Configurazione Firewall su pfSense per Isolamento Metasploitable2

L'obiettivo dell'esercizio è stato quello di configurare un ambiente di rete segmentato tramite pfSense, in modo da bloccare l'accesso alla piattaforma DVWA presente sulla macchina Metasploitable2 quando la connessione proviene dalla macchina Kali Linux. Questo risultato è stato ottenuto creando una terza interfaccia di rete su pfSense, configurandola e applicando una regola firewall mirata. Pur impedendo l'accesso HTTP alla Metasploitable, era necessario che il traffico ICMP (ping) rimanesse consentito, così da verificare che il blocco riguardasse solo il servizio web e non la raggiungibilità generale.

Struttura della Rete

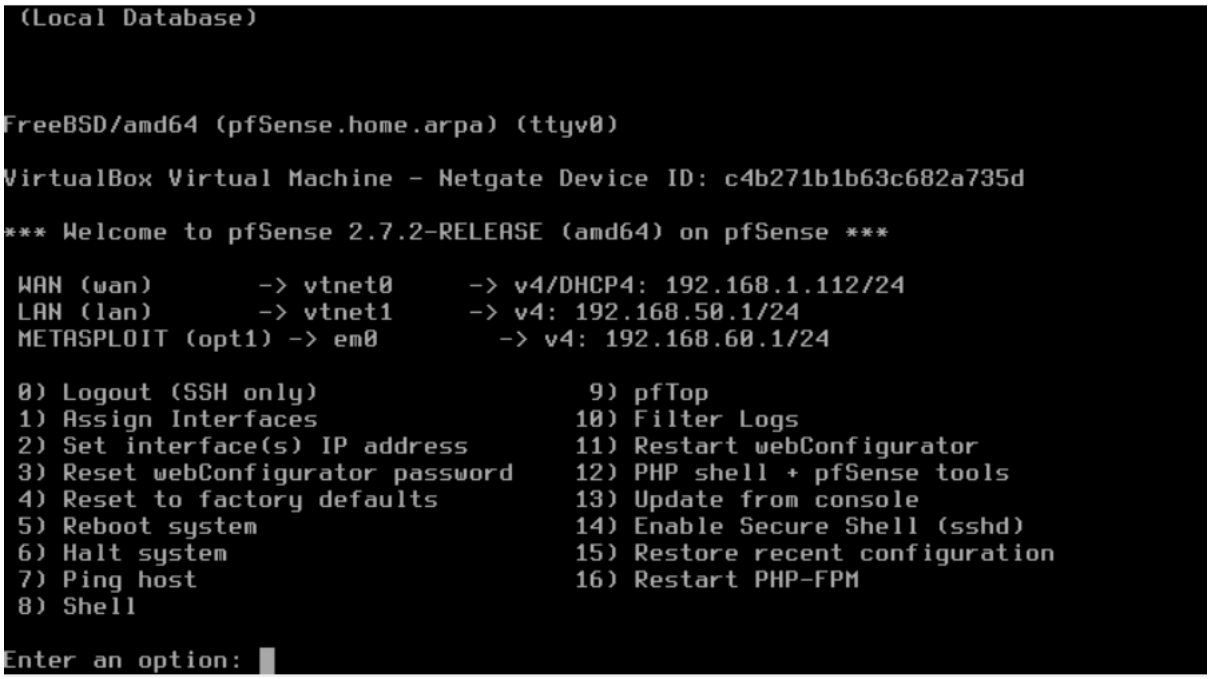
Nel sistema pfSense sono state configurate tre interfacce:

WAN – Rete esterna

LAN – Rete Kali Linux

METASPLOIT – Rete Metasploitable2

Durante l'avvio della macchina di pfSense è stato possibile verificare la loro corretta assegnazione e gli indirizzi IP associati.

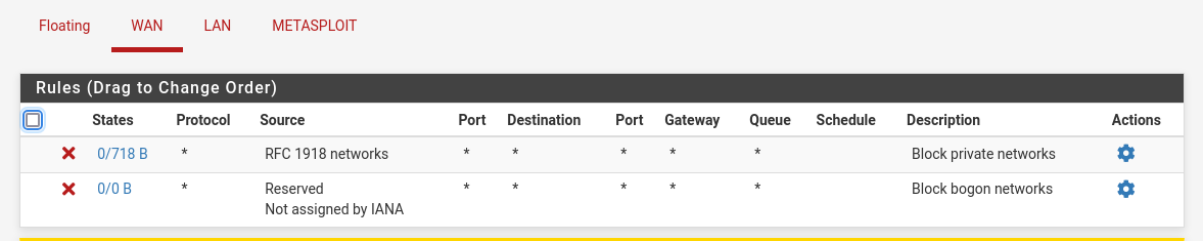


La macchina Kali è stata collegata alla rete LAN mentre Metasploitable è stata collegata alla OPT1(METASPLOIT), garantendo così una separazione fisica e logica tra i due host vulnerabile e attaccante.

