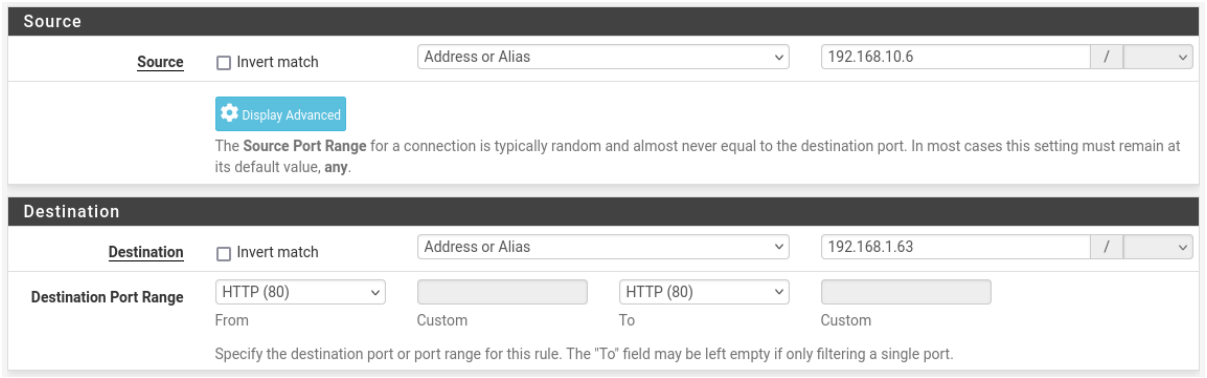


Successivamente avremo un'interfaccia dove avremo dei settaggi da effettuare:

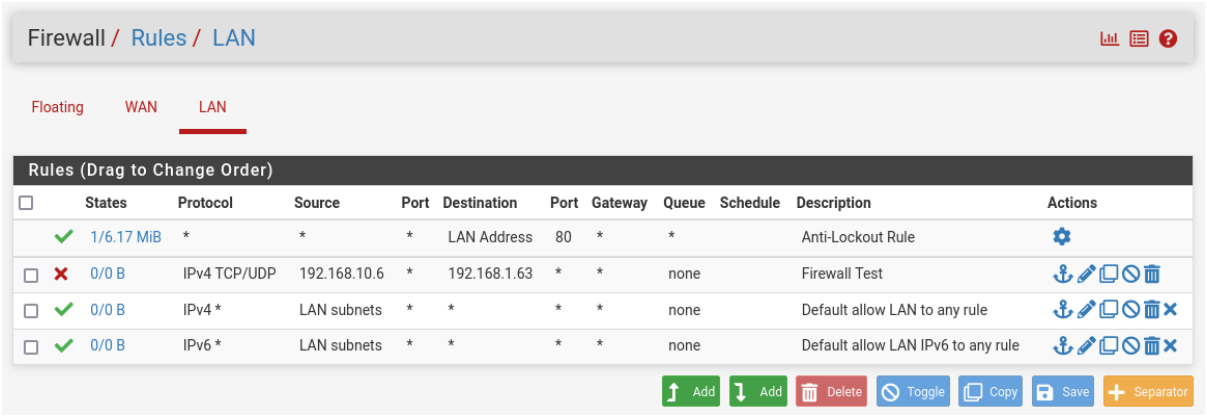
Action: in questa sezione si può scegliere come gestire il traffico se farlo passare o bloccarlo. (In questo caso scegliamo Block per impedire il passaggio del traffico)
Interface: L'interfaccia da dove arrivano i pacchetti
Address family: La versione del protocollo Ipv4 o Ipv6 a quale applicare la policy.
Protocol: Si sceglie il protocollo (tcp, udp ...)



