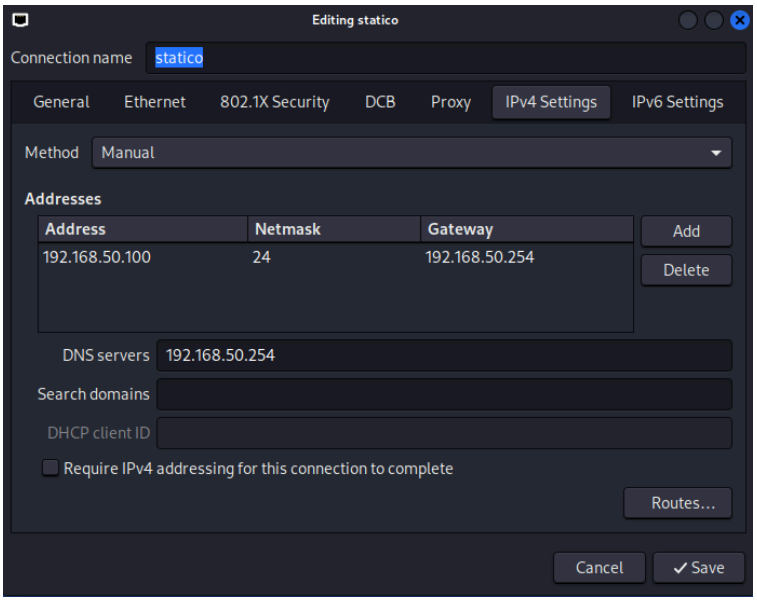
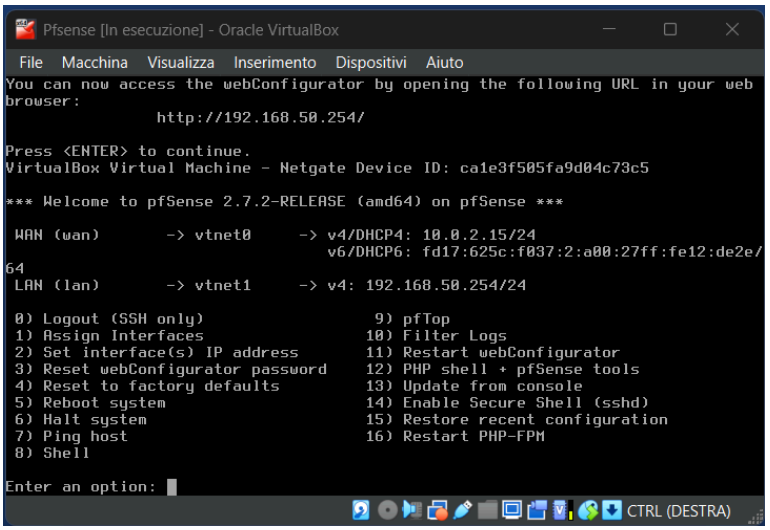
Esercizio per il progetto settimanale Unit 1 - S3 - L5
Svolto da Gioele Parla

Esercizio: Creazione di una regola Firewall.

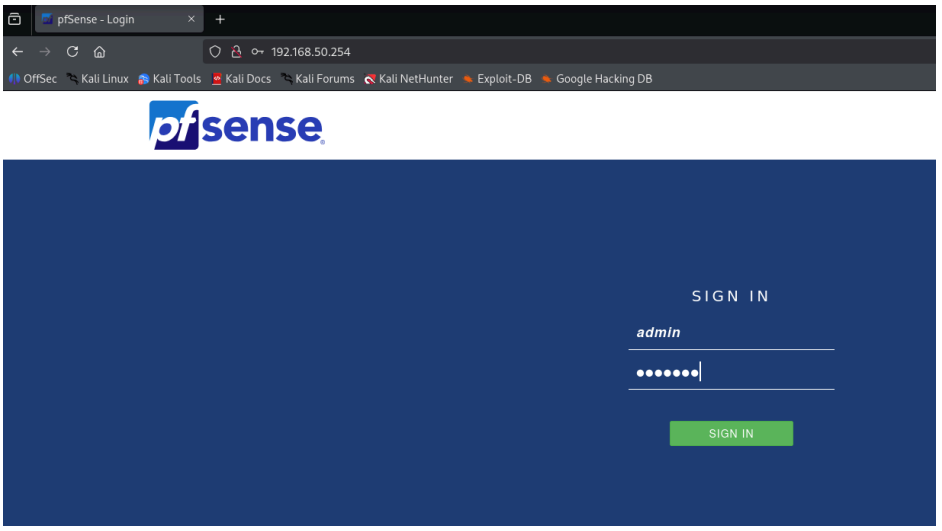
Per prima cosa giusto per impostare correttamente tutto l'ambiente di rete configuriamo la nostra rete di KALI in **statica** e andando su edit connections per comodità impostiamo gateway e DNS servers su 192.168.50.254 poicè la pfsense ogni tanto cambia il suo DHCP prendendo spunto da uno statico della macchina e si mette come gateway sull'1 quindi preferiamo mettere la pfsense sulla 254.