Configurazione WebGUI di pfSense

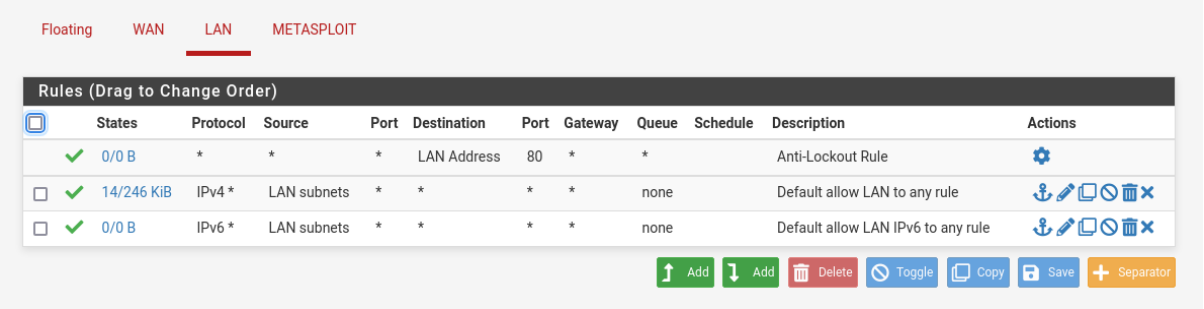
Accedendo alla WebGUI di pfSense dalla Kali, è stata attivata l'interfaccia OPT1 e configurata con un indirizzo IP statico coerente con la rete dedicata a Metasploitable2. Successivamente sono state analizzate le regole firewall predefinite di ciascuna interfaccia.

Regole Firewall – WAN



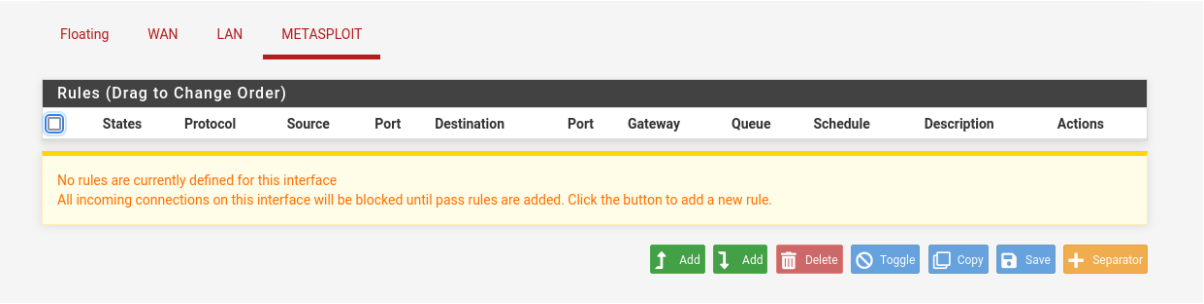
La WAN mantiene le sue regole standard e non richiede modifiche poiché il traffico che ci interessa filtrare è quello proveniente dalla LAN verso OPT1.

Regole Firewall – LAN



Sulla LAN è presente la regola che permette il traffico in uscita verso qualsiasi destinazione. Questa regola permette inizialmente alla Kali di accedere alla DVWA sulla Metasploitable.

