Progetto S3/L5 – Creazione policy pfSense

Obiettivo:

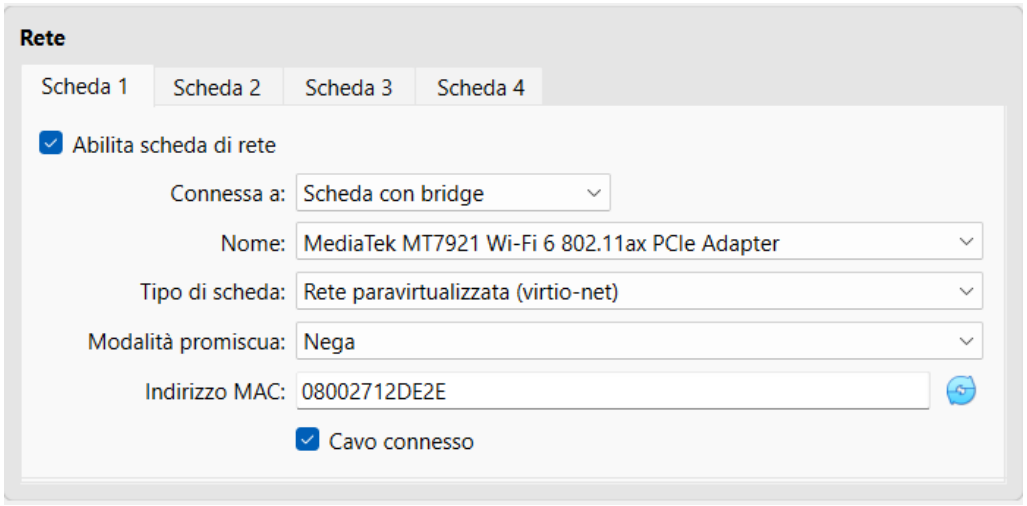
L'obiettivo di questo progetto è quello di configurare un ambiente virtuale e di implementare una regola di firewall su pfSense, al fine di bloccare l'acceso e lo scan tra due macchine virtuali, Kali Linux e Metasploitable2, collocate su due reti differenti.

I. Architettura di rete e configurazione

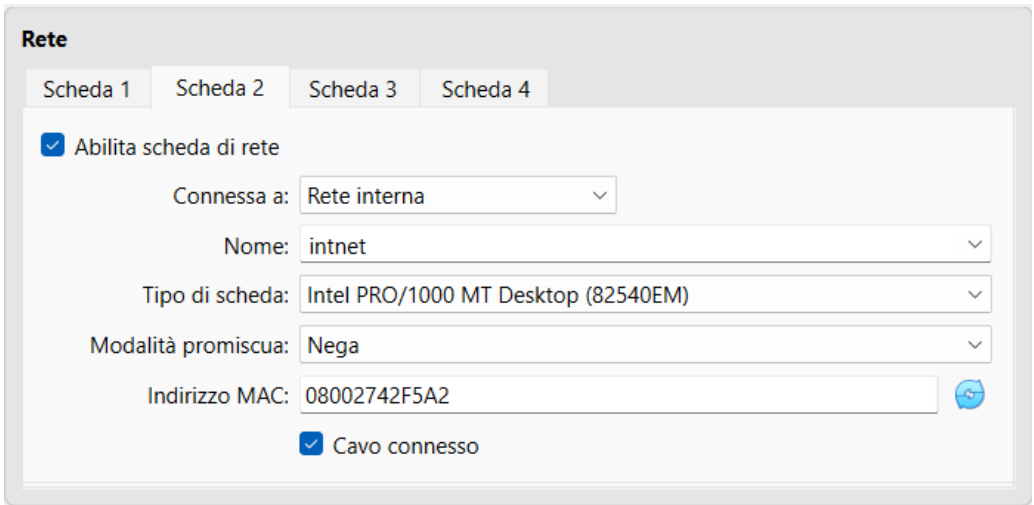
Per simulare l'ambiente richiesto, è stata implementata la seguente topologia di rete in Oracle VirtualBox:

- **pfSense**: macchina intermediaria che gestisce tre interfacce di rete e agisce da firewall.
- **Kali Linux**: la macchina da cui viene tentato l'accesso e lo scan della porta. È collocata su una rete LAN chiamata intnet.
- **Metasploitable2**: la macchina bersaglio. È collocata su un'altra rete LAN chiamata intnet1.

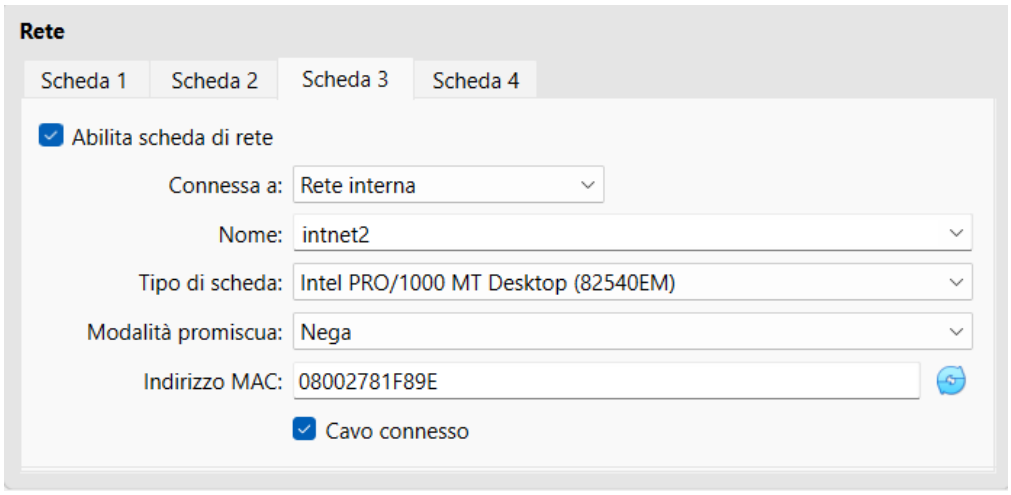
Scheda di rete 1 pfSense



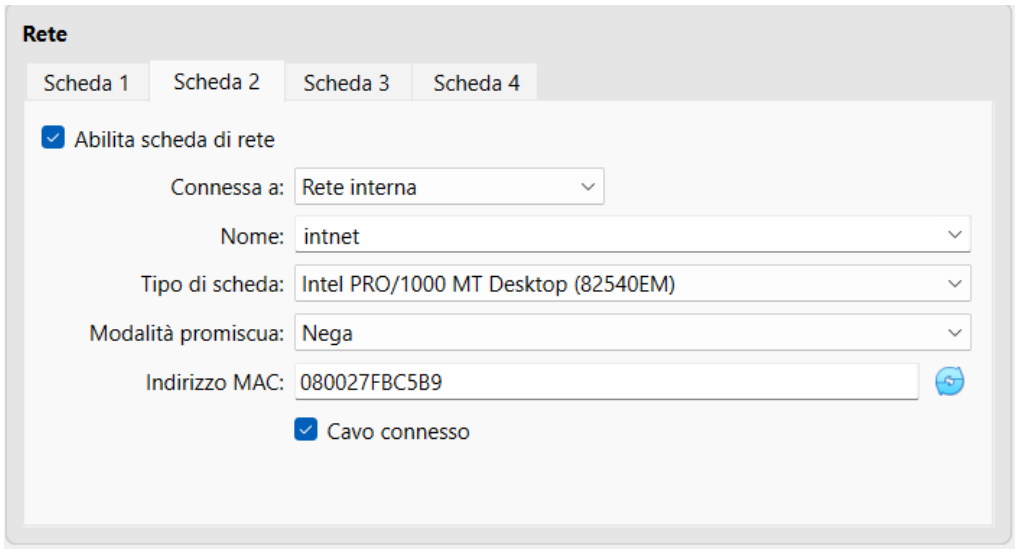
Scheda di rete 2 pfSense



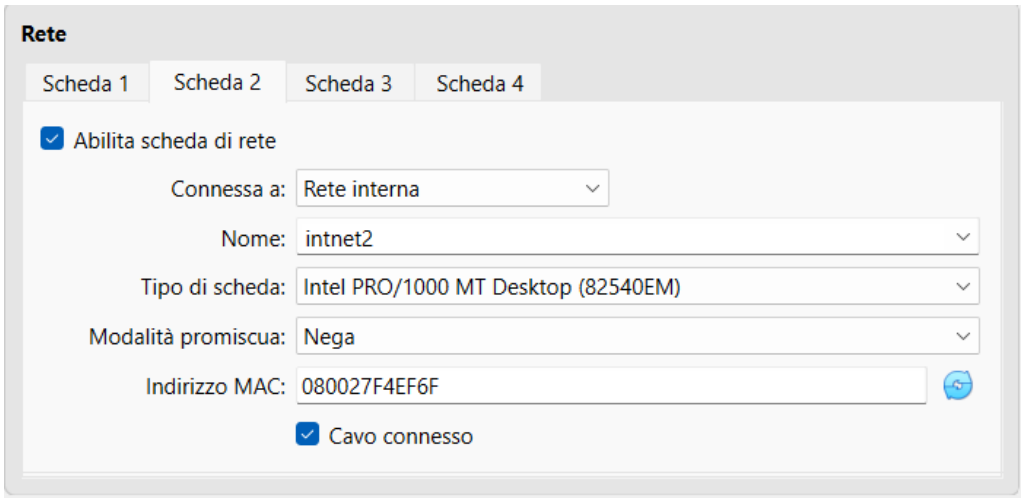
Scheda di rete 3 pfSense



Scheda di rete Kali Linux



Scheda di rete Metasploitable2



II. Configurazione degli indirizzi IP

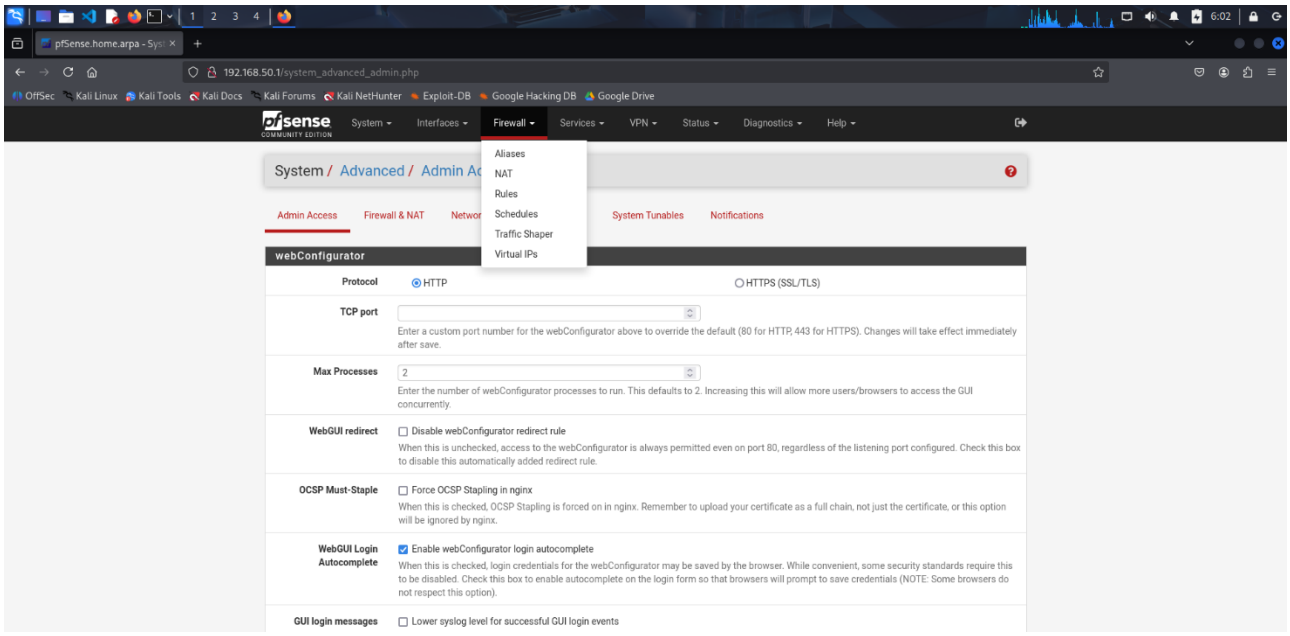
Dopo aver configurato le schede in VirtualBox e avviato le VM, sono stati assegnati i seguenti indirizzi IP:

- **pfSense:**
  - **Scheda con bridge**: 192.168.1.111/24
  - **LAN1**: 192.168.50.1/24 (gateway per Kali).
  - **LAN2**: 192.168.60.1/24 (gateway per Metasploitable2).
- **Kali Linux**:
  - **IP**: 192.168.50.100/24
  - **Default gateway**: 192.168.50.1
- **Metasploitable2**:
  - **IP**: 192.168.60.101/24
  - **Default gateway**: 192.168.60.1

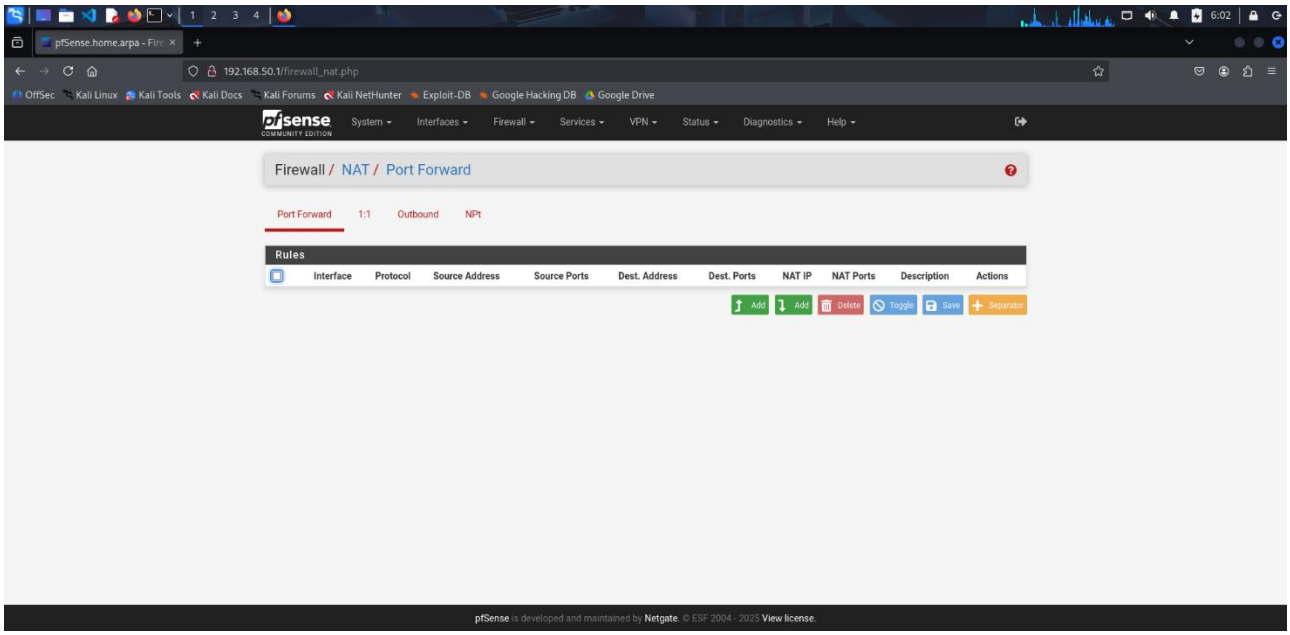
III. Creazione della regola firewall

Tramite pfSense Web (raggiunto da Kali con https://192.168.50.1), è stato configurato un firewall per bloccare le connessioni TCP dirette alla porta 80 di Metasploitable2.

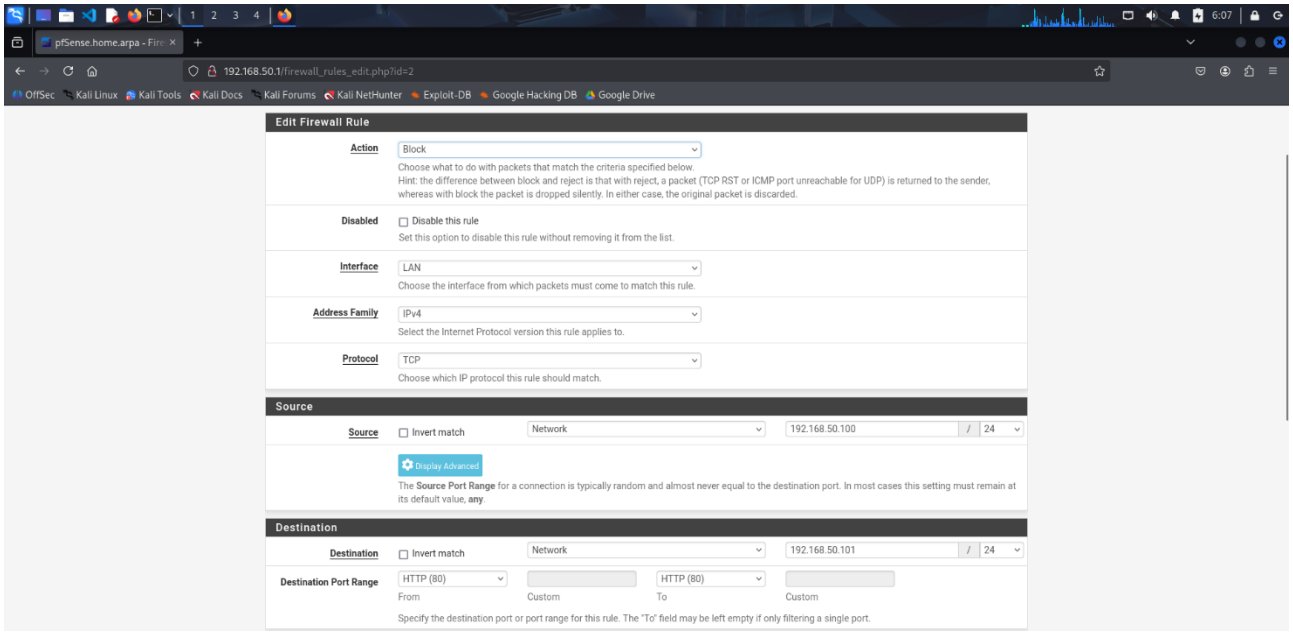
1) Cliccare su 'Firewall' e dopodiché su 'Rules'



2) Cliccare su ‘Add’ per creare una nuova regola



3) Regole per la configurazione del firewall



IV. Verifica del funzionamento del firewall

Dopo l'applicazione della regola, ho effettuato due test di connettività per verificare l'efficacia del firewall.

Scan Nmap sulla porta 80 di Metasploitable2 (nmap -Pn -p 80 192.168.60.101)

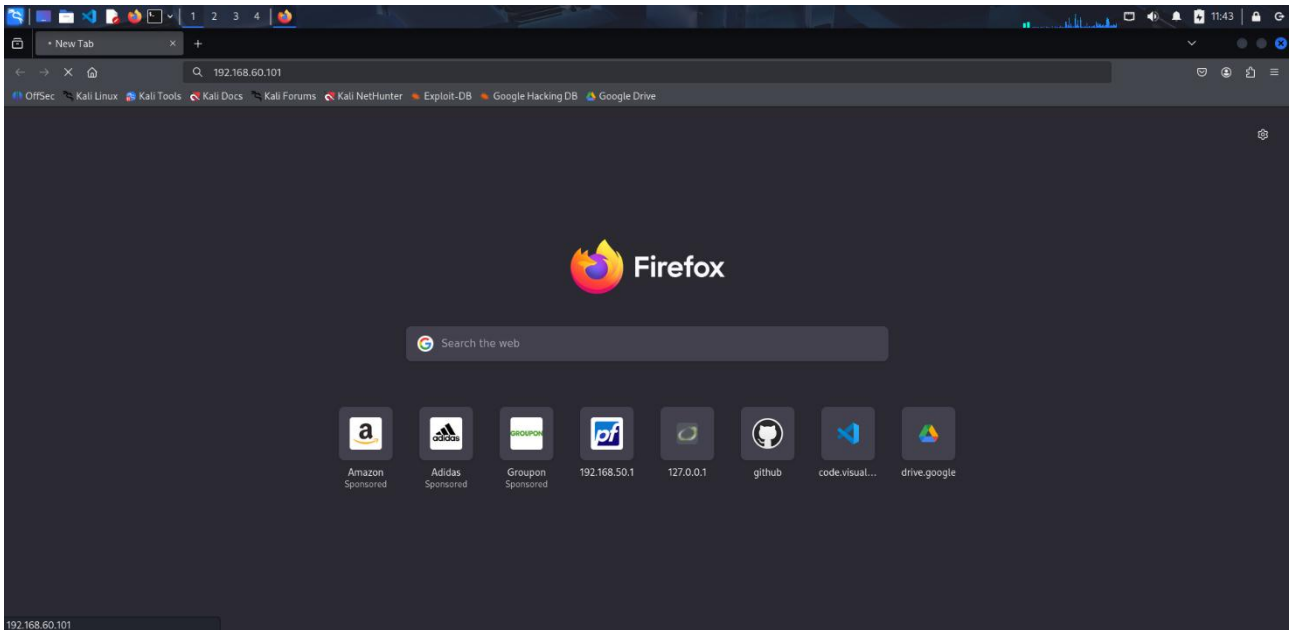
```
┌──(kali㉿kali)-[~]
└─$ nmap -Pn -p 80 192.168.60.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-18 05:57 EDT
Nmap scan report for 192.168.60.101
Host is up.

PORT   STATE    SERVICE
80/tcp filtered http

Nmap done: 1 IP address (1 host up) scanned in 2.19 seconds
```

La porta 80 risulta filtrata dal firewall.

Tentativo di accesso all'applicazione web di Metasploitable2 dalla macchina Kali Linux tramite il browser web.



La connessione non riesce a stabilirsi (schermata di caricamento fissa).

V. Conclusioni

L'esercizio è stato completato con successo. La configurazione della rete ha permesso di isolare la Kali e la Metasploitable2 su due reti differenti, rimanendo però in comunicazione grazie a pfSense. La regola firewall è riuscita a bloccare correttamente il traffico sulla porta 80 dalla Kali alla Metasploitable2.