Progetto S3/L5

In questo laboratorio l'obiettivo è stato configurare una regola **firewall** su **pfSense** per impedire a una macchina attaccante (**Kali Linux**) di effettuare scansioni o accedere alle applicazioni web (nello specifico è stato utilizzato **DVWA**) ospitata su una macchina target (**Metasploitable**). Un requisito fondamentale è stato garantire la segmentazione della rete, posizionando le due **macchine** su sottoreti distinte.

Come prima cosa dobbiamo configurare le "schede di rete virtuali" su VirtualBox. Dobbiamo simulare che **Kali** e **Metasploitable** siano in due stanze diverse, collegate solo da **pfSense**.

1. Configurazione pfSense (router centrale)

Andando sulle impostazioni di rete impostiamo le 3 schede di rete di cui abbiamo bisogno.

- **Scheda 1 (WAN):** "Scheda con bridge" (dà accesso ad internet).
- **Scheda 2 (LAN):** Impostata su **Rete Interna** (chiamala **kalinet**).
- **Scheda 3 (OPT1):** Abilitiamo la scheda e la impostiamo su **Rete Interna** (chiamala **metasplnet**).

Si imposta in questo modo perchè pfSense deve avere un piede in ogni rete per poterle collegare e filtrare.

2. Configurazione Kali (macchina attaccante)

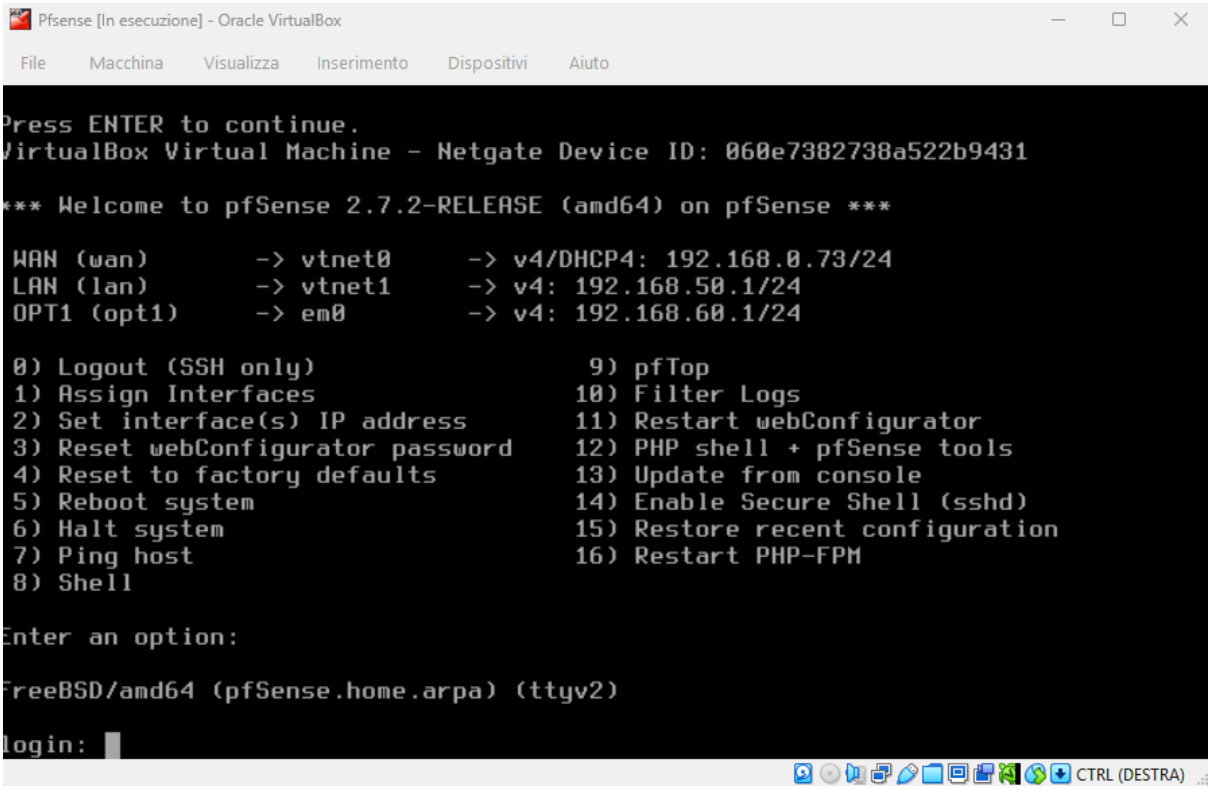
- Andiamo sulle impostazioni di rete della **Kali Linux** e impostiamo come la scheda di rete su “ **Rete Interna** ” selezionando **“kalinet”.**

3. Configurazione Metasploitable (macchina attaccata)

- Andiamo sulle impostazioni di rete della **Metasploitable** e impostiamo come la scheda di rete su “ **Rete Interna** ” selezionando **“metasplnet”.**

Successivamente ci colleghiamo dal browser della **Kali** all’interfaccia web della pfSense per impostare una nuova interfaccia di rete, in questo caso sarà **OPT1**, che corrisponderà alla rete “**metasplnet**”.

Configurazione delle schede di rete su pfSense

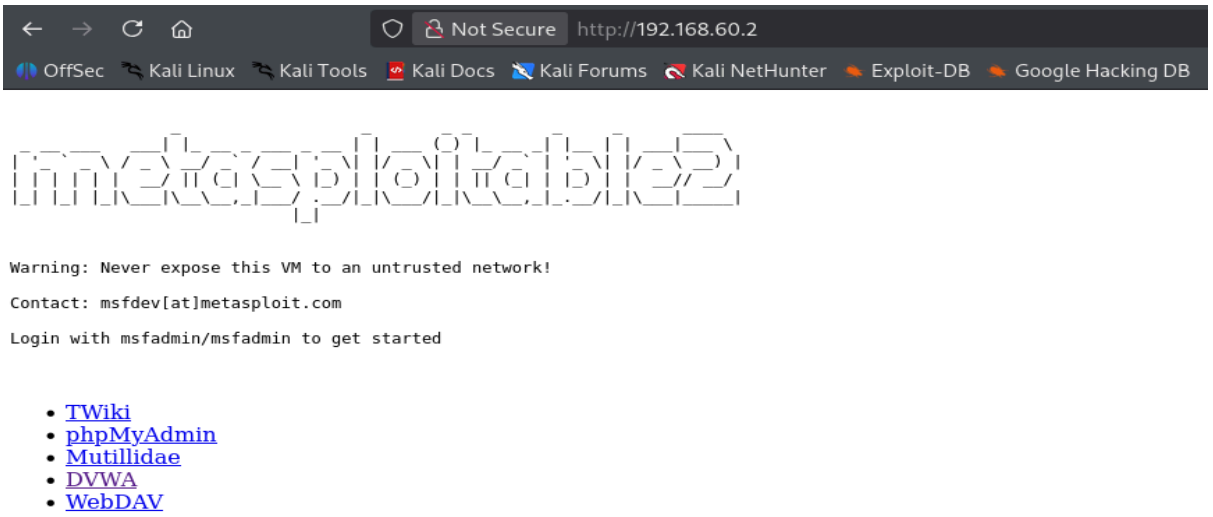


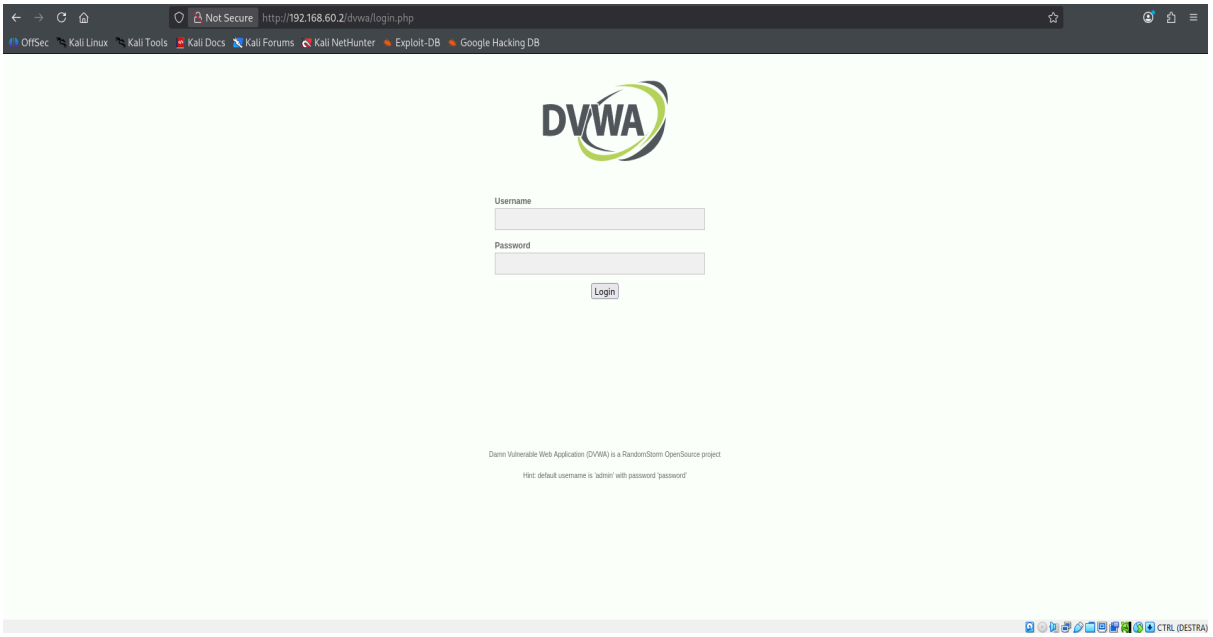
Da questa schermata si può osservare la configurazione delle 3 schede di rete:

1. **WAN** (dà accesso ad internet)
2. **LAN** (rete relativa alla Kali)
3. **OPT1** (rete relativa alla Metasploitable)

Collegamento interfaccia web della Metasploitable da browser della Kali.

Prima di andare ad impostare le regole del **Firewall** verifichiamo l'effettiva possibilità di poterci connettere all'interfaccia web della **Metasploitable** dal browser della **Kali**

