M3 - Settimana 9 - Giorno 5 - RELAZIONE - 05/09/2025 - Giuseppe Gigliotti - PFSENSE

Questa esercitazione è divisa in due fasi preliminari 1 e 2 e una terza che sarà l'esercizio da svolgere autonomamente 3.

Esercizio che prevede la creazione di un'ulteriore rete e l'applicazione di una policy firewall tra le due reti;

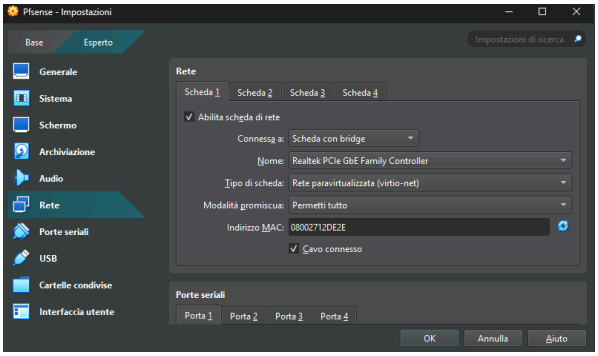
Facoltativo: approfondimenti sulla gestione dei log e del troubleshooting di rete

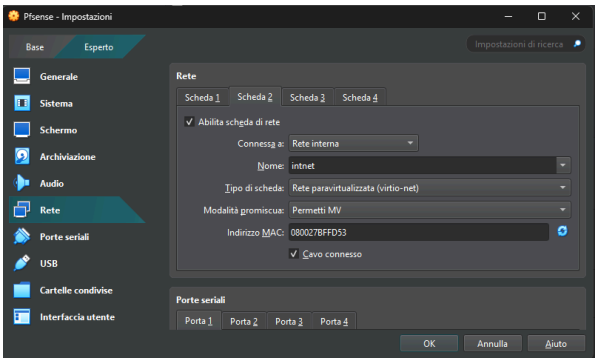
1. Installazione di Pfsense e configurazione architettura di partenza (aka architettura target)

Per quando riguarda l'installazione e la configurazione della nuova macchina Pfsense, lasciamo solo immagini della macchina a risultato finito, in quanto essa è stata configurata durante l'esercitazione.

- Nella prima immagine vediamo la configurazione della scheda 1 in modalità "bridge" per poter utilizzare internet sulle nostre macchine.
- Nella seconda immagine vediamo la configurazione della scheda 2 in modalità "rete interna" per avere le nostre due macchine (kali e metasploitable) nella

stessa sottorete



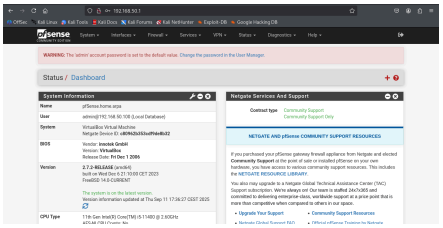


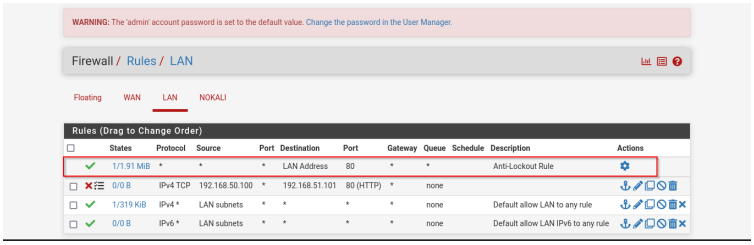
Il risultato finale sarà come nell'immagine sottostante!

2. Creazione guidata di una policy firewall generica

- Configurata la pfsense ed aver assegnato l’indirizzo IP 192.168.50.1 (ci farà da default gateway), passiamo sulla kali e da browser nella barra degli indirizzi inseriamo lo stesso IP per raggiungere la pfsense.

