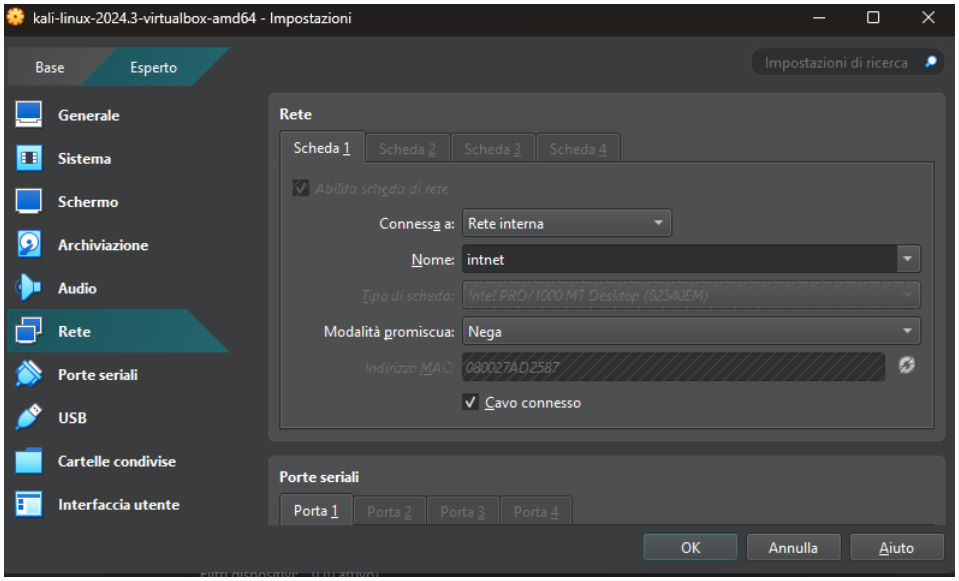
S3/L5

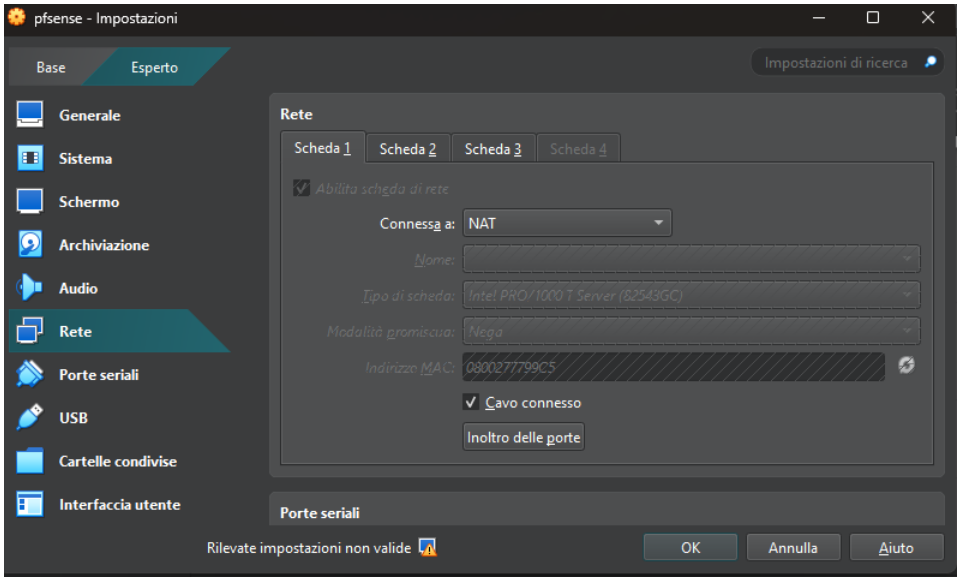
L’esercizio di oggi consiste nel creare una regola firewall che blocchi l’accesso alla DVWA (su metasploitable) dalla macchina Kali Linux e ne impedisca di conseguenza lo scan. Un requisito fondamentale dell’esercizio è che le macchine Kali e Metasploitable siano su reti diverse, potete aggiungere una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

Il nostro laboratorio è così composto:

Kali (192.168.50.2)

