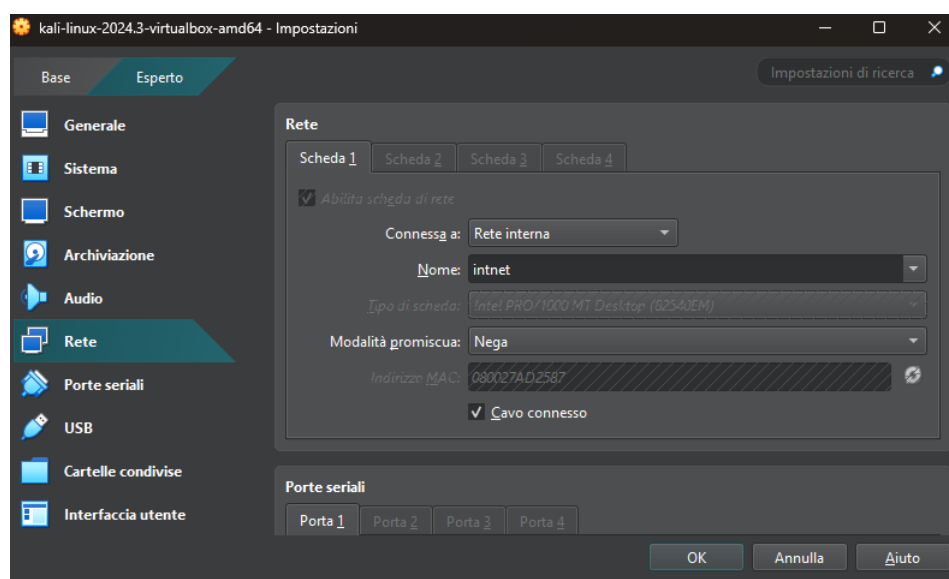


S3/L5

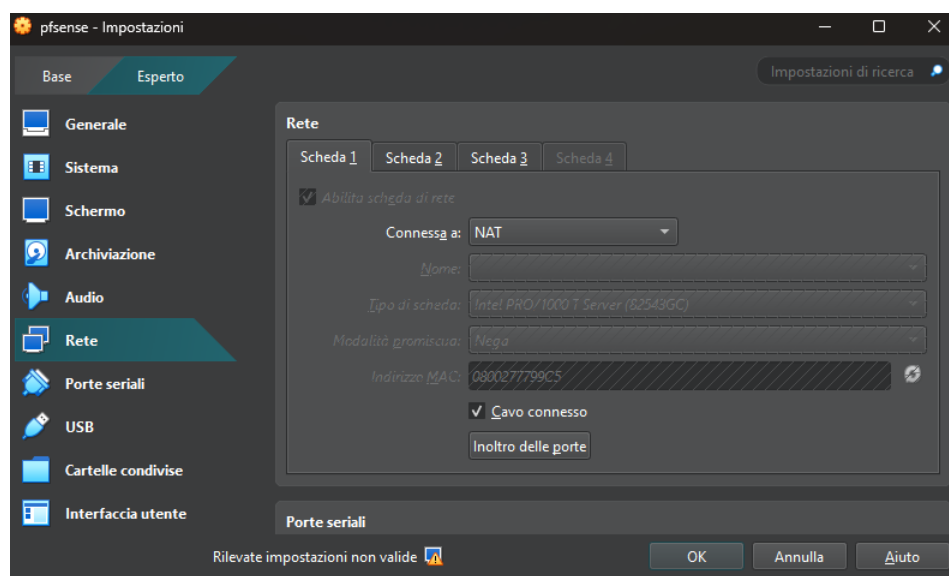
L'esercizio di oggi consiste nel creare una regola firewall che blocchi l'accesso alla DVWA (su metasploitable) dalla macchina Kali Linux e ne impedisca di conseguenza lo scan. Un requisito fondamentale dell'esercizio è che le macchine Kali e Metasploitable siano su reti diverse, potete aggiungere una 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)

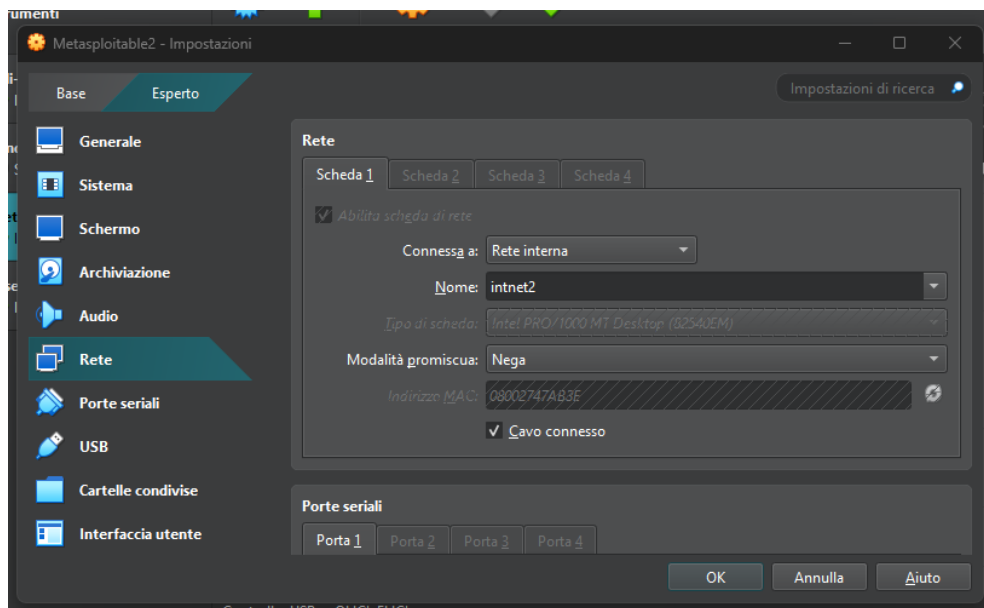


Pfsense (192.168.1.46)



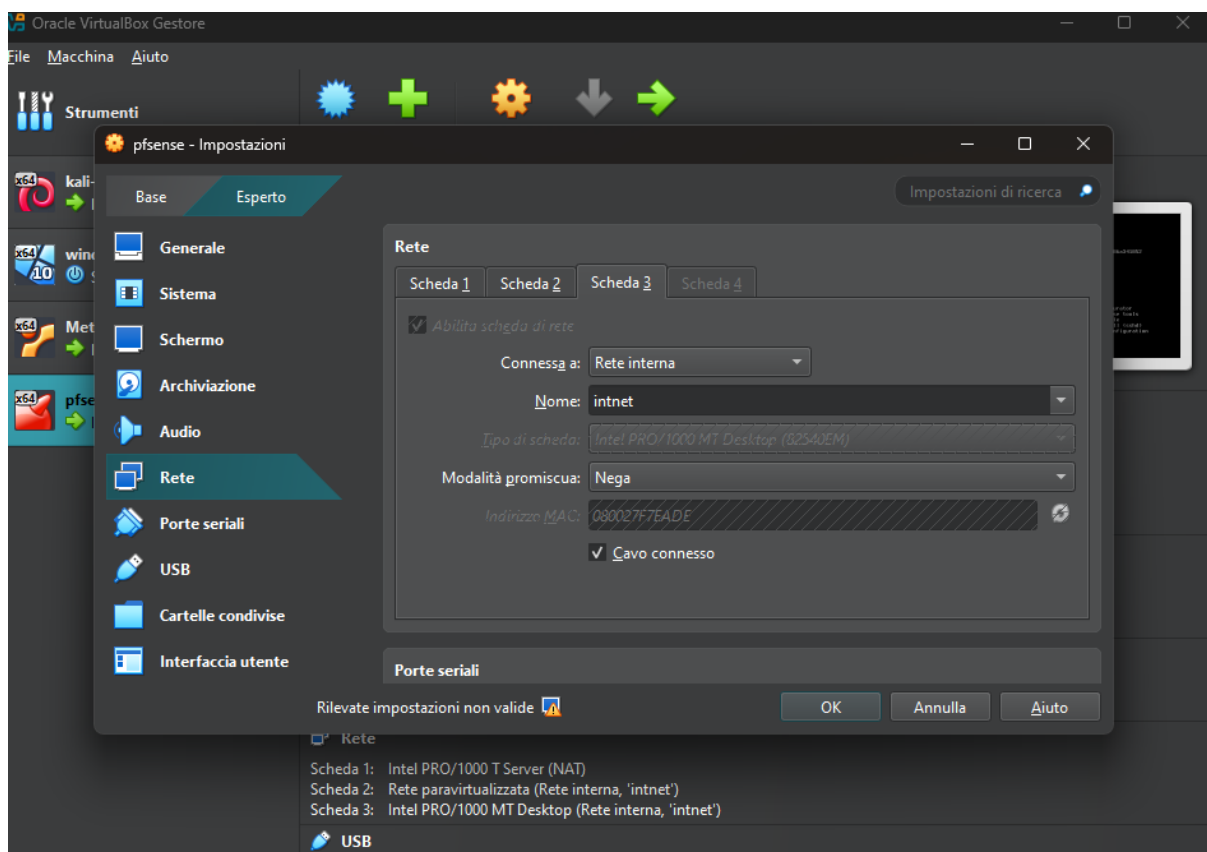
Mentre invece la scheda 2 e 3 sono su rete interna (intnet e intnet2)