Source: In questa sezione si può scegliere che tipo di sorgente inserire, come un indirizzo ipv4/6 network ... , in questo caso si inserisce l'ipv4 della macchina kali (192.168.10.6).
Destination: In questa sezione si può scegliere che tipo di sorgente inserire, come un indirizzo ipv4/6 network..., in questo caso si inserisce l'ipv4 della macchina metaspoitable (192.168.1.63)
Destination port range: In questa sezione si specificano le porte destinazione. (In questo caso si inserisce la porta di default per le richieste http (80).

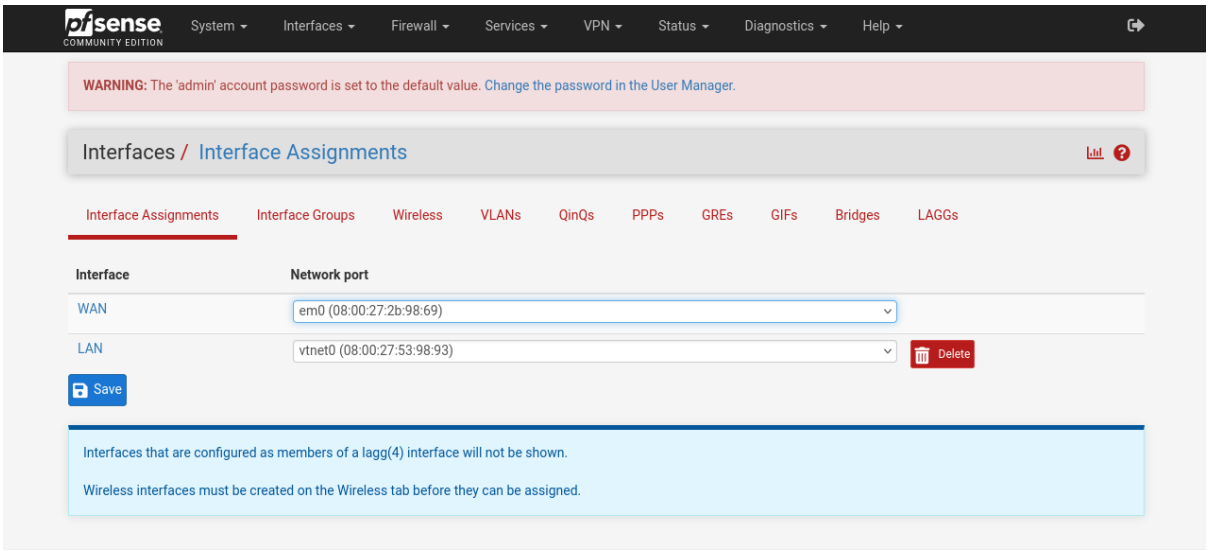


Si clicca infine su Save e la regola Firewall verrà creata:



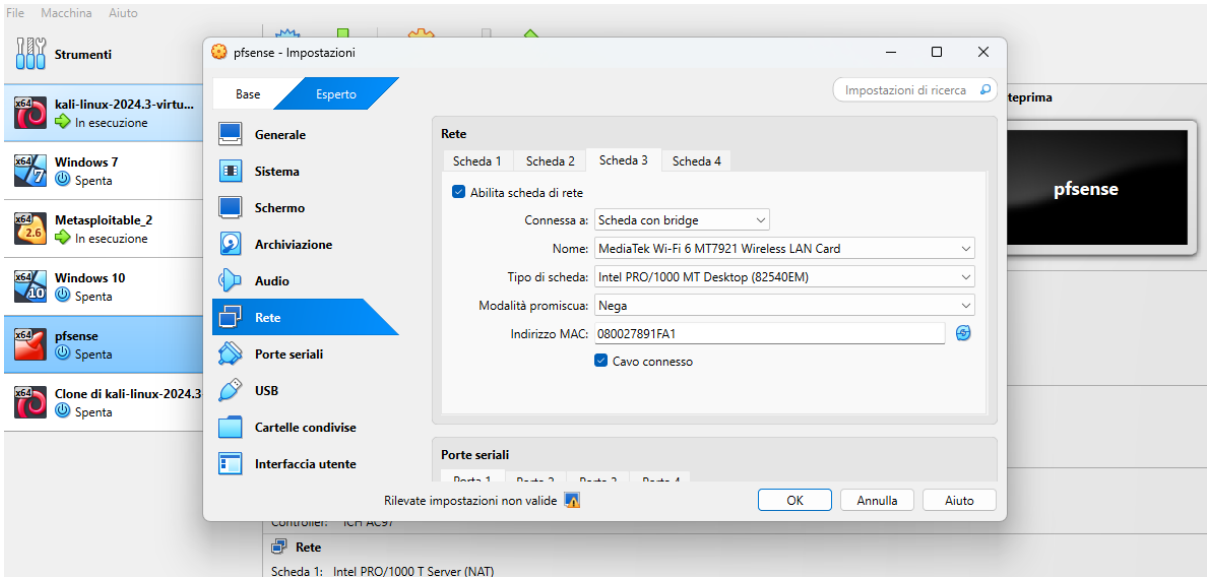
Ora bisogna creare l'interfaccia per l'altra rete (192.168.1.0) ossia quella di metaspoitable senò pfsense non la conosce.

