Creazione rete firewall

1. Prefazione

Nel report di oggi, viene chiesto di creare una rete firewall all'interno della stessa rete, come da consegna dovremo creare una Policy avvalendoci dello strumento PFsense e negare, attraverso una rete sorgente, un IP di destinazione; gli IP della Kali e di Metasplotable devono essere su reti diverse

2. Strumenti

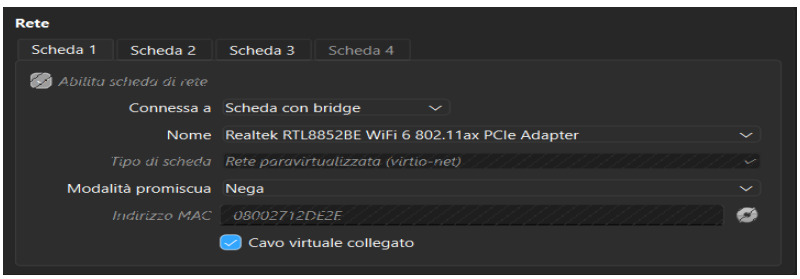
Per fare ciò che la consegna ci chiede, avremo bisogno di 3 Macchine virtuali:

- Kali linux: la macchina sorgente da cui dovremo operare per configurare Pfsense e negare il traffico alla macchina Metaspltable.
- Pfsense: che farà da router a cui dovremo impartire gli ordini di bloccare il traffico della Metasplotable
- Metasplotable: la macchina target da bloccare

3. Configurazione

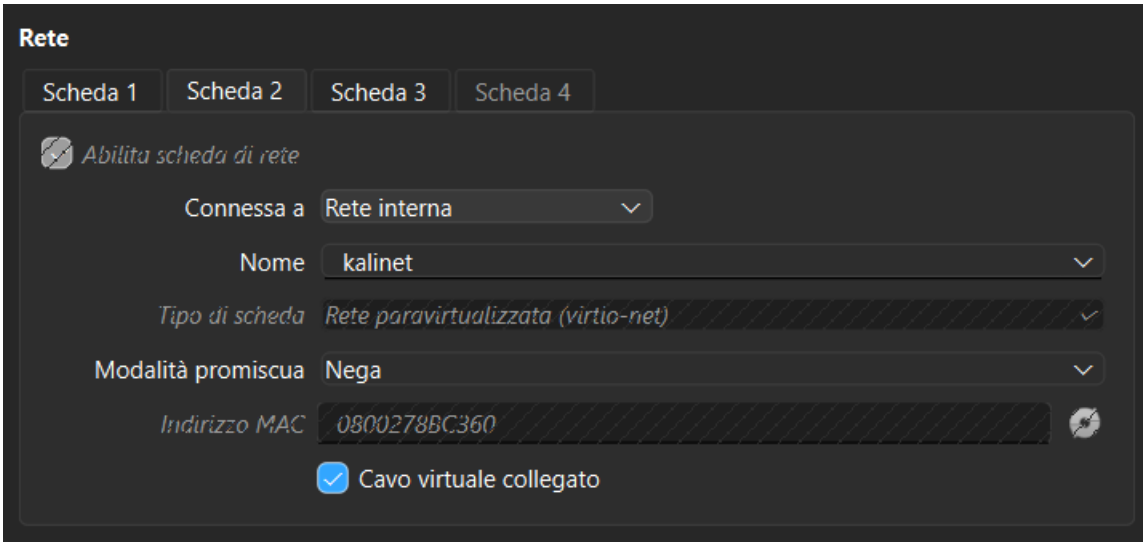
Per poter configurare i dispositivi come da consegna, dobbiamo aprire innanzitutto Oracle Virtual Box per poter gestire le nostre VM, andare in impostazioni della PFsense e assegnarle 3 schede di rete:

- Scheda rete1:



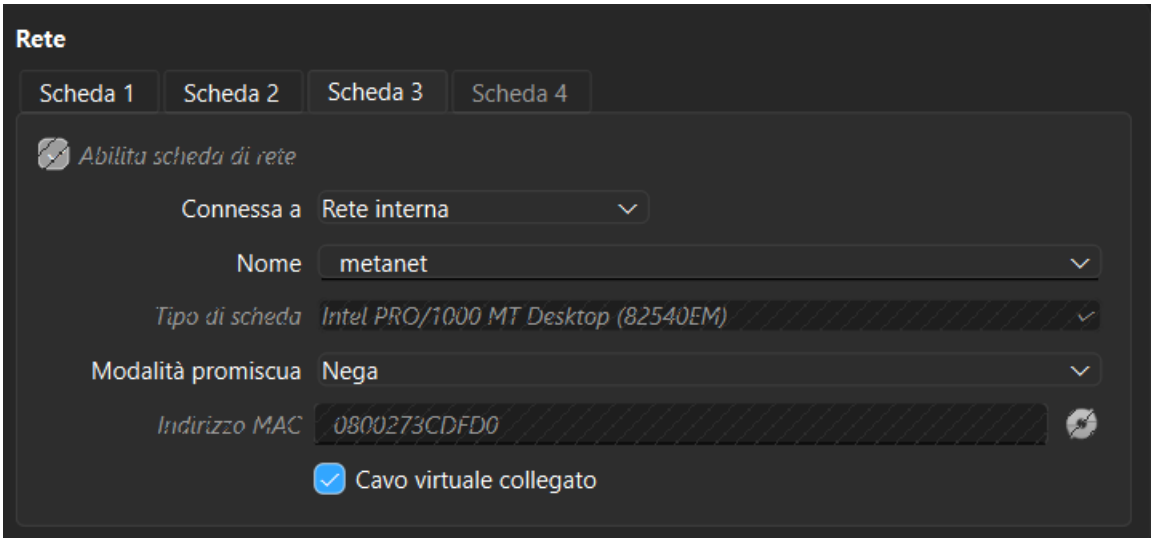
Scheda in Bridge, in modo da far condividere l'IP del nostro router di casa alla PFsense, sarà quindi la nostra rete WAN.

- Scheda rete2:



Creiamo una rete LAN per connettere la Kali con la PFsense

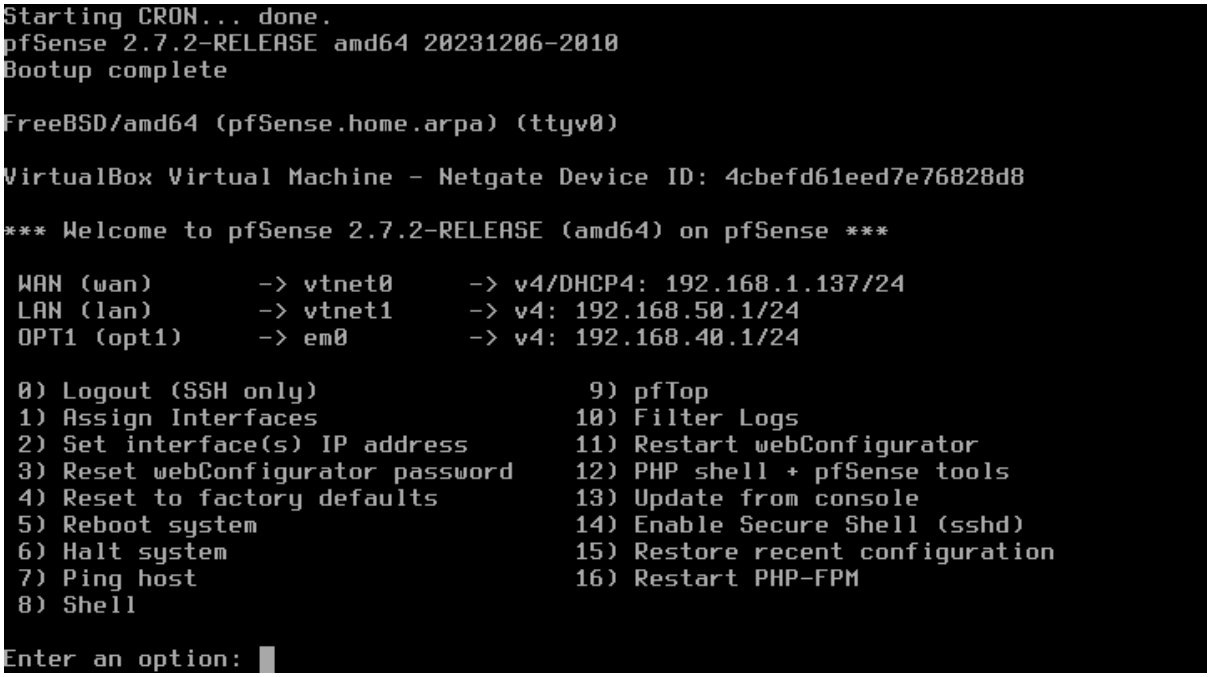
- Scheda rete3:



Creiamo una rete LAN per connettere la Metasplotable con la PFsense

Una volta create le 3 schede di rete, apriamo rispettivamente PFsense e Kali per avere le configurazioni desiderate per la Kali e per la Metasplotable.