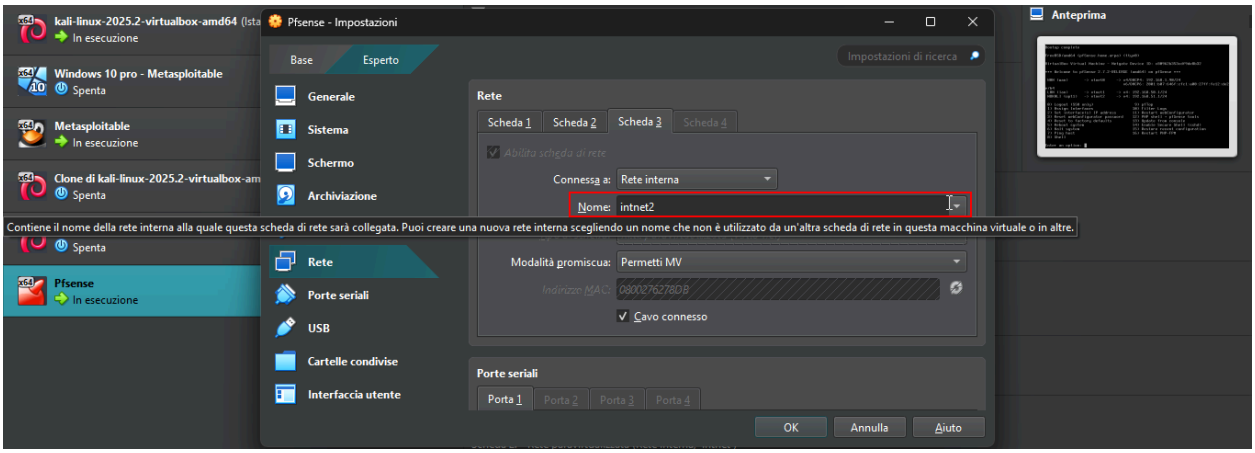
- Inserite le credenziali di default (username :admin , password : pfsense), arriviamo sulla dashboard di pfsense.
- Configuriamo anche dal browser, andiamo su Firewall nel menù a tendina e selezioniamo su Rules
- Arrivati su Rules, andiamo su LAN, e possiamo vedere che esiste già una policy firewall generica che permette di usare qualsiasi protocollo, qualsiasi sorgente, su porta 80 che va sulla lan e non viene bloccata mai