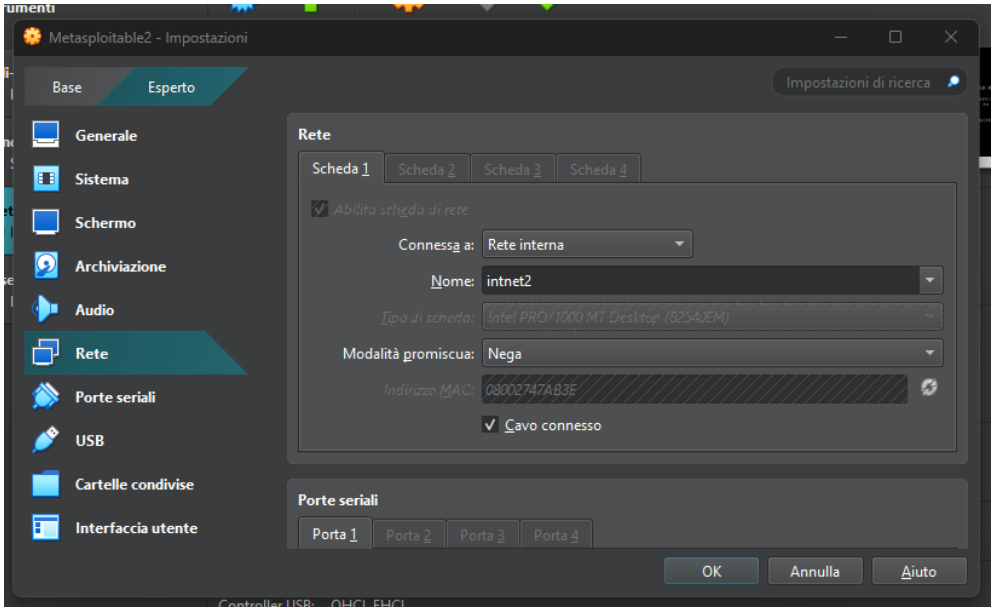


Pfsense (192.168.1.46)



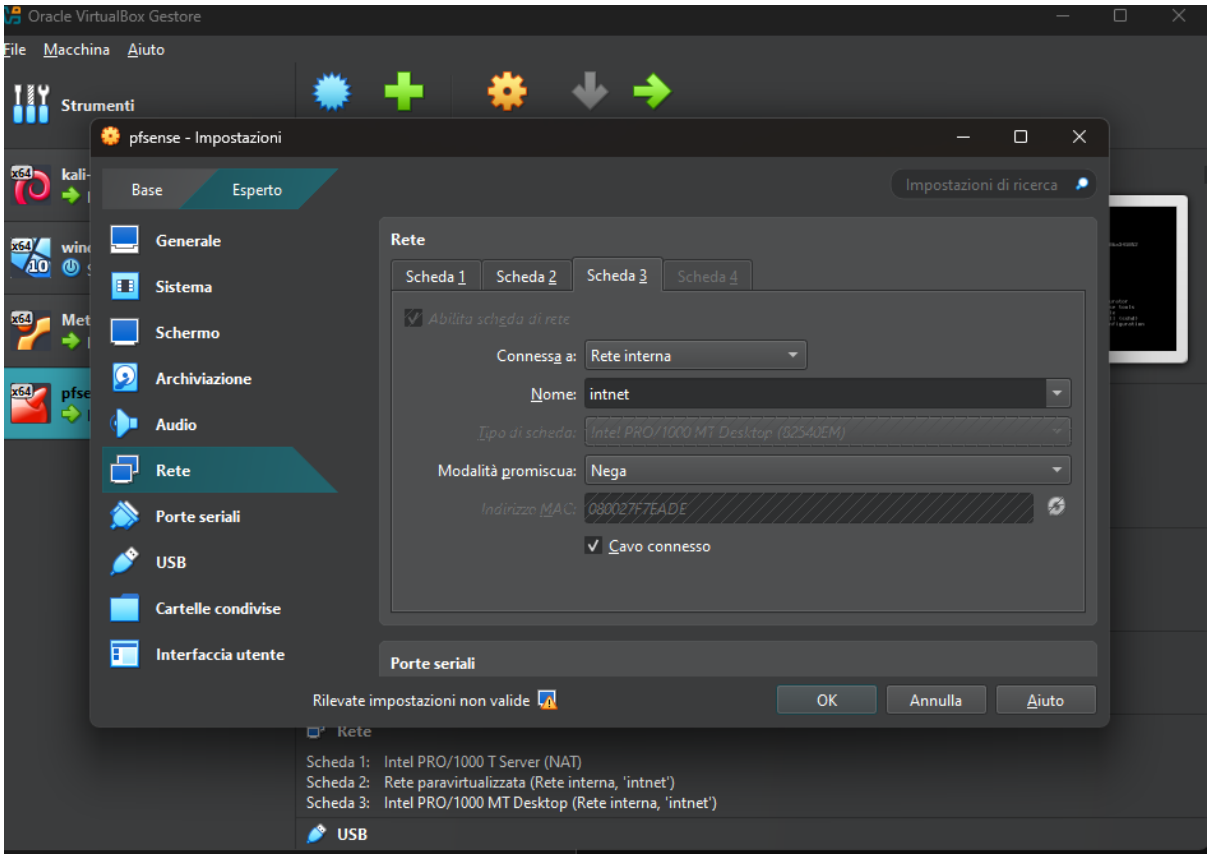
Mentre invece la scheda 2 e 3 sono su rete interna (intnet e intnet2)