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 e andiamo sul sito dalla macchina kali, accedendo tramite utente e password ci ritroveremo nella home:

The screenshot shows a web browser window with the URL `192.168.50.1`. The browser's address bar and tabs are visible. The pfSense web interface is displayed, featuring a top navigation bar with the pfSense logo and a menu with items like System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The 'Interfaces' menu item is highlighted with a red box. Below the navigation bar, a warning message states: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." The main content area is titled "Status / Dashboard" and contains two panels. The left panel, "System Information", lists details such as Name (pfSense.home.arpa), User (admin@192.168.50.2), System (VirtualBox Virtual Machine), BIOS (Vendor: innotek GmbH, Version: VirtualBox, Release Date: Fri Dec 1 2006), Version (2.7.2-RELEASE (amd64), built on Wed Dec 6 20:10:00 UTC 2023, FreeBSD 14.0-CURRENT), and CPU Type (Intel(R) Core(TM) i5-9400F CPU @ 2.90GHz). The right panel, "Netgate Services And Support", shows the Contract type as "Community Support" and "Community Support Only". Below this, a section titled "NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES" provides information about community support resources and a link to the "NETGATE RESOURCE LIBRARY".

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Status / Dashboard

System Information	
Name	pfSense.home.arpa
User	admin@192.168.50.2 (Local Database)
System	VirtualBox Virtual Machine Netgate Device ID: 5a51132112f86a341852
BIOS	Vendor: innotek GmbH Version: VirtualBox Release Date: Fri Dec 1 2006
Version	2.7.2-RELEASE (amd64) built on Wed Dec 6 20:10:00 UTC 2023 FreeBSD 14.0-CURRENT The system is on the latest version. Version information updated at Fri Dec 13 14:42:18 UTC 2024
CPU Type	Intel(R) Core(TM) i5-9400F CPU @ 2.90GHz

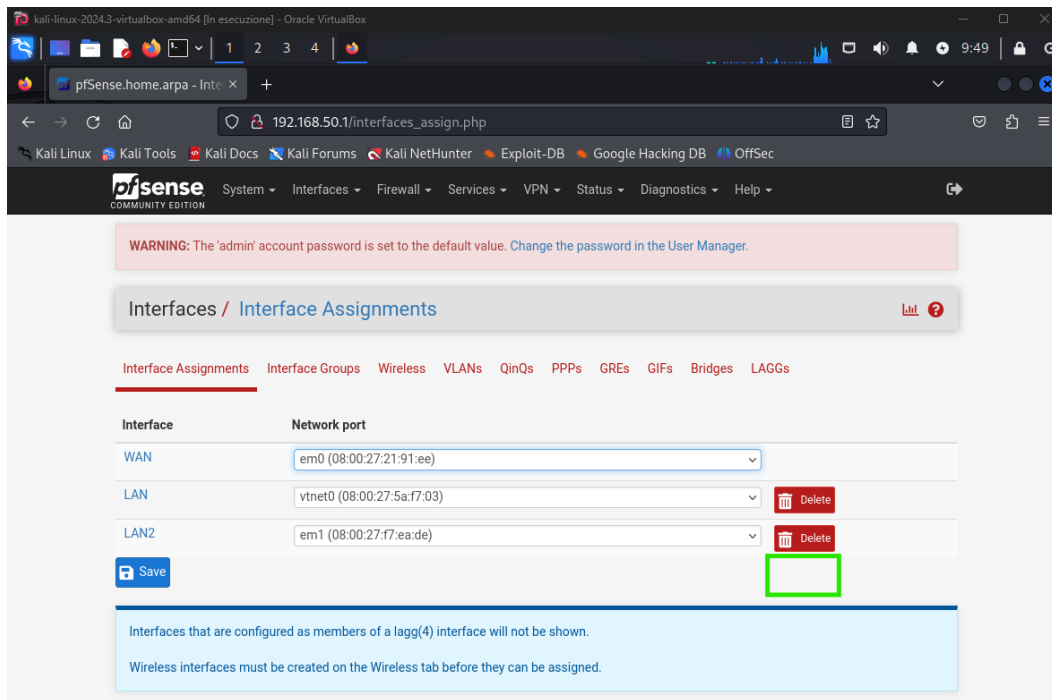
Netgate Services And Support	
Contract type	Community Support Community Support Only

NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES

If you purchased your pfSense gateway firewall appliance from Netgate and elected **Community Support** at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the [NETGATE RESOURCE LIBRARY](#).

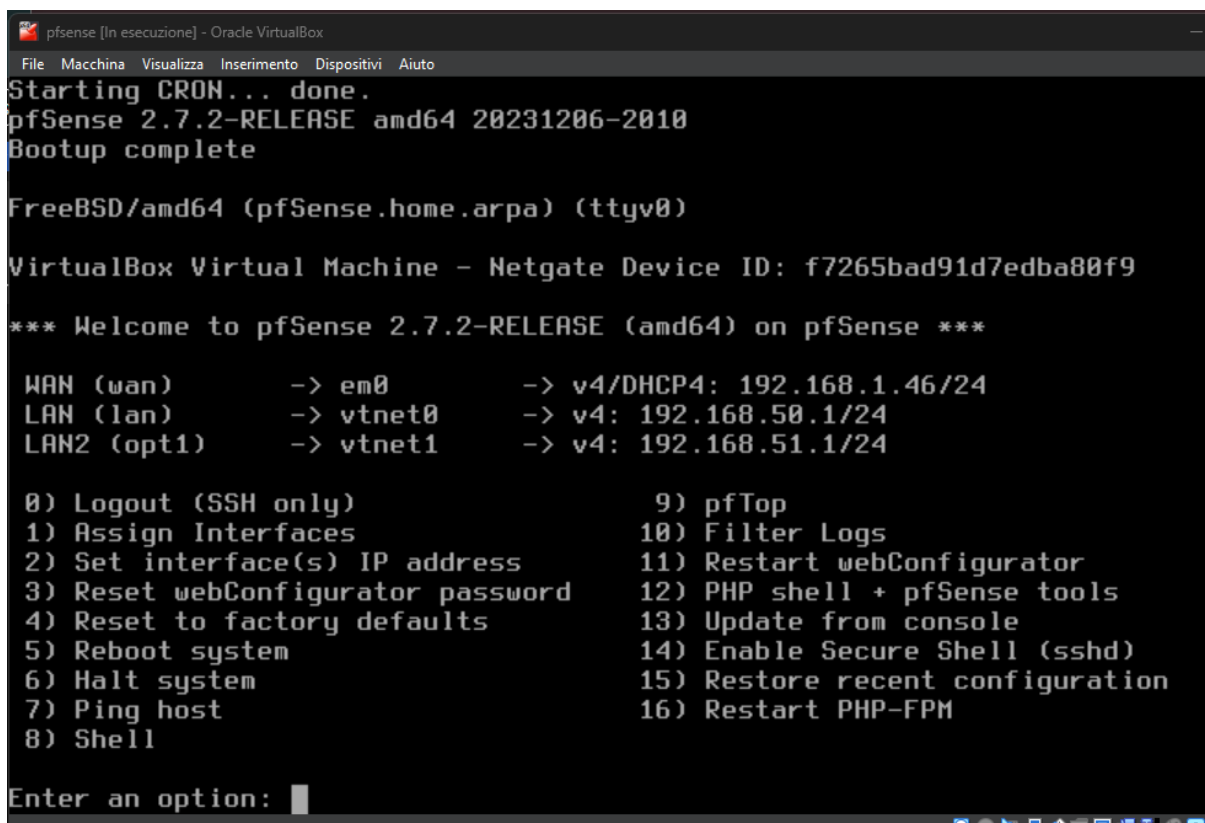
You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.