Si va su Interfaces --> Interface Assignments

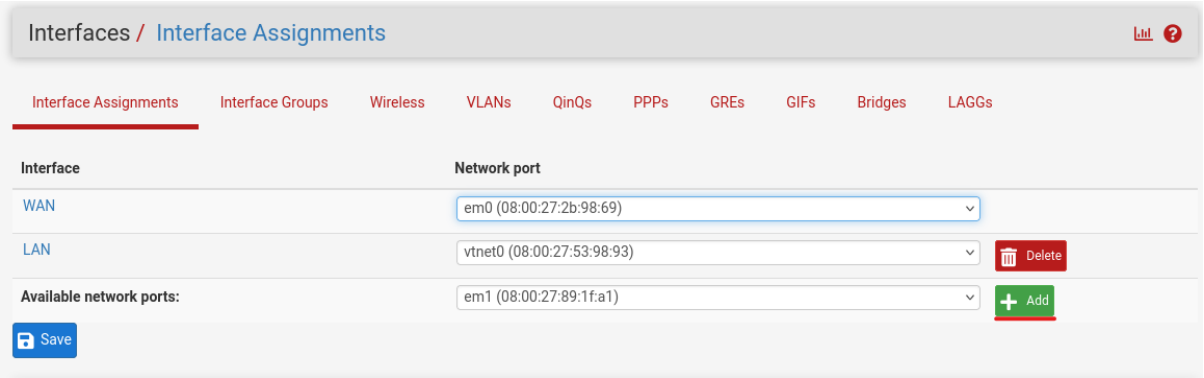


Come vediamo però abbiamo solamente 2 interfacce una per la wan e una per la lan, quindi bisogna aggiungerne una 3* per l'altra rete.

