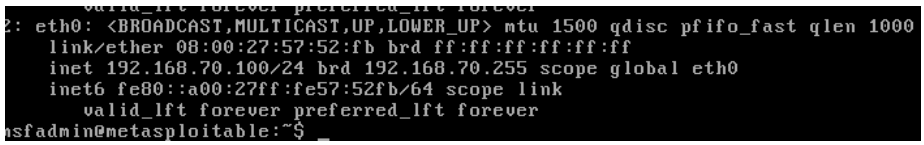
Progetto S3L5.

Creazione policy Pfsense

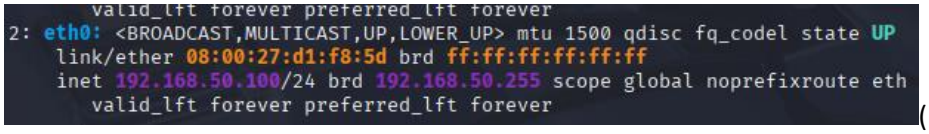
“Crea una regola firewall che blocchi l’accesso alla DVWA (su Metasploitable) dalla macchina Kali Linux e ne impedisca di conseguenza lo scan. Un requisito fondamentale dell’esercizio è che le macchine Kali e Metasploitable siano su reti diverse, potete aggiungere una nuova interfaccia di rete a Pfsense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

Configurazione delle reti:

- **Meta (Metasploitable)** ha IP: 192.168.70.100 con gateway 192.168.70.1.
- **Kali Linux (intnet)** ha IP: 192.168.50.100 con gateway 192.168.50.1.
- Come possiamo notare, le due macchine sono su reti separate.



(Meta)

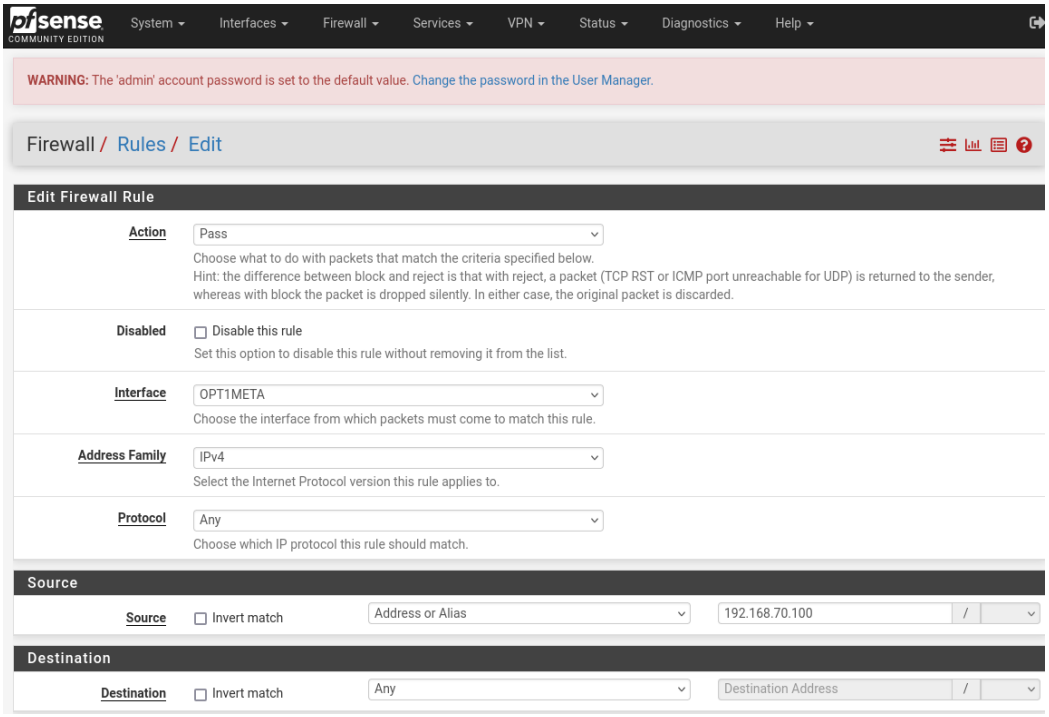


(Kali)

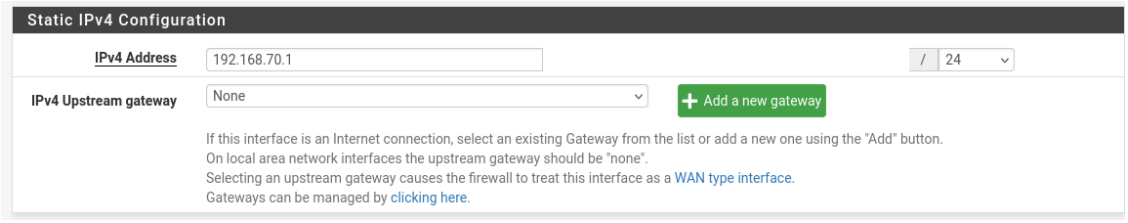
Aggiunta di una nuova interfaccia su pfSense:

Successivamente, è stata configurata una terza rete per pfSense, che funge da gateway tra le due macchine. Per farlo, è stato avviato pfSense, e tramite il browser di Kali Linux è stata aggiunta l'interfaccia OPT1Meta. Dopo aver aggiunto questa interfaccia, è stato necessario configurare il gateway appropriato.

1. Aggiunta dell'interfaccia OPT1Meta a pfSense per gestire la rete Meta.



2. Configurazione del gateway per l'interfaccia Meta.



Impostazione delle Regole su pfSense:

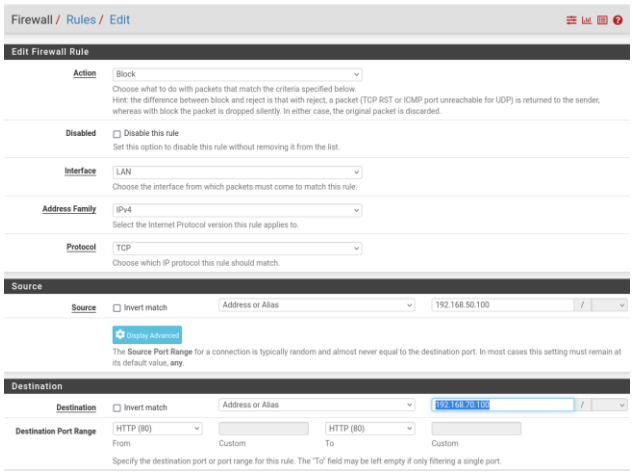
Dopo aver configurato la rete Meta su pfSense, abbiamo creato un set di regole firewall attraverso la tab **"Rules"** di pfSense.

Le regole sono state configurate come segue:

- **Azione: Bloccare** (Block) – La regola blocca i pacchetti che corrispondo ai criteri definiti.
- **Interfaccia: LAN** – La regola si applica ai pacchetti in arrivo sulla rete locale(LAN).
- **Indirizzo di Origine (Source):** L'indirizzo IP **192.168.50.100** (Kali) è stato selezionato come sorgente da bloccare.

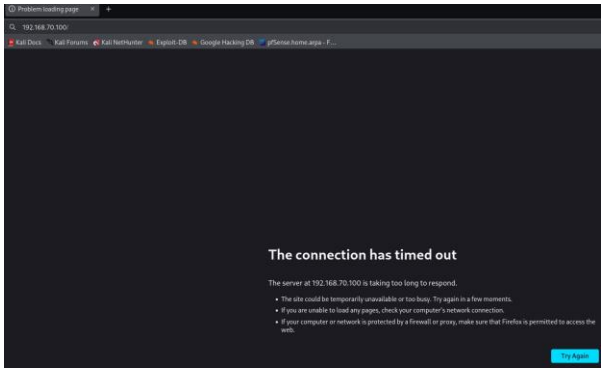
- **Indirizzo di Destinazione (Destination):** L'indirizzo IP **192.168.70.100** (Metasploitable2) è stato selezionato come destinazione da bloccare.
- **Protocollo: TCP** – La regola è applicata ai pacchetti TCP.
- **Porta di Destinazione: HTTP (porta 80)** – La regola impedisce il traffico verso il servizio HTTP sulla macchina Metasploitable.

Questa configurazione blocca l'accesso della macchina Kali al servizio HTTP sulla macchina Metasploitable, impedendo così eventuali scansioni.



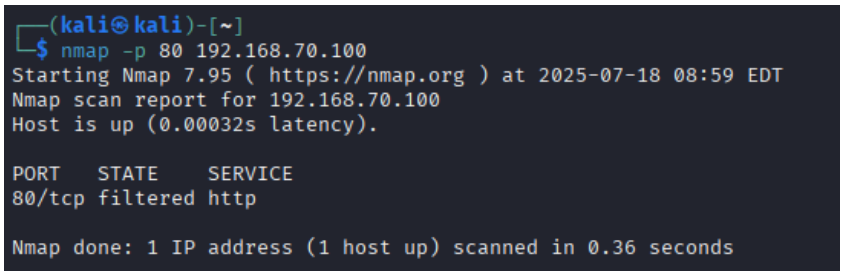
Fatto questo il nostro obbiettivo è stato raggiunto, non ci resta che testarne l'efficienza.

N.B. Qualsiasi tipo di modifica viene apportata su PfSense va salvata, altrimenti l'impostazione andrà persa una volta lasciata la pagina.



Una volta configurato il firewall con le regole appropriate, l'obiettivo è stato raggiunto, e l'accesso a DVWA su Metasploitable è stato correttamente bloccato da Kali.

Ora, per testare l'efficacia della regola, sarà necessario eseguire una scansione con **Nmap** sul terminale di Kali per verificare se il traffico viene effettivamente bloccato.



Nmap indica che la porta **80/tcp**, utilizzata dal servizio HTTP su Metasploitable, è **"filtered"**. Questo significa che il traffico diretto alla porta HTTP è stato bloccato, senza che Nmap ricevesse una risposta chiara. Questo è coerente con l'obiettivo della regola firewall che abbiamo creato precedentemente.

Quindi, la regola firewall che abbiamo creato sta funzionando correttamente, bloccando l'accesso alla DVWA su Metasploitable da Kali Linux, come richiesto dall'esercizio.

Conclusioni personali:

Oggi l’esercizio ha messo alla prova le conoscenze che ho acquisito finora, e inizialmente non nego di essermi sentito sopraffatto. Tuttavia, ho cercato di mantenere la calma, affrontando ogni fase con logica e pazienza, questo mi ha permesso di visualizzare i passaggi necessari per arrivare alla soluzione. So che il mio report possa essere migliorato, ma ho preferito focalizzarmi prima sulla risoluzione della traccia, per poi dedicarmi con alla documentazione finale. Sono consapevole che questa scelta influirà sul livello del mio documento, ma credo che l’approccio che ho adottato mi abbia permesso di arrivare alla soluzione.