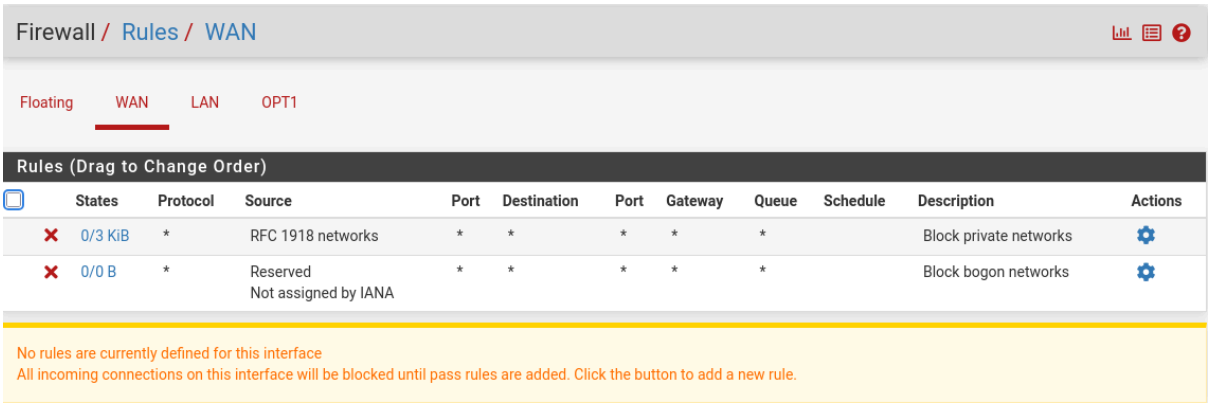




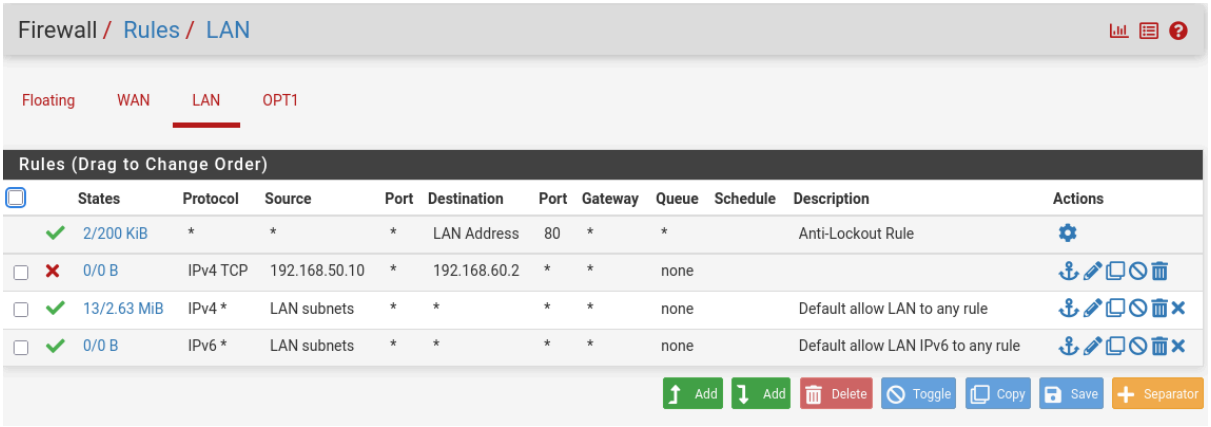
Creazione della Regola Firewall

Creazione delle regole firewall che bloccano l'accesso alla **DVWA** (su **Metasploitable**) dalla macchina **Kali** e ne impedisca lo scan.

Regole Firewall per WAN

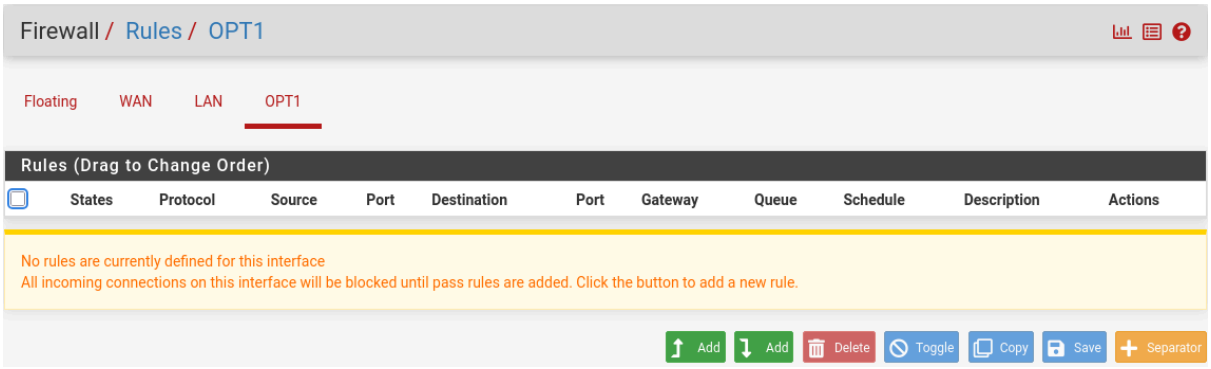


Regole Firewall per LAN



Regola impostata sul protocollo **TCP** per permettere il ping con la Metasploitable che è possibile grazie al protocollo **ICMP**.