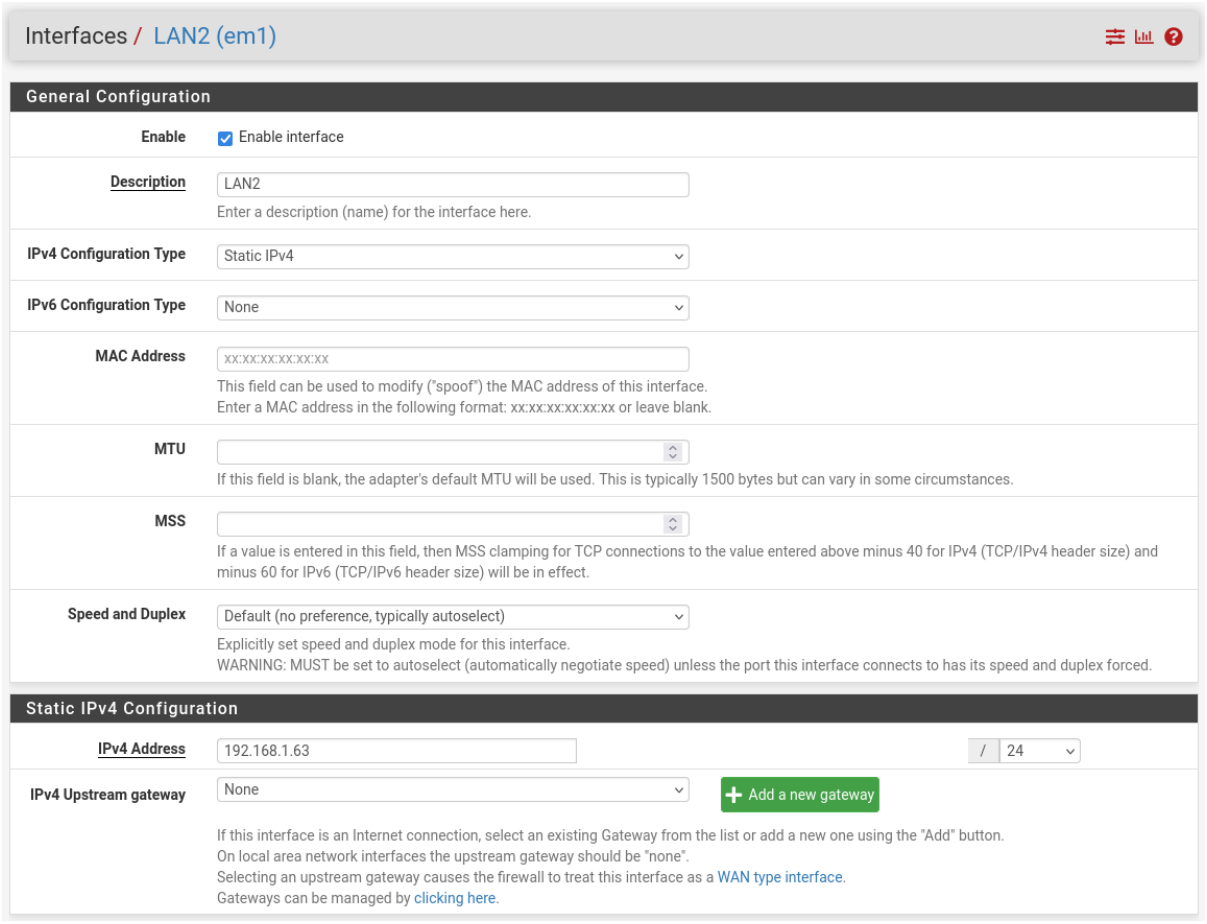
Si torna quindi in questo caso su VirtualBox, pfsense e si aggiunge una 3* scheda di rete.



Cosi' facendo dopo che si è riavviata la macchina pfsense, se si torna sull'interfaccia gui nella sezione Interface, possiamo configurare la 3* interfaccia.