Andando sull'interfaccia di pfsense da VirtualBox dovremo impostare la LAN su **192.168.50.254** e per impostarla ci basterà seguire i comandi andando prima su 2, dichiarare di non voler attivare il DHCP e poi impostare manualmente

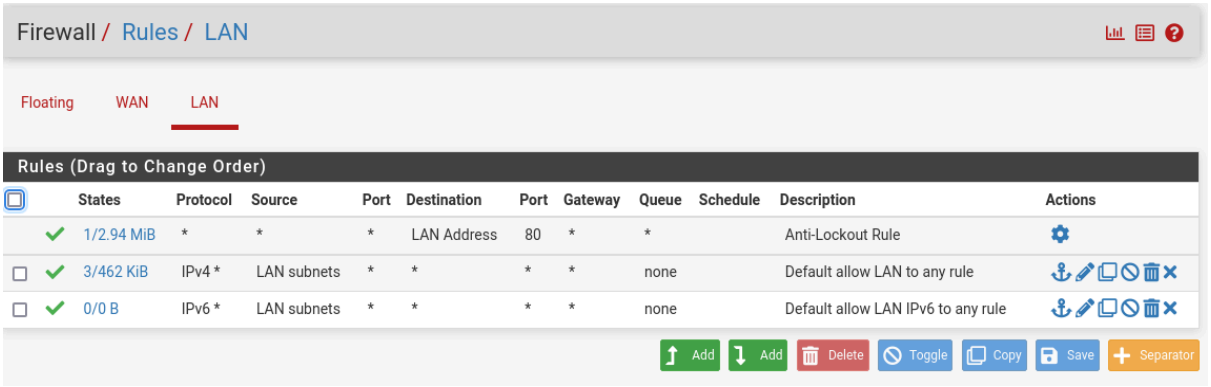


Una volta configurato andando sul browser di kali accediamo sull'UTM 192.168.50.254 e funzionerà già da firewall

- 

Una volta entrati nel nostro firewall possiamo procedere con il nostro esercizio che chiede:

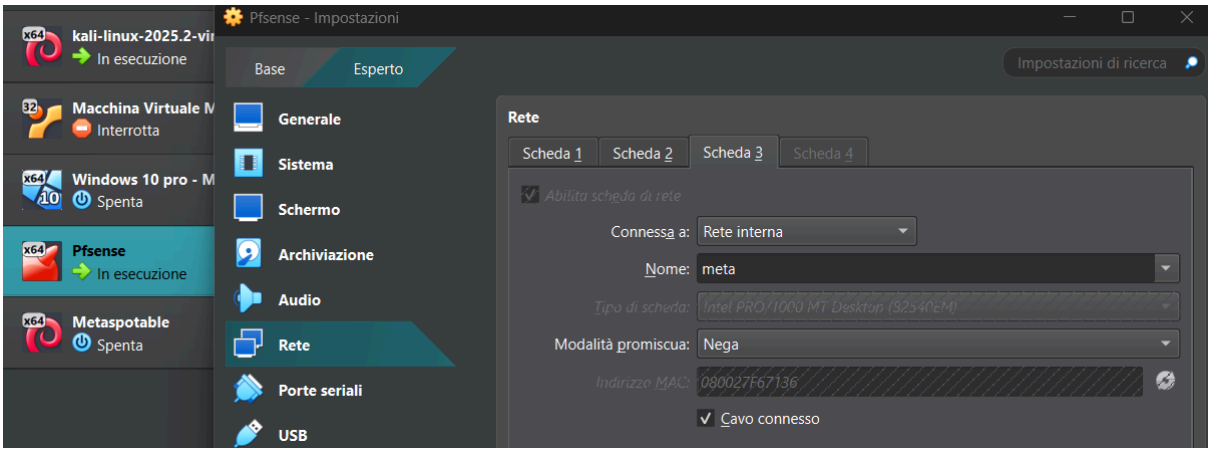
Creare una regola firewall che blocchi l'accesso alla DVWA (su metasploitable) dalla macchina Kali Linux e ne impedisca di conseguenza lo scan.