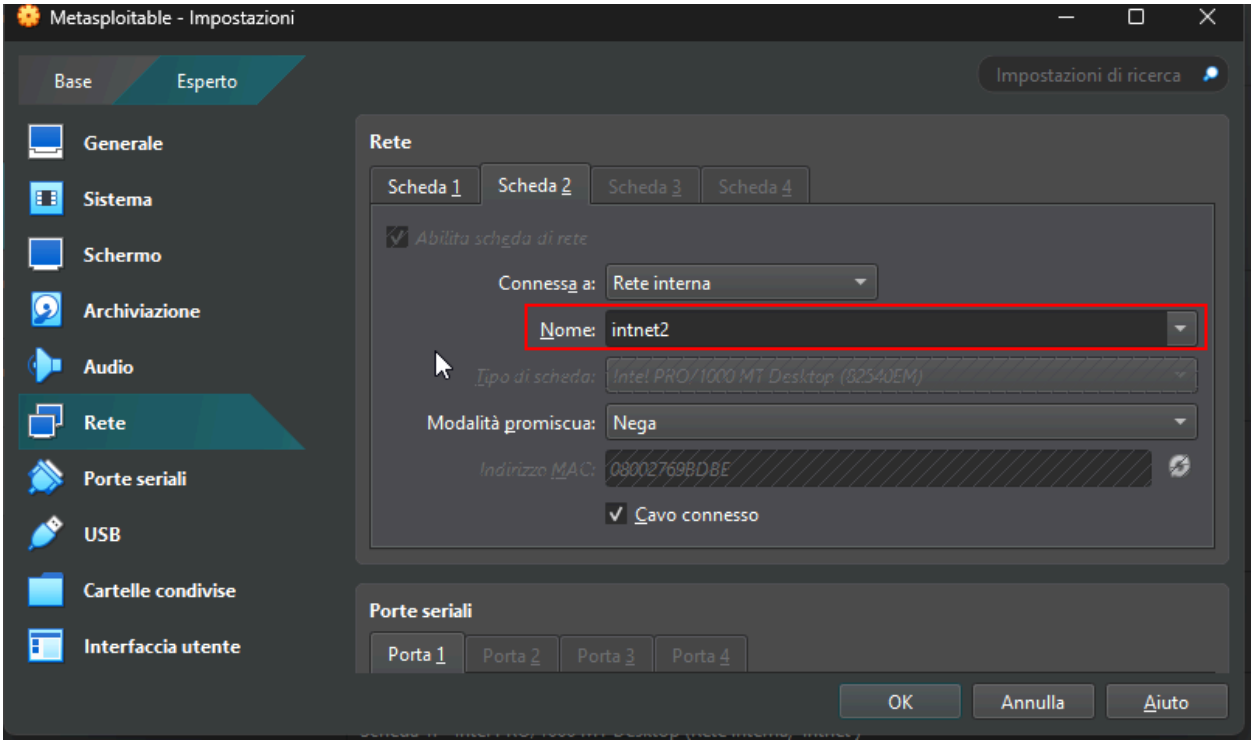


3. Esercizio che prevede la creazione di un’ulteriore rete e applicazione di una policy firewall tra le due reti.

- Per fare questo andiamo sulla pfsense e la spegniamo
- Andiamo nelle impostazioni della macchina virtuale pfsense ed aggiungiamo un’altra interfaccia di rete.
- Abilitiamo la scheda 3, su rete interna, e visto che l’esercizio chiede un’ulteriore rete cambiamo il nome in intnet2

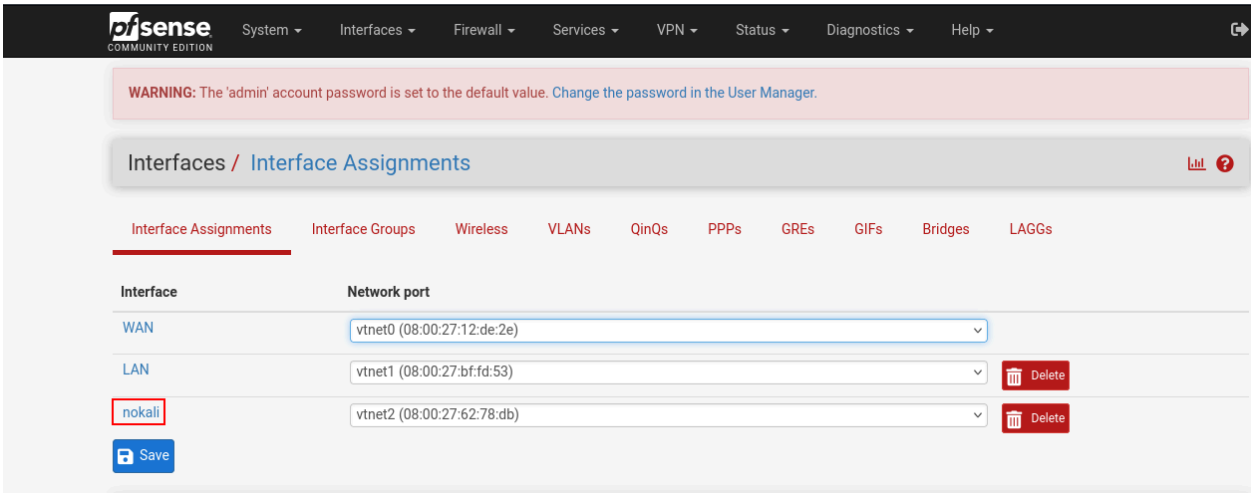


- Stessa cosa facciamo sulla metasploitable, andiamo in impostazioni di rete e abilitiamo la scheda 2 e cambiamo la rete in inet2