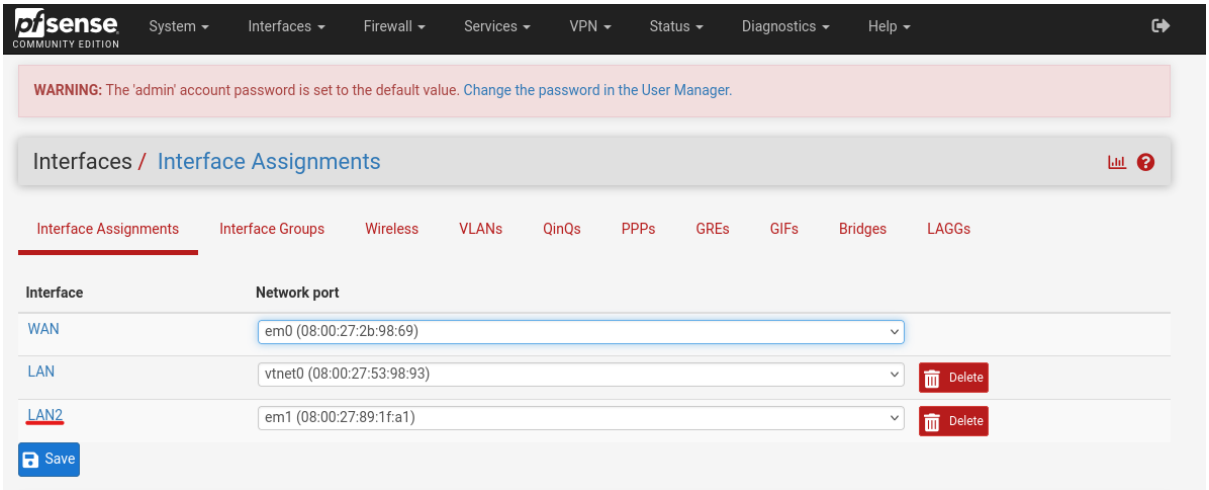


Ora andiamo a crearla e a settarla:



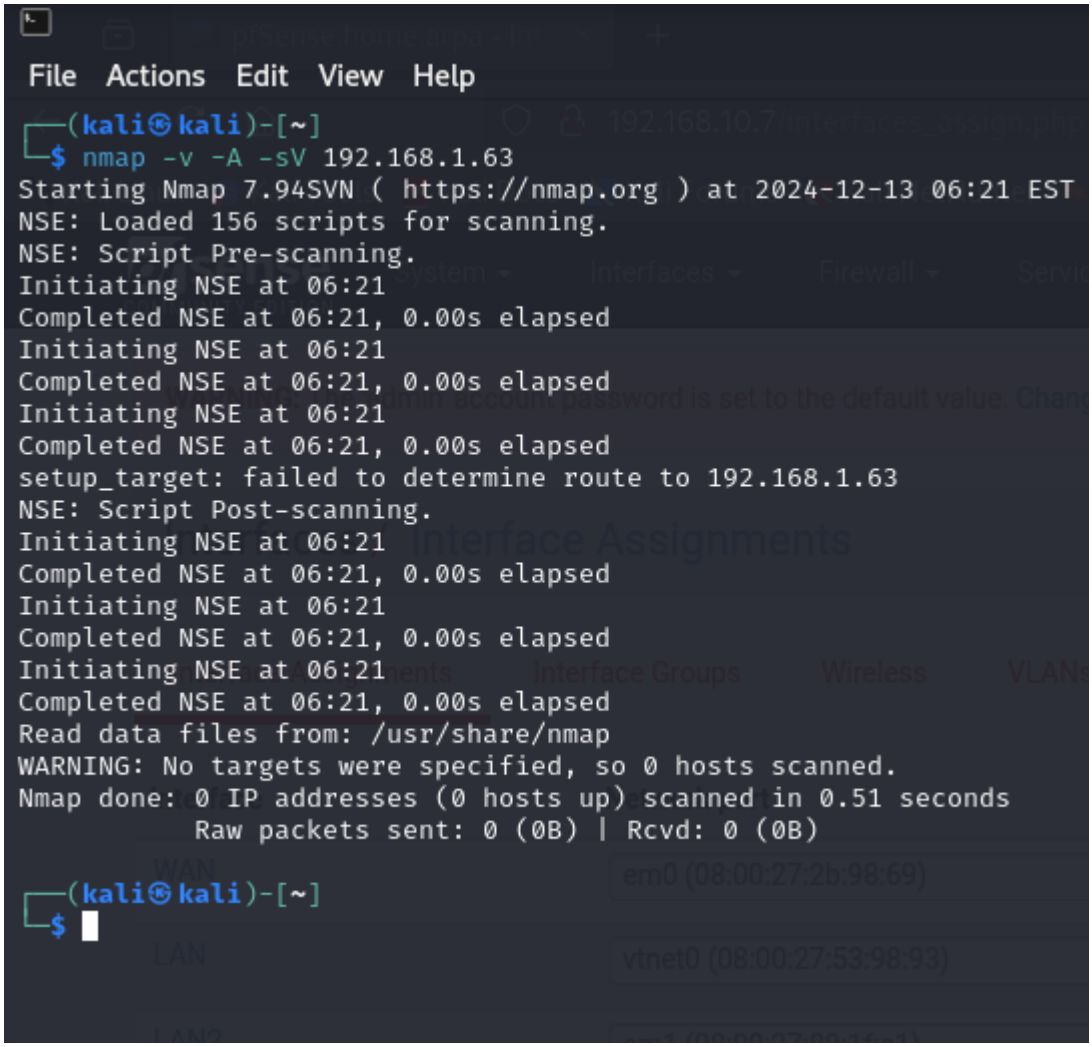
Gli assegniamo il nome (Lan2), tipo ip Static IPV4, e gli configuriamo l'ipv4 della macchina metasploitable (192.168.1.63 /24).