Metasploitable (192.168.51.2)

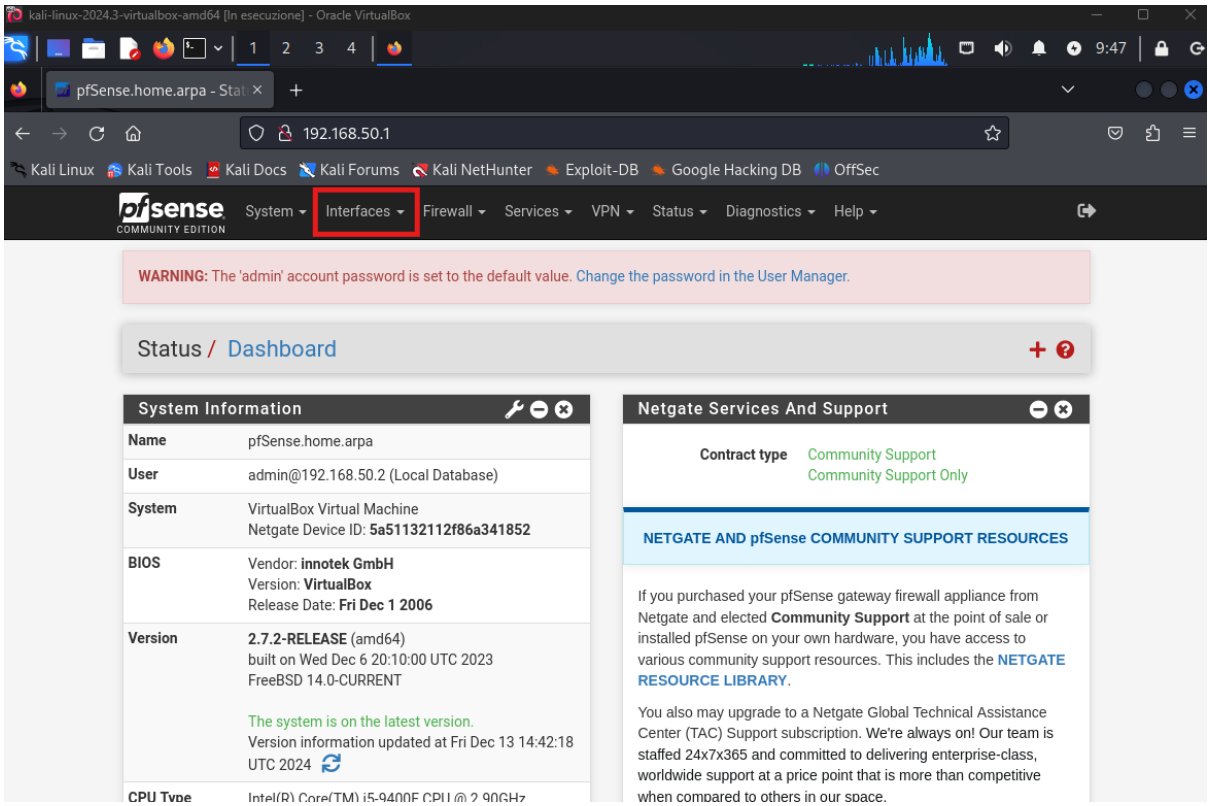


Il primo step è collegare pfsense al nostro kali è recarci sul sitoweb di pfsense, per creare una nuova interfaccia che sarà quella a cui collegheremo il nostro Metasploitable.

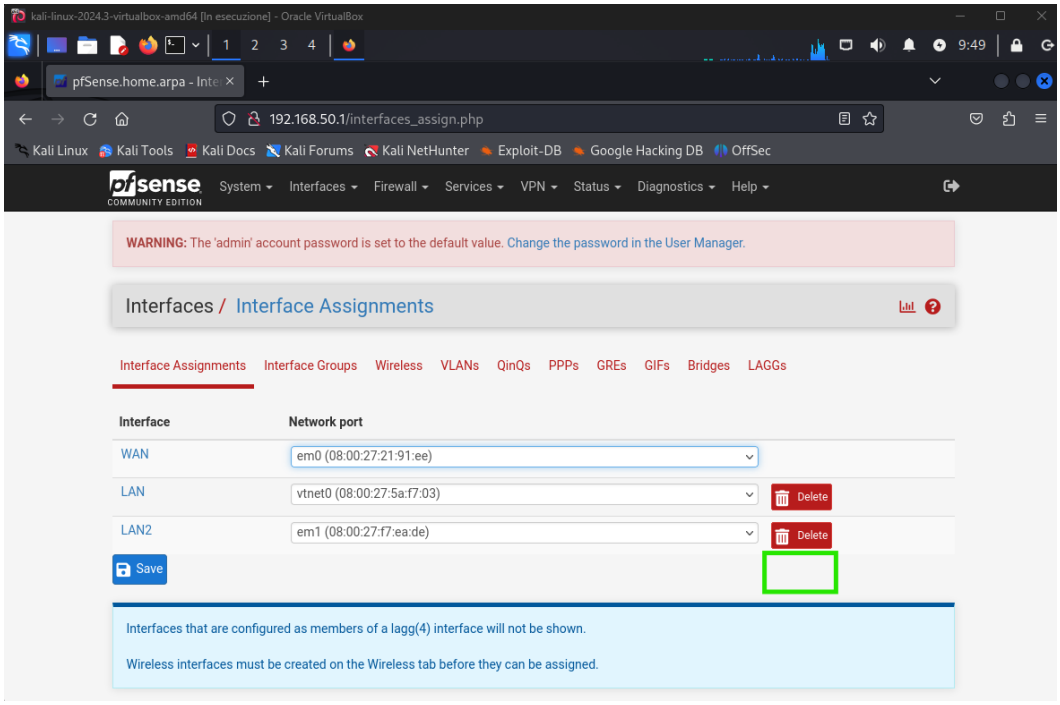
La chiameremo LAN2, per crearle bisogna innanzitutto spegnere la macchina virtuale di pfsense è aggiungere una scheda di rete.



Dopo di che riaccendiamo la macchina è andiamo sul sito dalla macchina kali, accedendo tramite utente e password ci ritroveremo nella home:

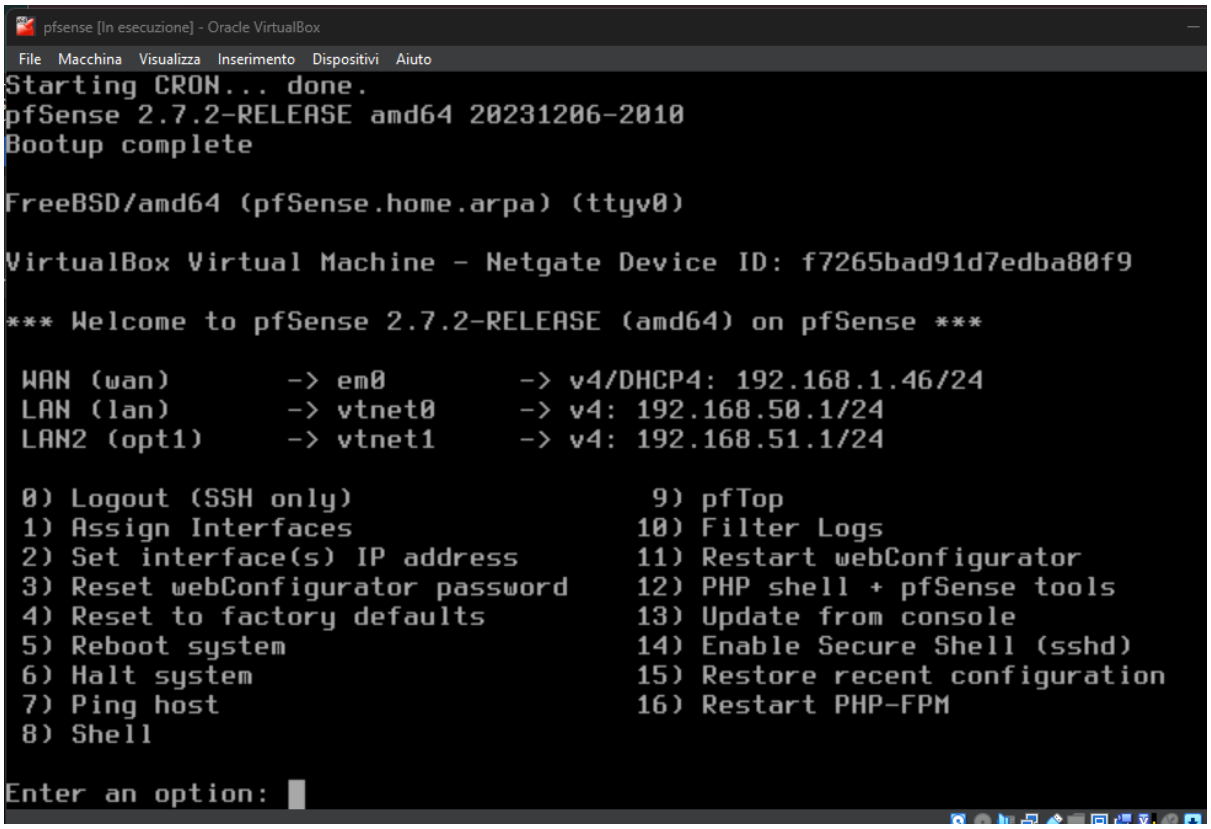


Schiacciamo su interfaces—assignements e ci ritroveremo nella schermata con le nostre interfaccie.



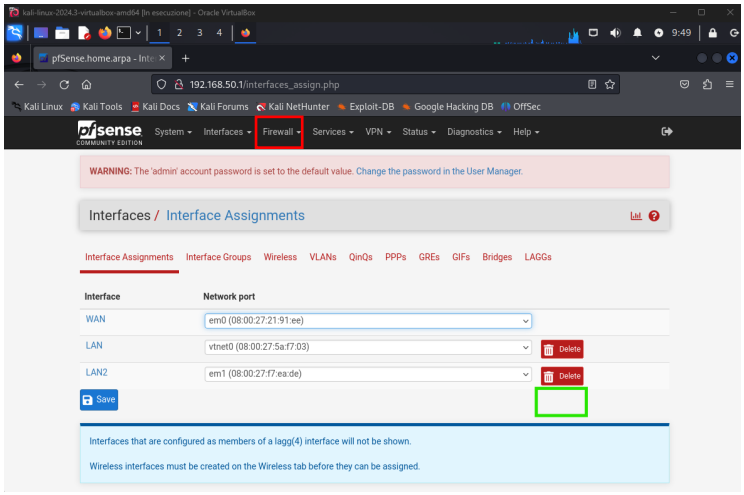
Nel rettangolo verde troverete la scritta “add” che dovrete schiacciare per creare la terza interfaccia che poi dobbiamo configurare con tutte le informazioni necessarie.(indirizzo ip e decidere se e statico o dinamico)

Una volta fatto ciò riavviando pfsense (la macchina virtuale):

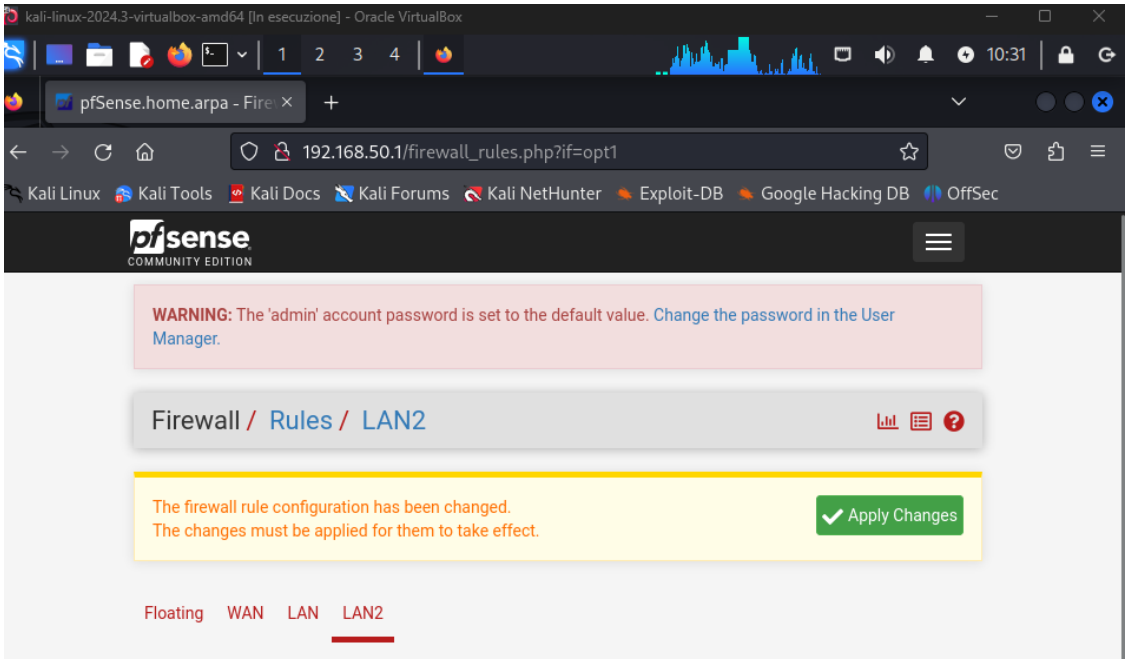


Possiamo notare che abbiamo tutte le nostre interfacce, la prima è la nat ovvero quella che ci manda su internet, mentre la seconda è per kali e la terza per metasploitable.

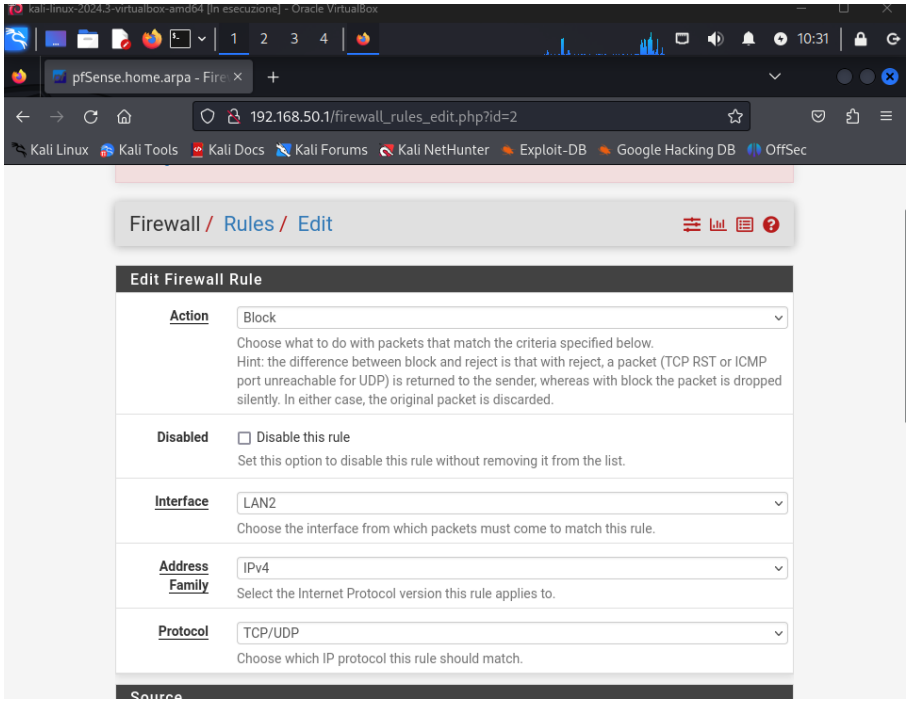
Dopo dobbiamo creare la nuova regola, quindi andiamo su “Firewall” e poi su “rules”.



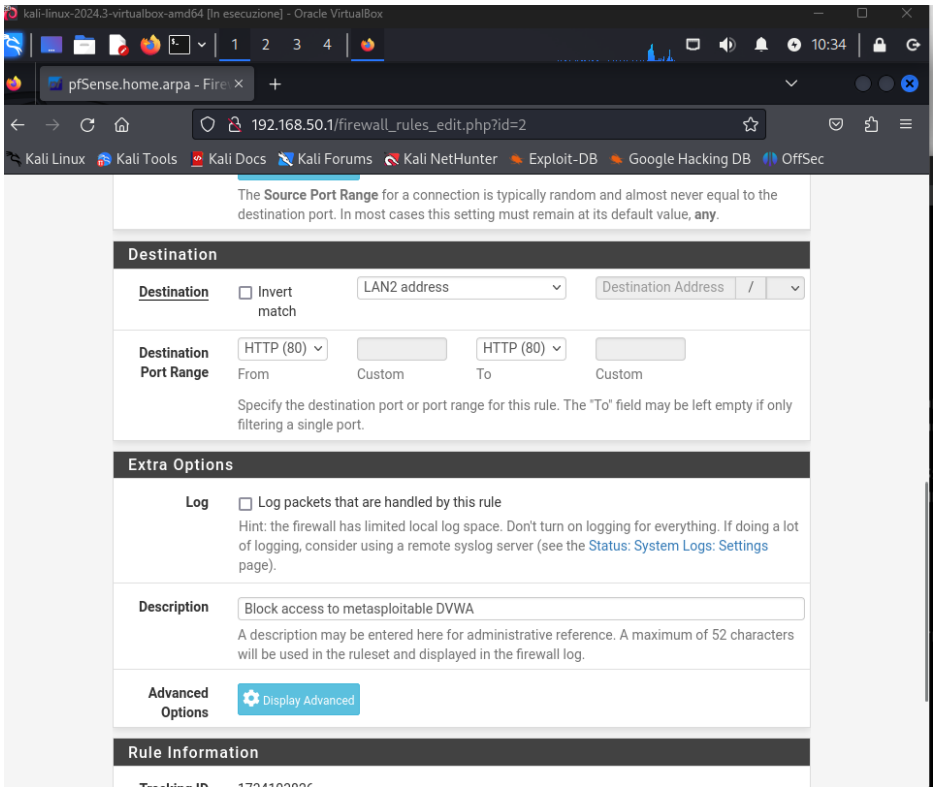
Vi ritroverete qui:



Dovrete schiacciare Add e poi compilare tutti i vari spazi



Gli diciamo ovviamente che deve bloccare, che l'interfaccia è quella della lan2, che l'ip e ipv4 e il protocollo TCP/UDP dato che passa attraverso http.



Specifichiamo chi è la sorgente e chi il destinatario è la porta 80(http).

Infondo c'è salva è una volta fatto questo dobbiamo fare anche "apply changes".

Ora dobbiamo verificare il tutto tramite un Ping alla macchina metasploitable, non sono riuscito a mettere le foto della verifica perché non sono riuscito, in linea teorica comunque si dovrebbero bloccare i contenuti che si inviano da Kali a metasploitable.

Un modo per verificare è fare un Ping dalla macchina di kali a metasploitable che in teoria dovrebbe essere bloccato.