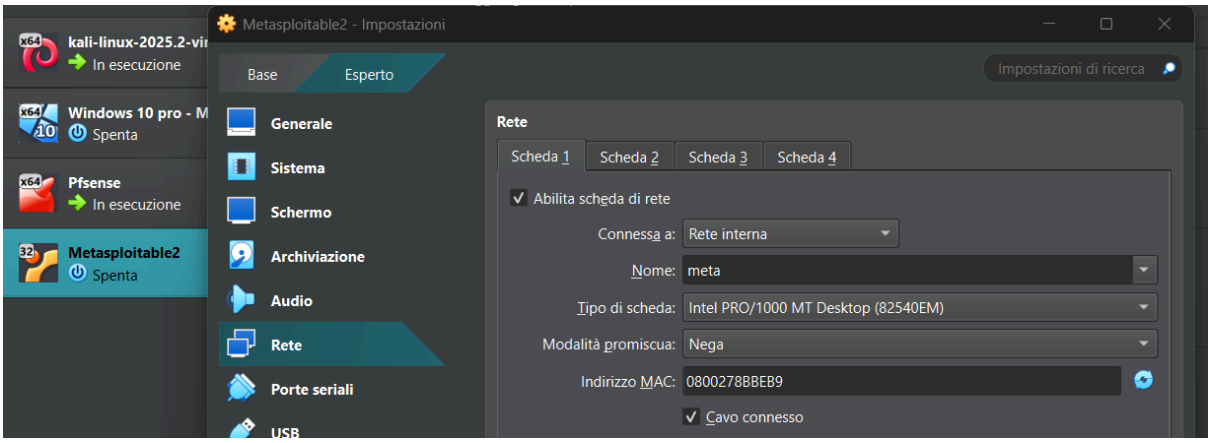


Quindi il nostro esercizio chiede di aggiungere una nuova regola rispetto a quelle già presenti, le rules sono importanti perchè tramite le rules è possibile configurare come deve comportarsi il nostro firewall col traffico di input per ognuna di queste wal/lan, le regole floating sono regole che valgono per tutti, in LAN la prima regola non posso modificarla e riguarda l'accesso a questa interfaccia web, potremo al massimo portarla in HTTPS invece le altre due regole LAN consentono la navigazione in internet separata in ipv4 e ipv6.

Dopo una breve panoramica configuriamo le reti delle nostre macchine kali e metaspoitable cosi da poter successivamente creare una regola firewall da applicare a queste 2 reti.

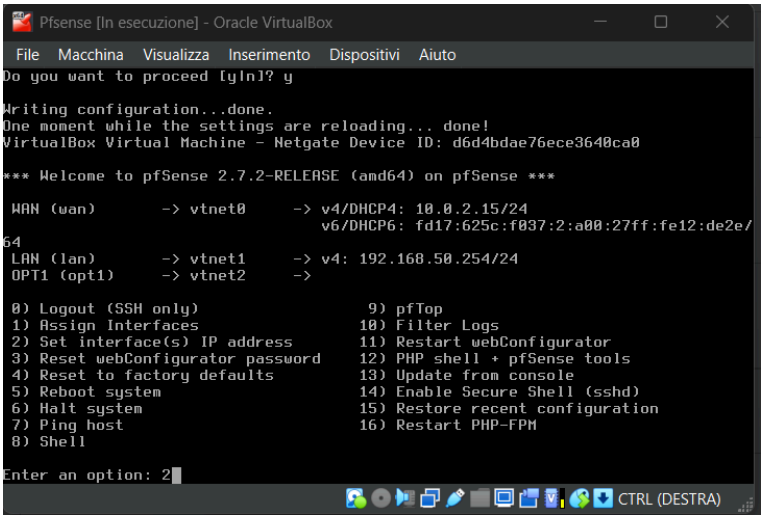
L’esercizio ci consiglia di impostare le macchine Kali e Metasploitable su **reti diverse**, quindi per prima cosa andiamo nelle impostazioni di rete di Pfsense su VirtualBox e aggiungiamo una nuova interfaccia di rete(scheda 3) che chiameremo “**meta**” cosi potremo gestire una ulteriore rete e successivamente andando in impostazioni di rete della macchina virtuale metasploitable 2 dovremo impostare la rete interna su “meta”.