Si clicca su save e controlliamo se l'interfaccia è stata creata.



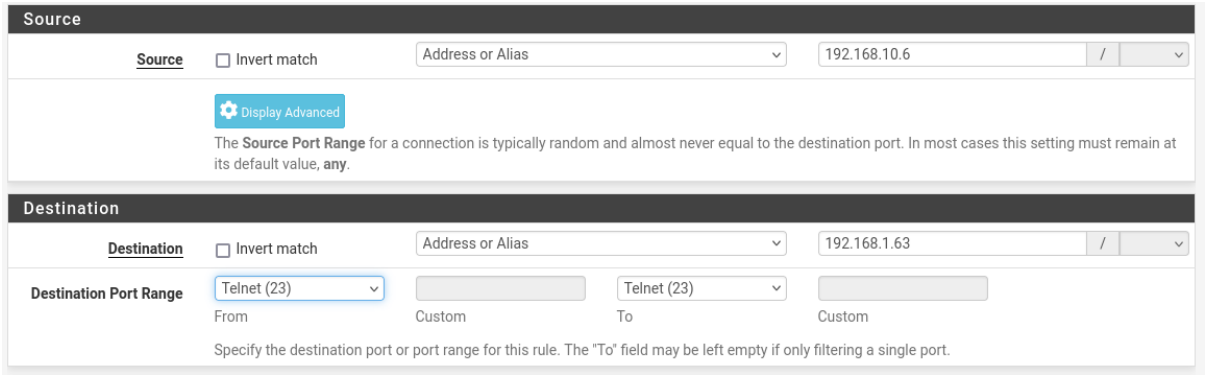
Infine andiamo ad effettuare la prova di scansione delle porte e dei servizi sulla macchina Metasploitable, da kali utilizziamo il comando:

”nmap -v -A –sV 192.168.1.63”