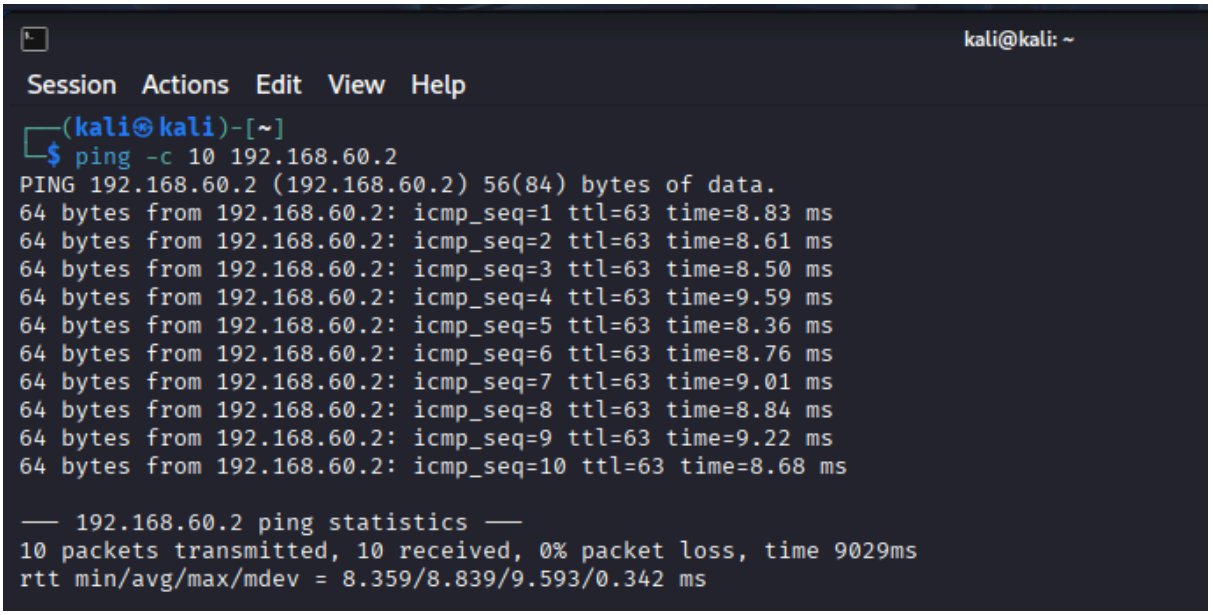
Regole Firewall per OPT1



Per questo specifico esercizio non è necessario configurare la tabella **OPT1**.

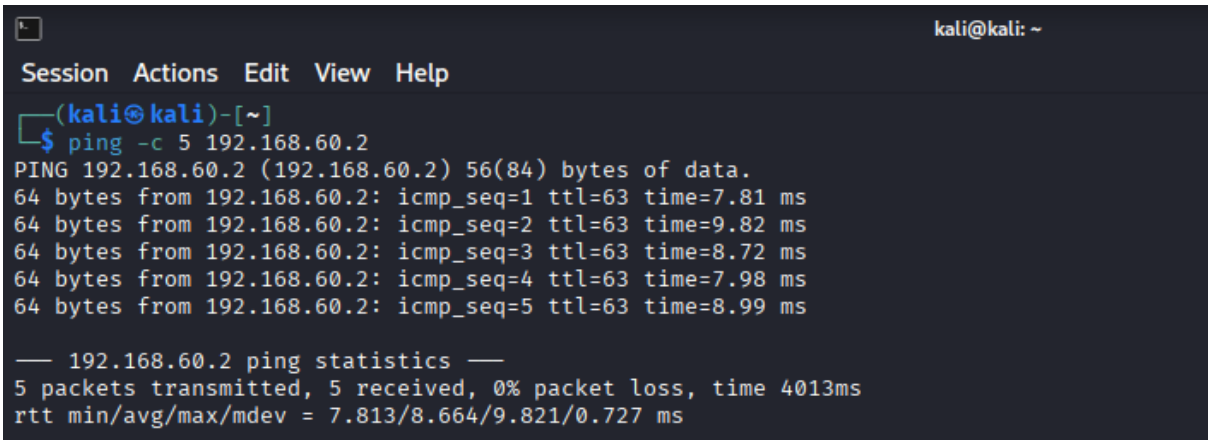
PING dalla Kali Linux alla Metasploitable prima dell'attivazione della regola di Firewall.

Ping funziona



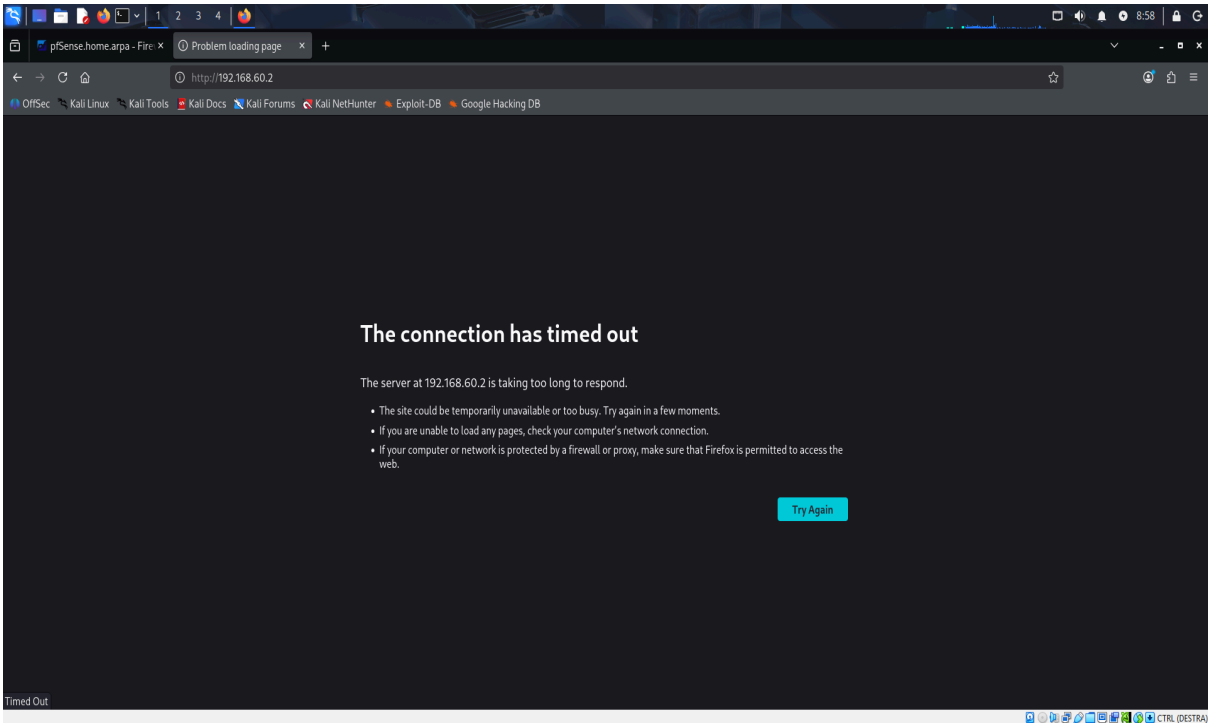
PING dalla Kali Linux alla Metasploitable dopo aver attivato la regola di Firewall

Ping funziona



Il **ping** continua a funzionare perchè abbiamo configurato la regola del **Firewall** specificatamente per il protocollo **TCP**. Quindi la **Kali** potrà effettuare il **ping** sia prima che dopo l'applicazione della regola**.**

Collegamento interfaccia web della Metasploitable da browser della Kali dopo aver inserito la regola di Firewall



In questo caso la connessione all'interfaccia web della Metasploitable fallisce.