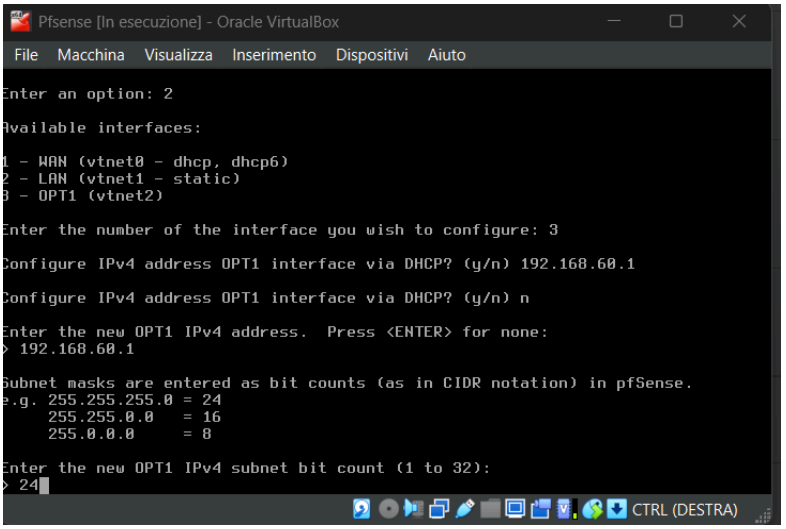


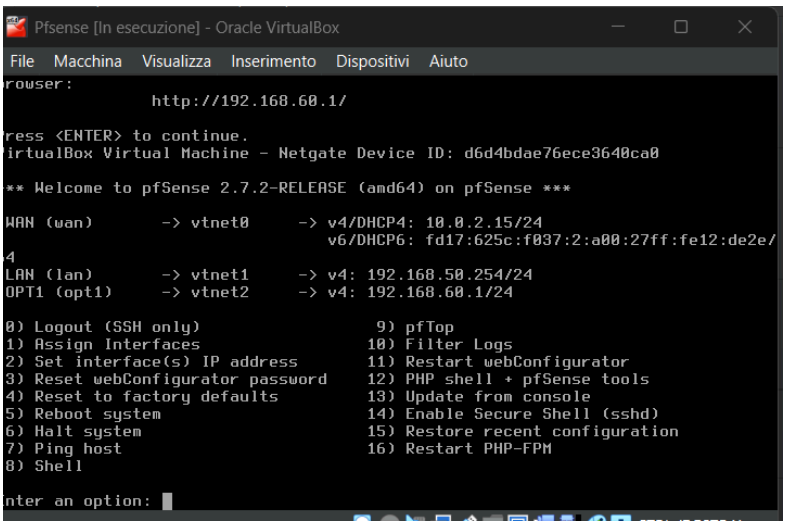


Una volta configurato VirtualBox con le corrette impostazioni di rete di pfsense e Metasploitable2 il passaggio successivo sarà quello di configurare la nuova rete meta all’interno di pfsense avviandola.

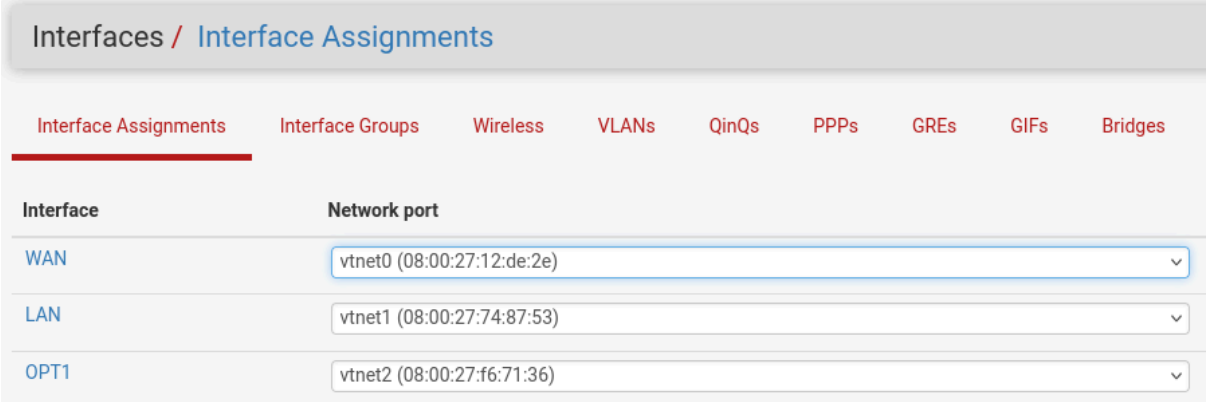
All’interno di Pfsense dobbiamo gestire la nuova rete **meta,** dalle impostazioni dovremo quindi aggiungere una nuova interfaccia di rete **vtnet2** e assegnare a questa interfaccia l’indirizzo IP ad esempio 192.168.60.1 cosi che questa interfaccia si occuperà della rete meta dove si trova metasploitable



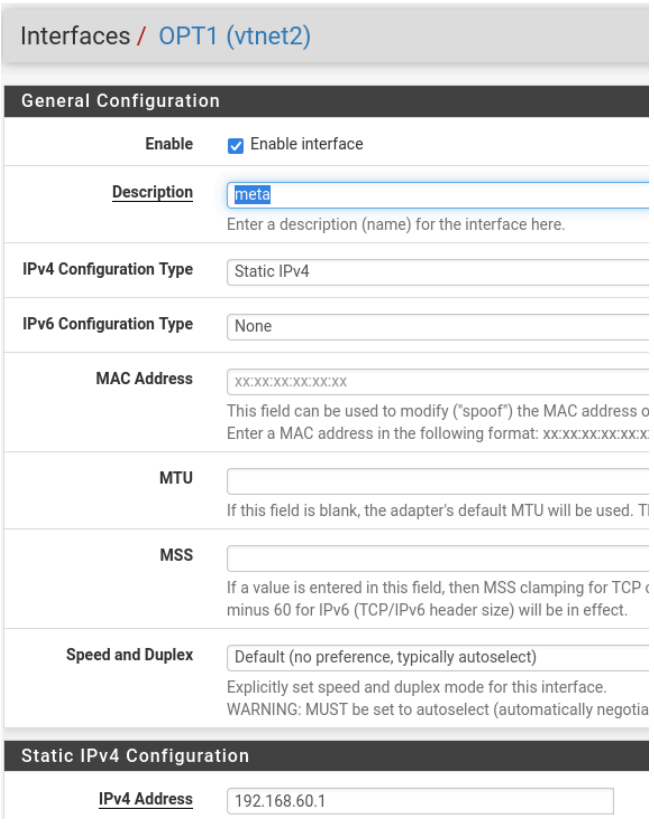




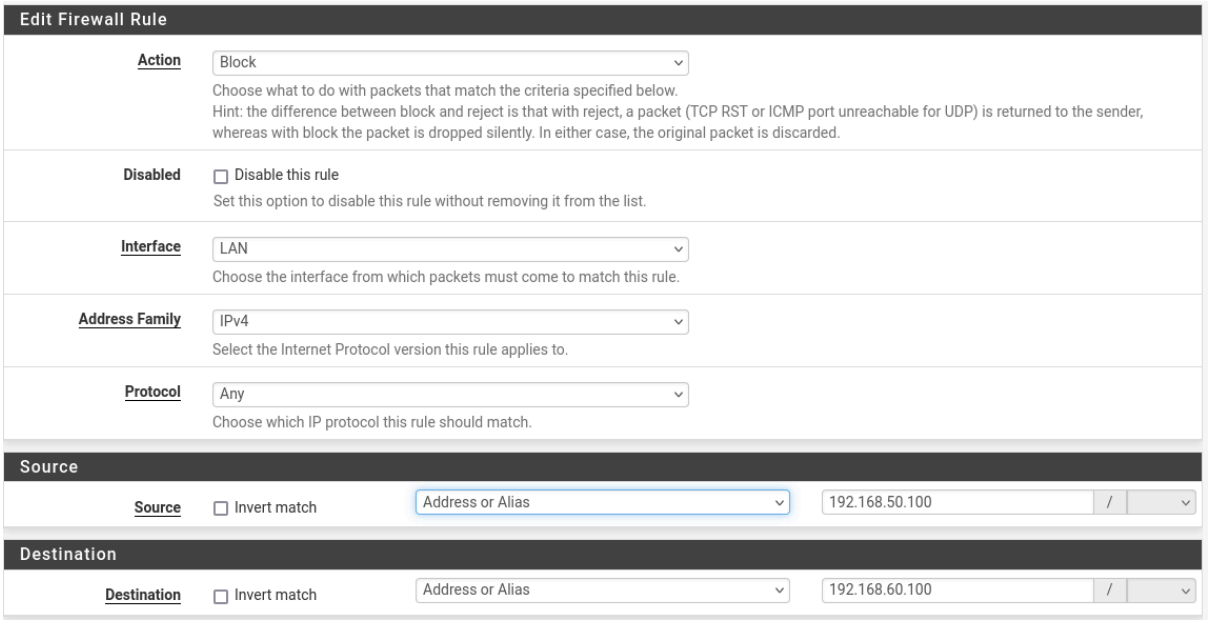
Adesso andiamo sulla Web Gui per attivare e configurare la nuova interfaccia come suggerisce l'esercizio e clicchiamo sulla OPT1



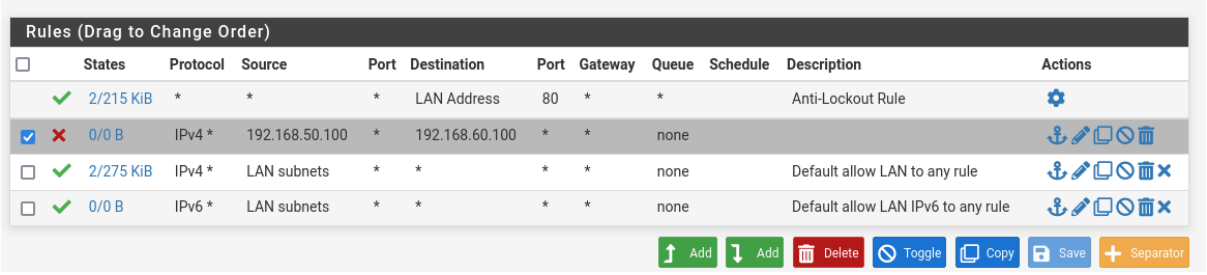
All’interno delle impostazioni di OP1 dovremo rinominare l’interfaccia in meta assicurandoci che abbia l’IPv4 corrispondente e salviamo le modifiche.



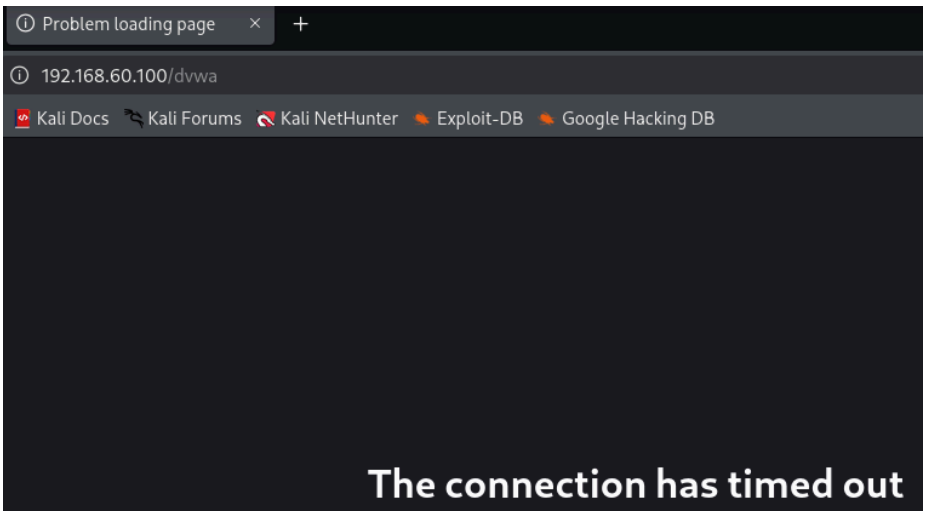
Una volta configurata l'interfaccia di rete possiamo proseguire alla creazione della nostra regola, andiamo in Firewall / rules e creiamo la nostra regola, su action impostiamo **BLOCK** poichè ci serve che blocchi l'accesso al DVWA e mettiamo come sorgente la macchina kali con l'indirizzo IP corrispondente e come destiazione la rete meta che abbiamo creato



una volta salvata la regola la troveremo all'interno della lista delle regole presenti sul nostro firewall, possiamo notare la **X** che rappresenta come sia una regola di blocco, come ultima azione dovremmo assicurarci che la regola sia posta in cima (quando l'ho creata ho usato la freccia su quindi si troverà gia posizionata in cima)



Una volta applicata la nostra regola sulla rete meta provando ad accedere alla DVWA di 192.168.60.100 ci darà **errore**.



Provando a fare delle ultime prove sul terminale di kali noteremo come riesce a comunicare con i gateway delle reti ma non con la nostra rete meta poichè abbiamo **bloccato** il traffico solamente tra la macchina kali e la macchina mettasploitable tramite la nostra regola.