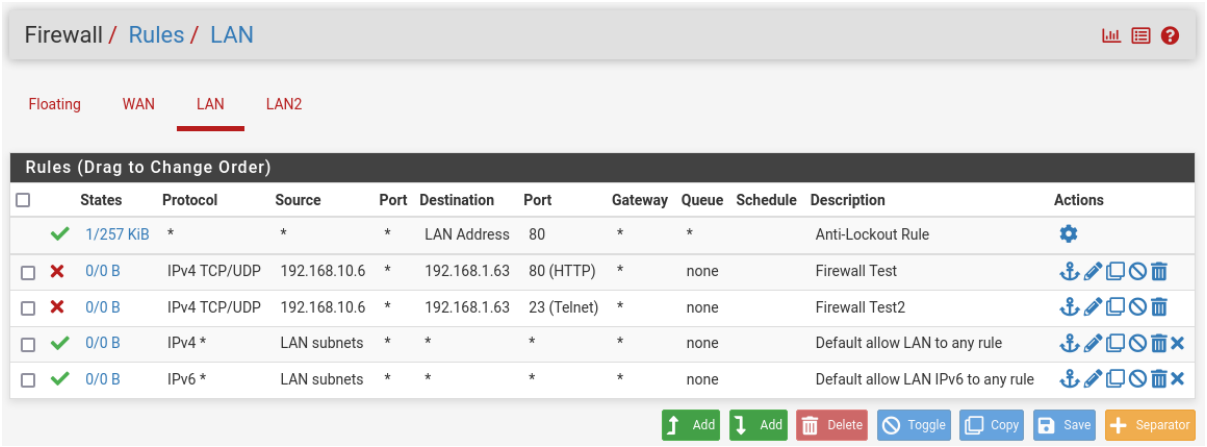


Avendo aggiunto la regola nel firewall lo scan da kali a metasploit non funziona, non riuscendo ad accedere a metasploitable, essendo che la regola è stata impostata su “Block”, il firewall impedirà il traffico che proviene dalla macchina kali (192.168.10.6) alla macchina Metasploitable (192.168.1.63) .

Per l’esercizio Bonus bisogna creare una regola su pfsense per bloccare da kali il telnet verso metasploitable, quindi bisogna creare una medesima regola soltanto cambiando la porta invece della porta 80, http di base, si mette la porta 23 standard del telnet.
Si va nella sezione Rules--> Lan e si crea una medesima regola cambiando soltanto la sezione Destination Port range, mettendo la porta 23 (predefinita del Telnet).

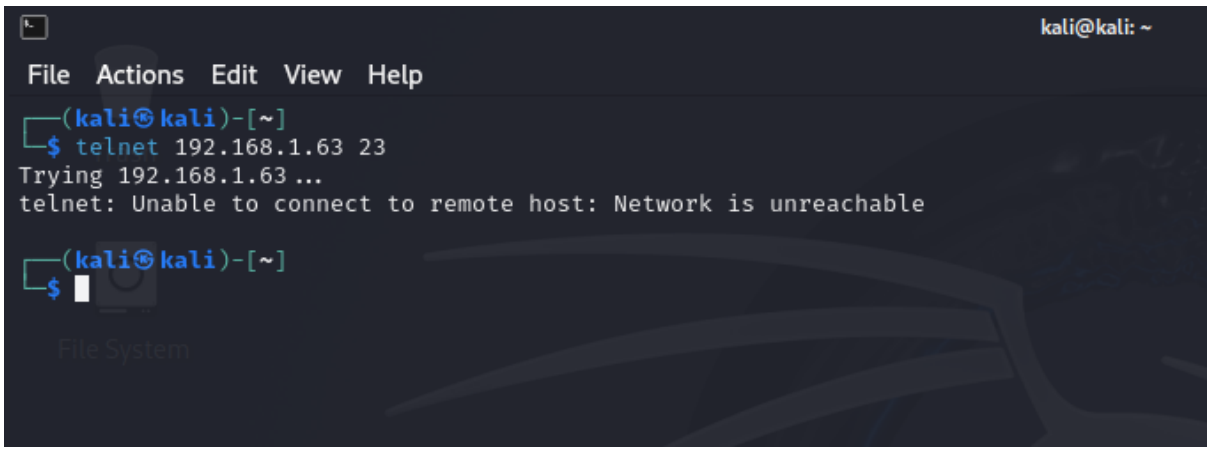


Infine avremo una situazione di questo tipo:



Ora per testare se il blocco funziona bisogna usare il comando: telnet + ip + porta dalla shell di kali:

“telnet 192.168.1.63 23” (indirizzo ip + porta)



Come da Output anche qui la 2* regola del firewall ha bloccato l’accesso al servizio Telnet da Kali verso Metasploitable.