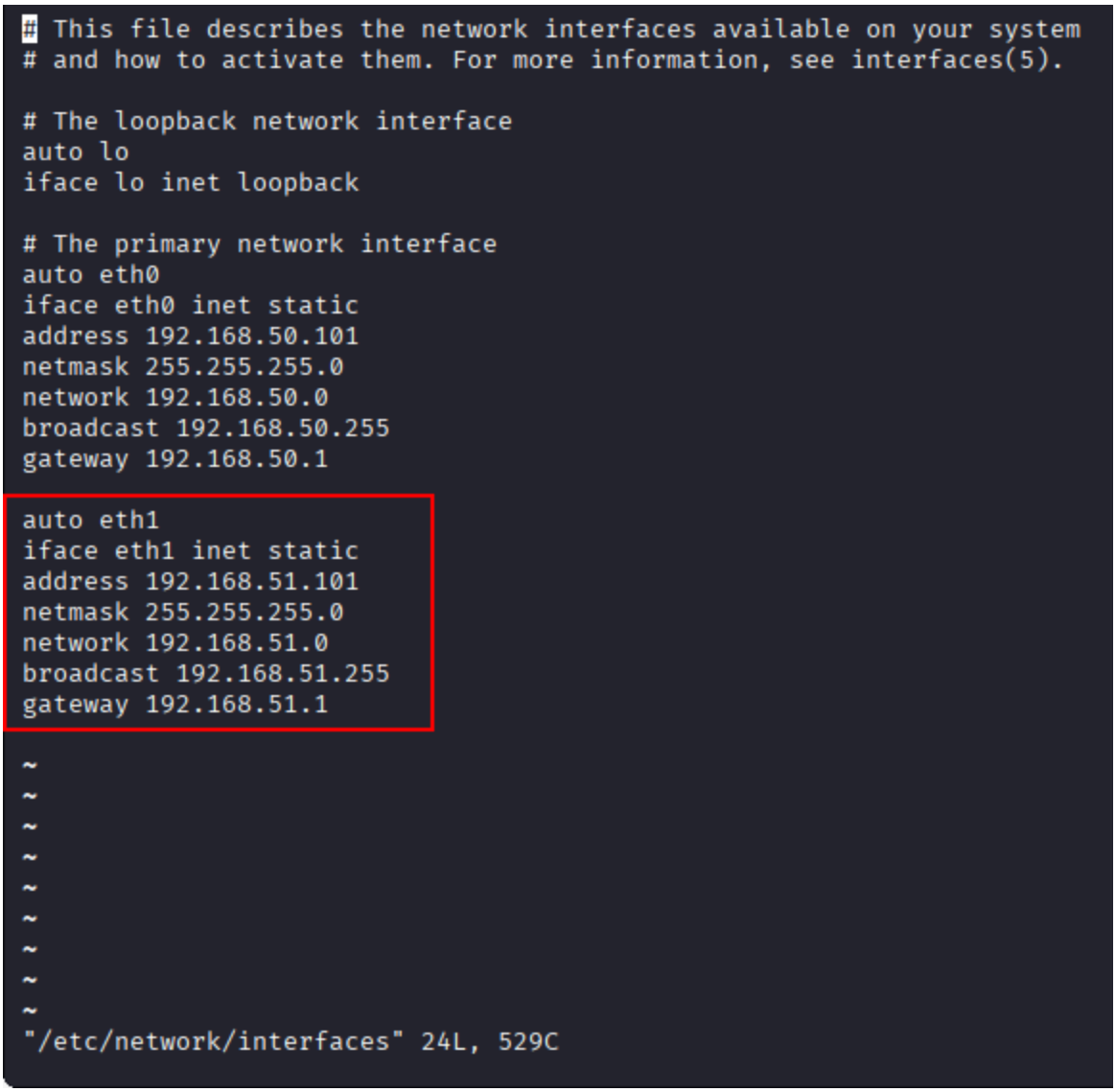
- Torniamo su kali sulla pagina browser di pfsense e dopo esserci riloggati (visto che per configurare la nuova scheda di rete abbiamo spento la macchina) andiamo in Interfaces e poi dal menù a tendina Assignements

- Aggiungiamo la nuova interfaccia (avrà il nome nokali). Nella configurazione mettiamo indirizzo IP statico e poi lo aggiungiamo dopo, che sarà 192.168.51.1. Alla fine possiamo salvare e tornare sulla metasploitable



- Sulla metasploitable utilizzando il comando, aggiungiamo la nuova sottorete

```
sudo vim /etc/network/interfaces # apriamo con vim il file di configurazione
# delle interfacce di metasploitable
```



E con il comando

```
sudo /etc/init.d/restart networking # ricarichiamo il file di
# configurazione della rete
```

- Aggiungiamo una nuova regola generica sull'interfaccia nokali (per semplificarci il lavoro copiamo una regola dall'interfaccia LAN già presente su

pfsense). Ricordiamo che nella regola la source deve essere su “nokali subnet” per non avere problemi di comunicazione.

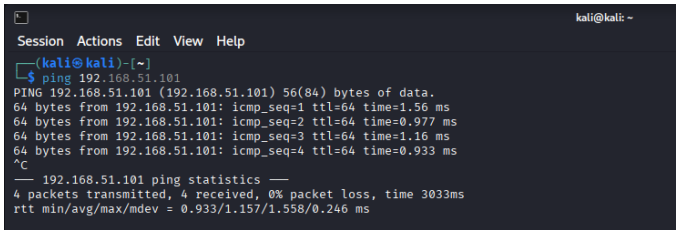
- Possiamo passare all’esercizio.

Esercizio:

Sulla base di quanto visto, creare una regola firewall che blocchi l’accesso alla DVWA (su metasploitable) dalla macchina Kali Linux e ne impedisca di conseguenza lo scan (fare uno screenshot che dimostri che prima lo scan per DVWA funzionava e ora non funziona più). 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. Connettetevi poi in Web GUI per attivare la nuova interfaccia e configurarla.

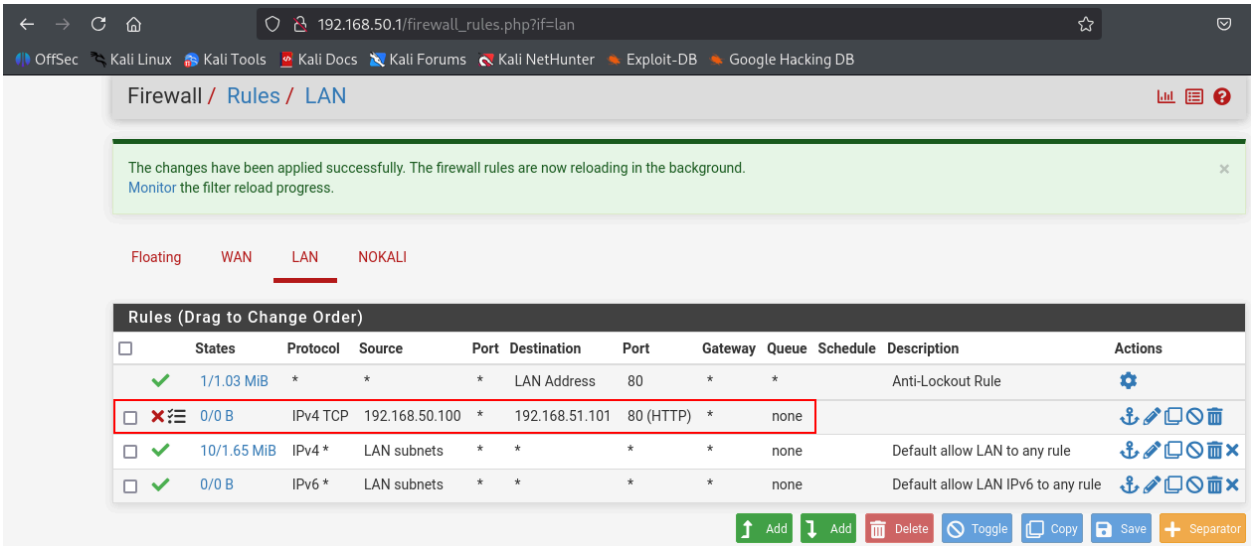
- Avendo già configurato una nuova interfaccia passiamo sulla creazione della regola