Aprendo PFsense, prendiamo l'indirizzo IP



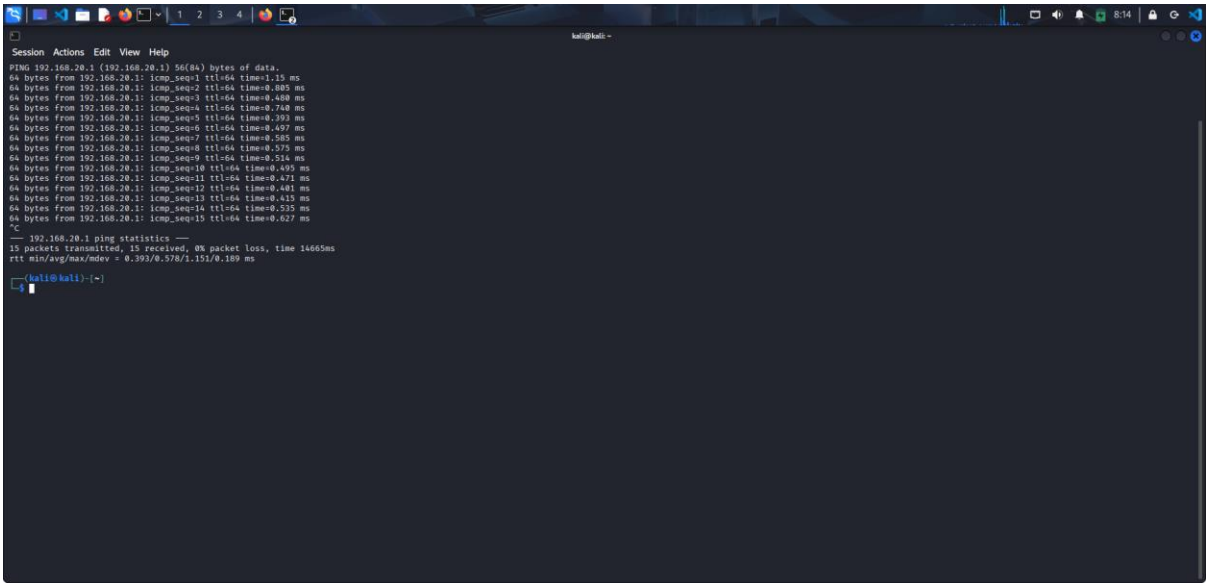
Prendiamo l'IP della PFsense e utilizziamo il browser della Kali: 192.168.1.137.

Facciamo l'accesso e andiamo nel menù, andiamo in "Interfces" e andiamo in "Assignments", dovrebbe portarci la voce ADD, selezioniamo OPT1, e successivmanete riguardando nella PFSense, ora abbiamo 3 schede, come da Screen; andiamo nella opzione 2, e configuriamo in modo che venga assegnato il DHCP alla Metasplotable.

Apriamo Metasplotable per modificare il file di rete con sudo nano /etc/network/interfaces

Poi modifichiamo static a DHCP.

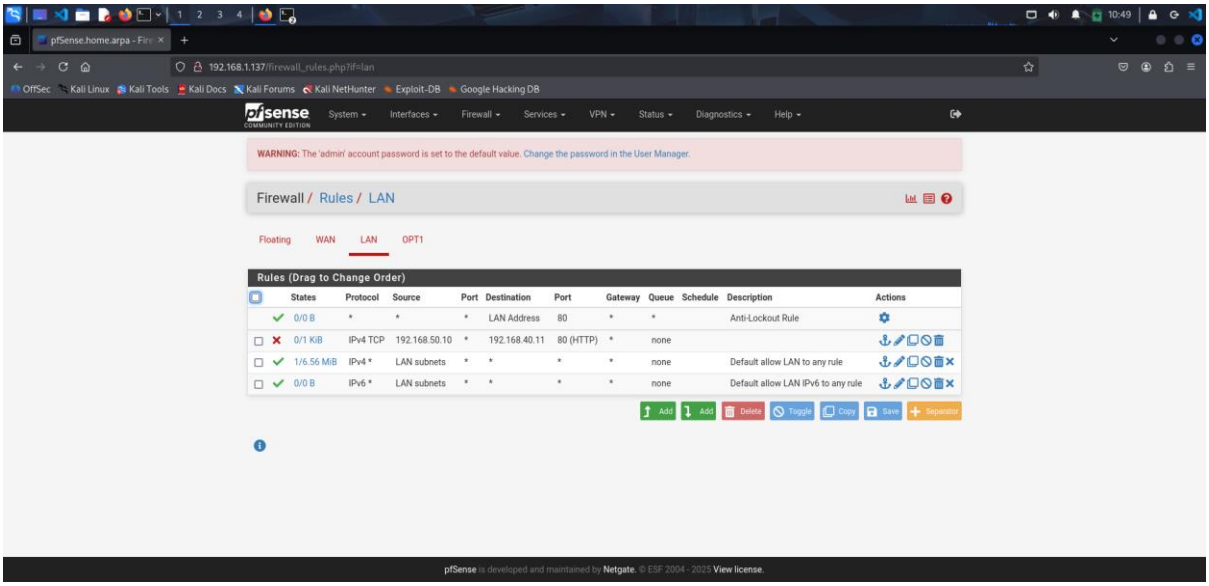
Una volta fatto ciò, dovrebbe essere tutto collegato, facciamo il ping dalla Kali alla Meta.