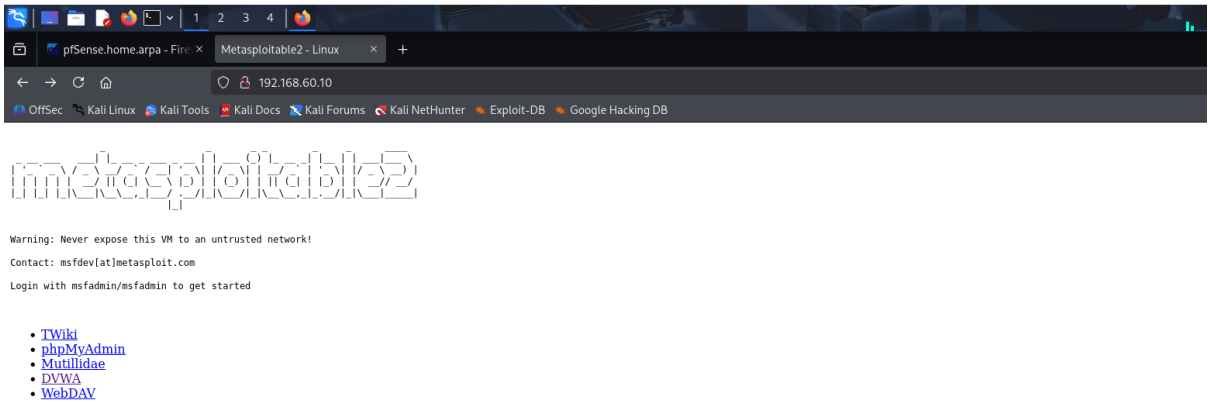
Regole Firewall – OPT1



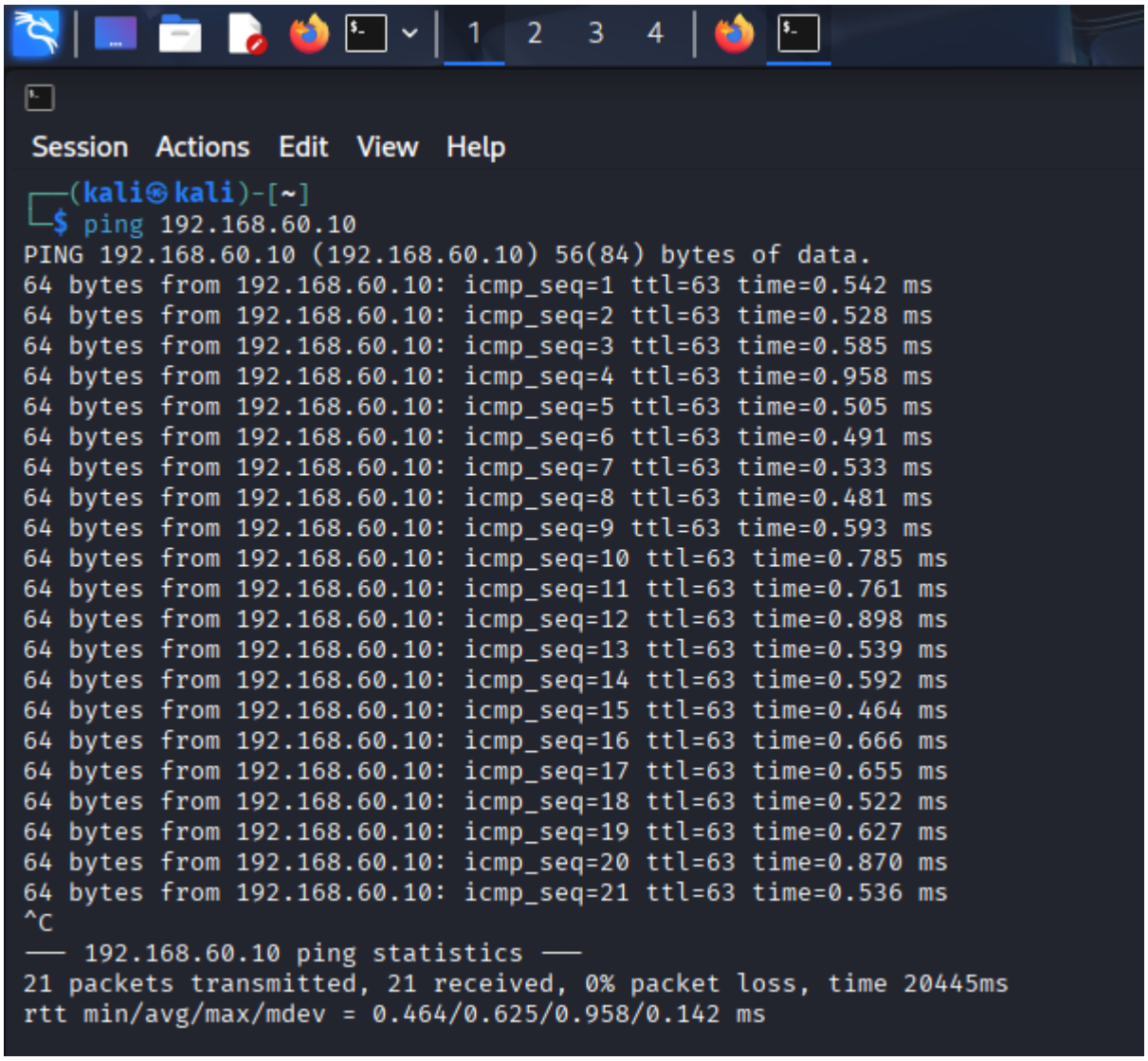
Test prima dell'applicazione della regola