- Controlliamo che l’accesso alla DVWA da kali sia possibile

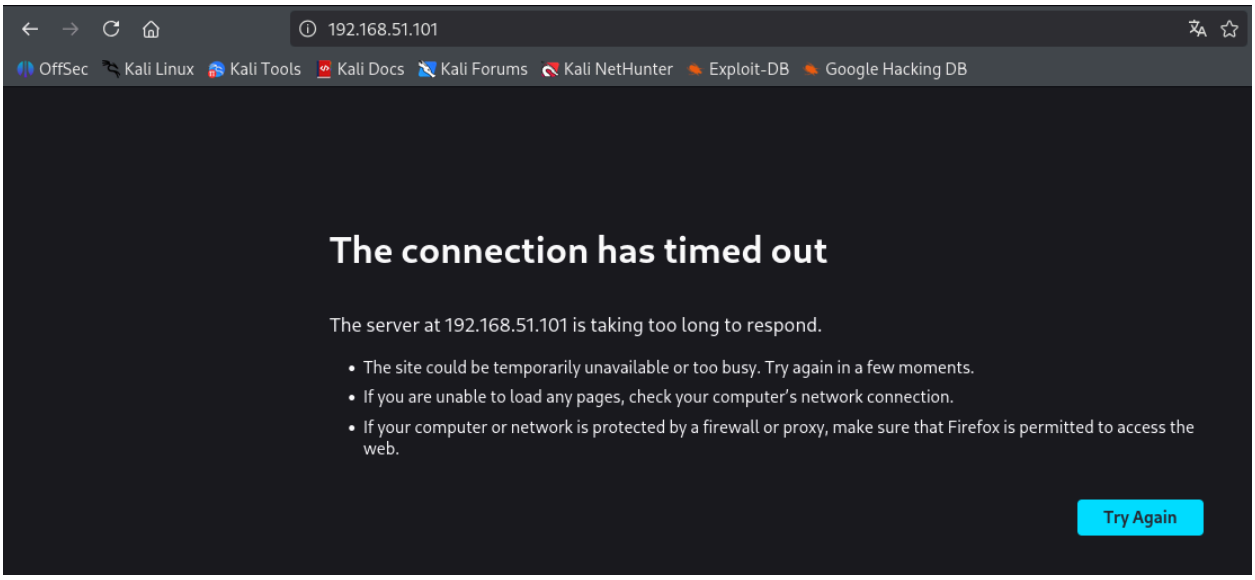


- Visto questo, andiamo su kali sulla pagina browser di pfsense e andiamo in Firewall e dal menù a tendina andiamo in Rules
- Aggiungiamo la regola, mettiamo come azione della regola Block (visto che dobbiamo bloccare l'accesso) , come source , seleziono adress o alias e inserisco l'ip della kali (192.68.50.100), mentre per destination o alias inserisco l'ip della nuova rete data alla metasploitable (192.168.51.101), inoltre essendo che la richiesta dell'esercizio è bloccare l'accesso sulla DVWA, andimao su destination port e selezionamo la porta 80 HTTP.
- Salviamo la configurazione e riproviamo a conneterci.

N.B. durante la configurazione della regola aggiungiamo la spunta sull'extra option Log, per poter svolgere l'esercizio facoltativo



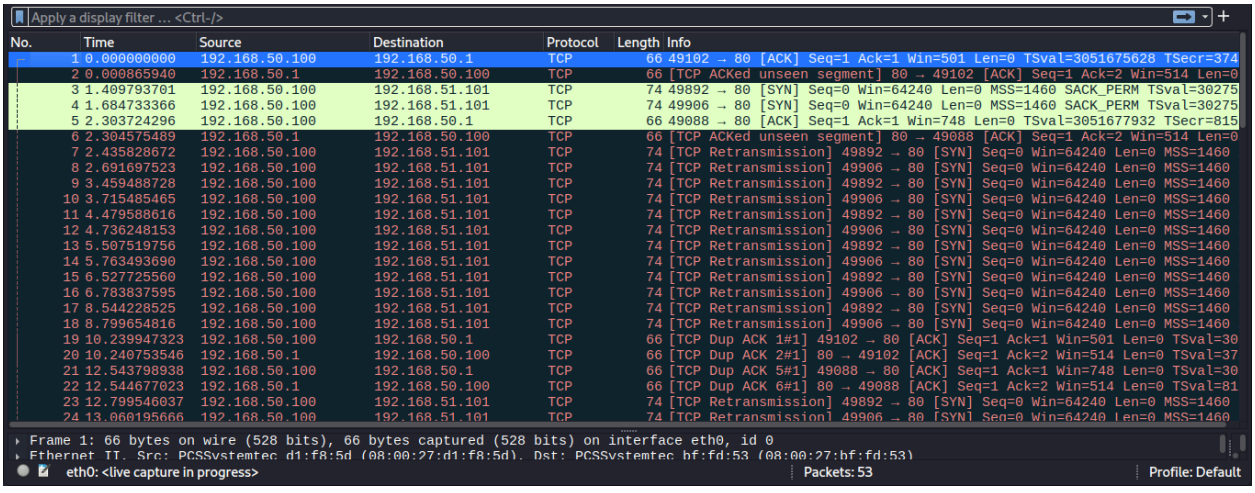
- Appena in funzione vediamo che la nostra regola blocca la comunicazione con la metasploitable, ma solo sulla porta 80.



FACOLTATIVO:

- Ispezionare i log del Firewall

Un ulteriore test può essere controllare il traffico tramite wireshark per vedere cosa succede con l'utilizzo della nostra regola



Possiamo avere la prova che la destinazione non ci sta rispondendo, ed il browser continua ad effettuare tentativi di connessione senza ricevere alcuna risposta.

- Infine, andando su kali sulla pagina browser di pfsense, clicchiamo su Status e dal menù a tendina andiamo su System Logs, andiamo su Firewall e dai log del Firewall abbiamo la conferma che la nostra regola, che abbiamo chiamato Block DVWA from Kali, sta effettivamente bloccando il traffico da Kali verso la DVWA (come vediamo nell'immagine)