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



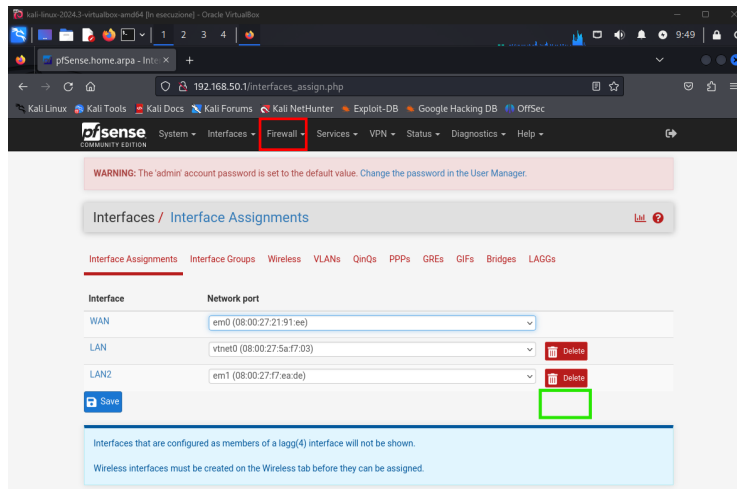
Nel rettangolo verde troverete la scritta “add” che dovete schiacciare per creare la terza interfaccia che poi dobbiamo configurare con tutte le informazioni necessarie.(indirizzo ip e decidere se e statico o dinamico)

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

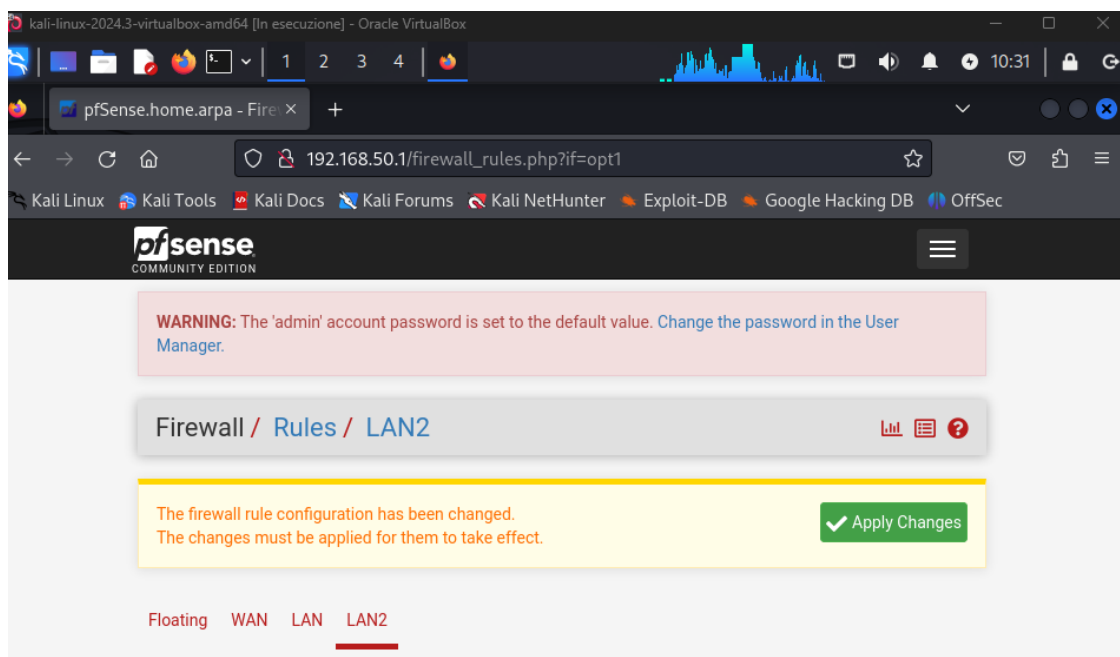


Possiamo notare che abbiamo tutte le nostre interfacce, la prima è la nat ovvero quella che ci manda su internet, mentre la seconda è per kali e la terza per metasploitable.

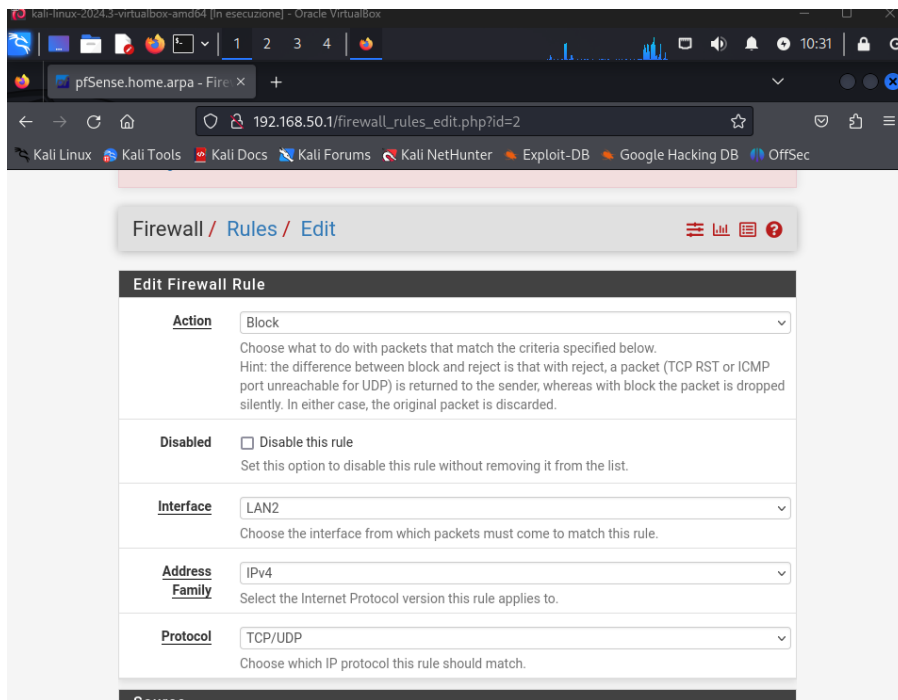
Dopo dobbiamo creare la nuova regola, quindi andiamo su “Firewall” e poi su “rules”.



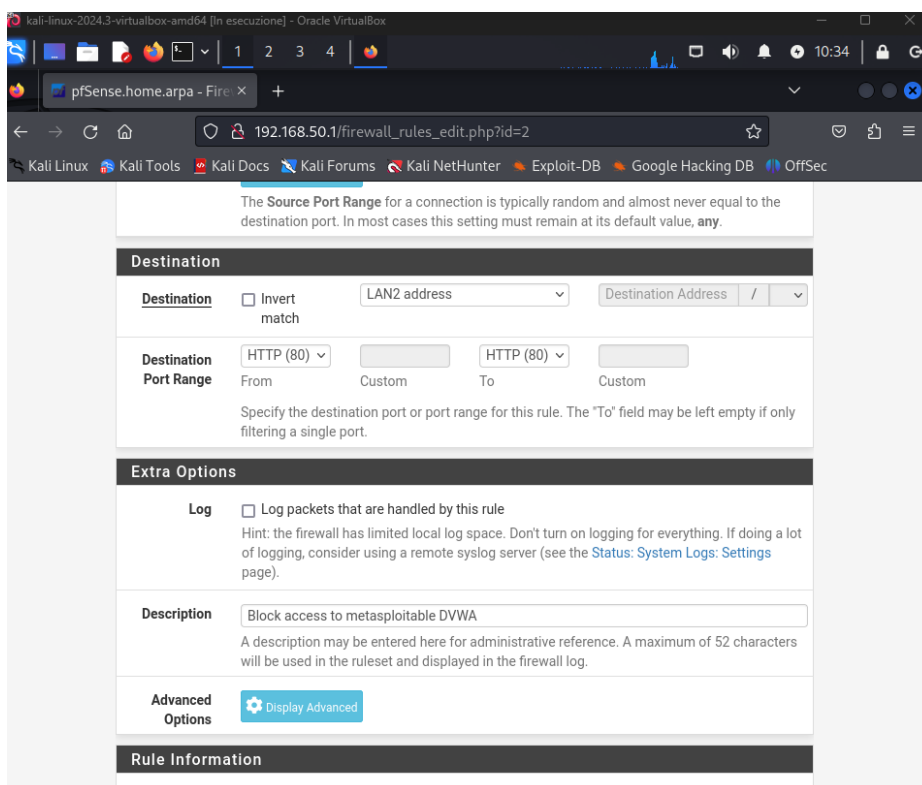
Vi ritroverete qui:



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 è 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.