Prima di introdurre il blocco, ho verificato che la Kali fosse in grado di:

Accedere alla pagina DVWA esposta dalla Metasploitable2



Eseguire un ping verso l'indirizzo IP della Metasploitable



Questi test dimostrano che inizialmente non esiste alcun filtraggio tra le due macchine e che la Kali può liberamente comunicare con Metasploitable.

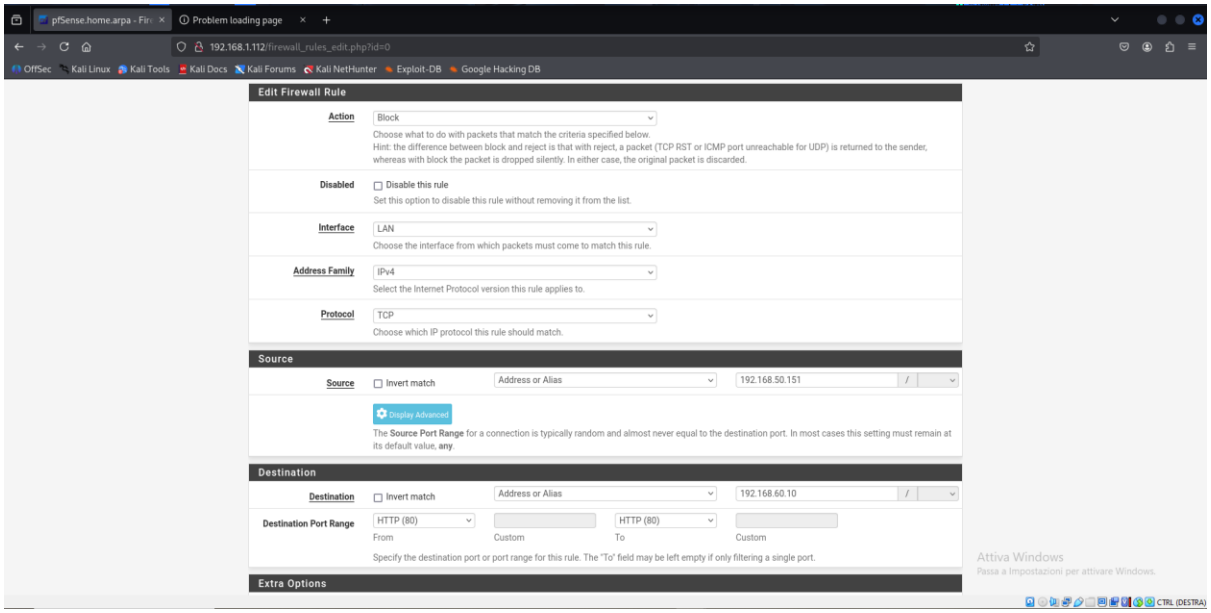
Creazione della regola di blocco

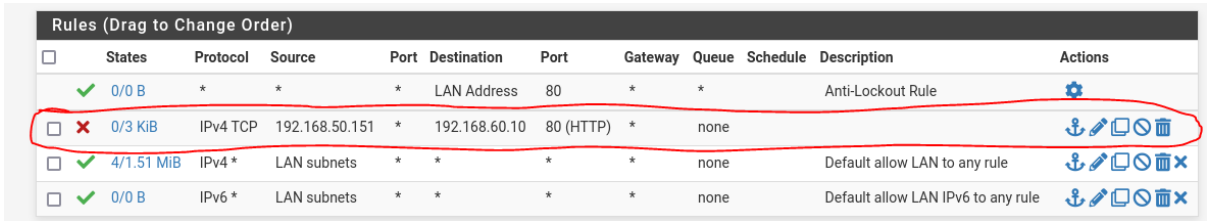
Per impedire l'accesso HTTP, ho inserito una regola firewall sull'interfaccia OPT1 che:

- Blocca il traffico TCP
- Proveniente dalla rete LAN
- Diretto alla macchina Metasploitable2
- Sulla porta 80 (HTTP)

La regola è stata posizionata in testa alla lista, così da essere applicata prima delle regole generiche di allow.

Dopo aver salvato le modifiche, pfSense ha applicato il nuovo comportamento immediatamente.

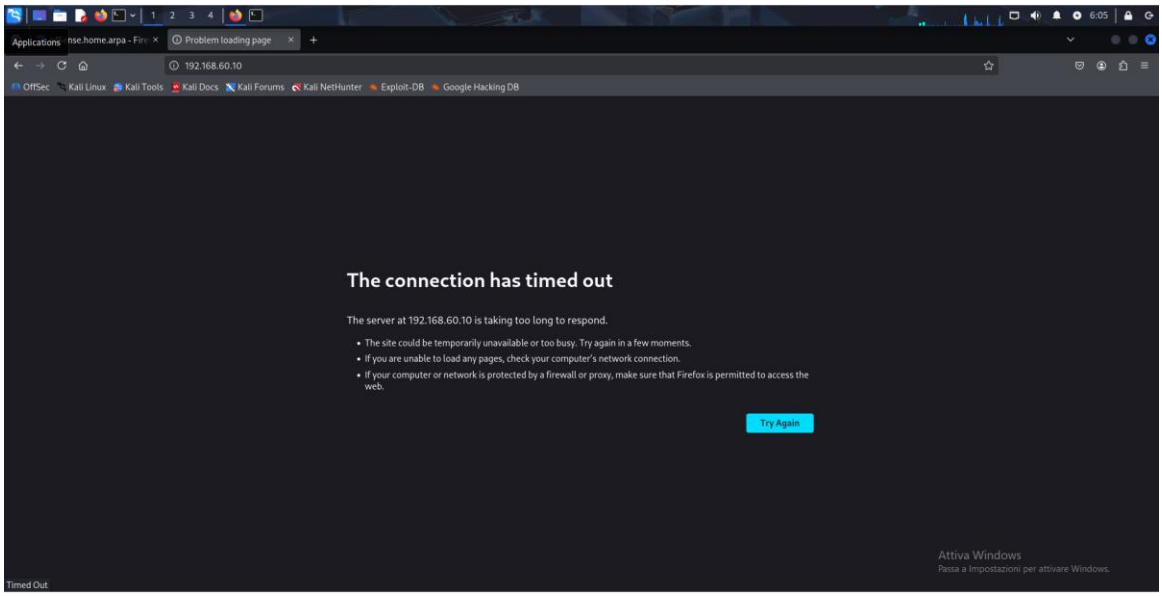




Test dopo l’applicazione della regola

Dopo l’inserimento della regola firewall, ho eseguito nuovamente i test:

Il browser della Kali non riesce più ad accedere alla DVWA, ricevendo timeout o connection refused.



Il ping verso Metasploitable continua a funzionare, confermando che è stato bloccato solo il traffico HTTP.

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.60.10
PING 192.168.60.10 (192.168.60.10) 56(84) bytes of data.
64 bytes from 192.168.60.10: icmp_seq=1 ttl=63 time=8.21 ms
64 bytes from 192.168.60.10: icmp_seq=2 ttl=63 time=0.512 ms
^[[B^[[B^[[B^[[B^[[B^[[B64 bytes from 192.168.60.10: icmp_seq=3 ttl=63 time=1.14 ms
64 bytes from 192.168.60.10: icmp_seq=4 ttl=63 time=0.466 ms
64 bytes from 192.168.60.10: icmp_seq=5 ttl=63 time=0.438 ms
64 bytes from 192.168.60.10: icmp_seq=6 ttl=63 time=0.932 ms
64 bytes from 192.168.60.10: icmp_seq=7 ttl=63 time=0.419 ms
64 bytes from 192.168.60.10: icmp_seq=8 ttl=63 time=0.491 ms
64 bytes from 192.168.60.10: icmp_seq=9 ttl=63 time=0.431 ms
64 bytes from 192.168.60.10: icmp_seq=10 ttl=63 time=0.455 ms
64 bytes from 192.168.60.10: icmp_seq=11 ttl=63 time=0.442 ms
64 bytes from 192.168.60.10: icmp_seq=12 ttl=63 time=0.482 ms
64 bytes from 192.168.60.10: icmp_seq=13 ttl=63 time=0.485 ms
^C
── 192.168.60.10 ping statistics ──
13 packets transmitted, 13 received, 0% packet loss, time 12192ms
rtt min/avg/max/mdev = 0.419/1.145/8.208/2.049 ms
```

Questi risultati confermano che il firewall è stato configurato correttamente e in modo granulare.