E’ apposto, Metasplotable è contattabile.

4. Policy Firewall

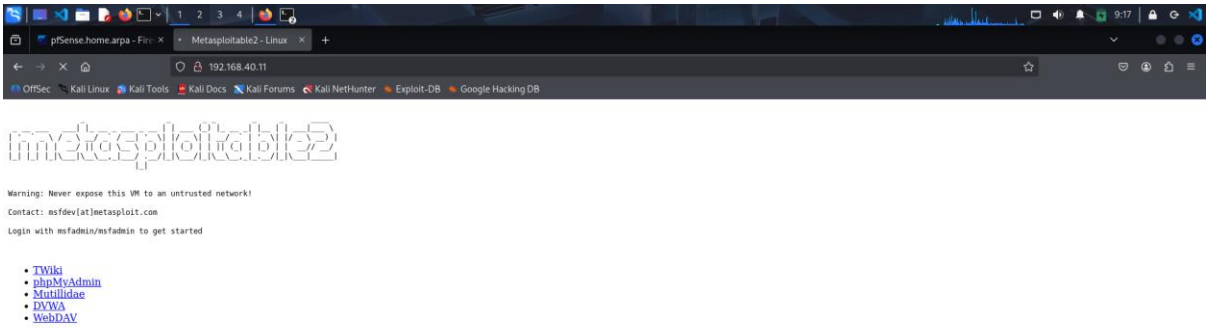
Come ultimo step, attraverso PFSense dobbiamo implementare un firewall in grado di bloccare il traffico dalla Kali alla Meta, quindi ritorniamo sul browser della Kali, entriamo in Pfsense e andiamo in “Firewall”, “Rules”; avremo 4 Opzioni:
Floating, WAN, LAN e OPT1.
A noi interessa interrompere il traffico all’interno della LAN, quindi clicchiamo lì e dovremo trovarci davanti una cosa del genere:



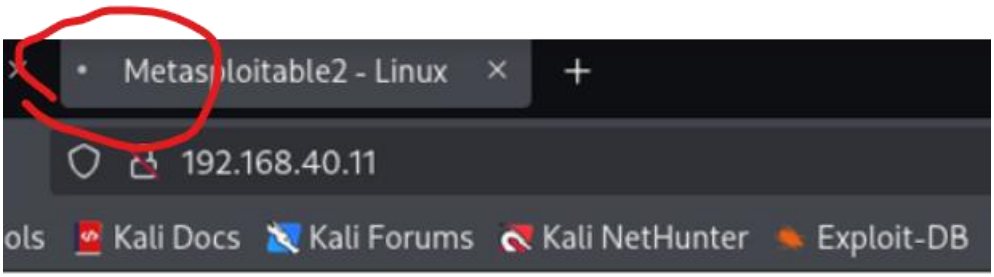
Andiamo in ADD e creiamo una nuova regola, consci del fatto che per poter funzionare, la regola deve essere in alto, come da screen.

Le azioni saranno le seguenti:

- In “Action” spuntiamo block: non solo non vogliamo far passare i pacchetti, ma non vogliamo notificare l’altra parte dello scambio fallito. (Abbiamo pass per far passare i pacchetti, Reject per bloccarli e notificare, e Block per non notificare).
- Interface: LAN: noi vogliamo ancora una volta confermare che vogliamo bloccare un dato indirizzo nella rete LAN di cui facciamo parte
- Address Family IPV4: la famiglia di configurazione a cui siamo interessati
- Protocol: quale tipo di protocollo vogliamo respingere
- Source: Address or Alias; la sorgente è la macchina che sta puntando il traffico da bloccare, in questo caso è la nostra Kali
- Destination: Address or Alias; la macchina puntata.
  Ed è la nostra Metasplotable.
  Salviamo e verifichiamo



Questo è prima di applicare la regola.
Successivamente, applicata la regola non lo sarà piu.


Metasploitable2 - Linux
192.168.40.11
ols
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB