

Report Configurazione PfSense

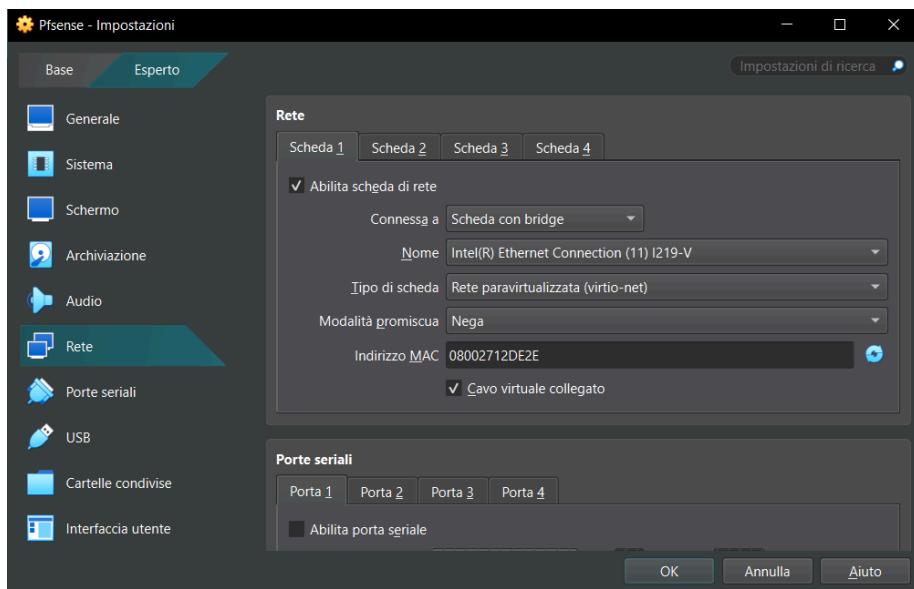
Obiettivo :

Creare 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.

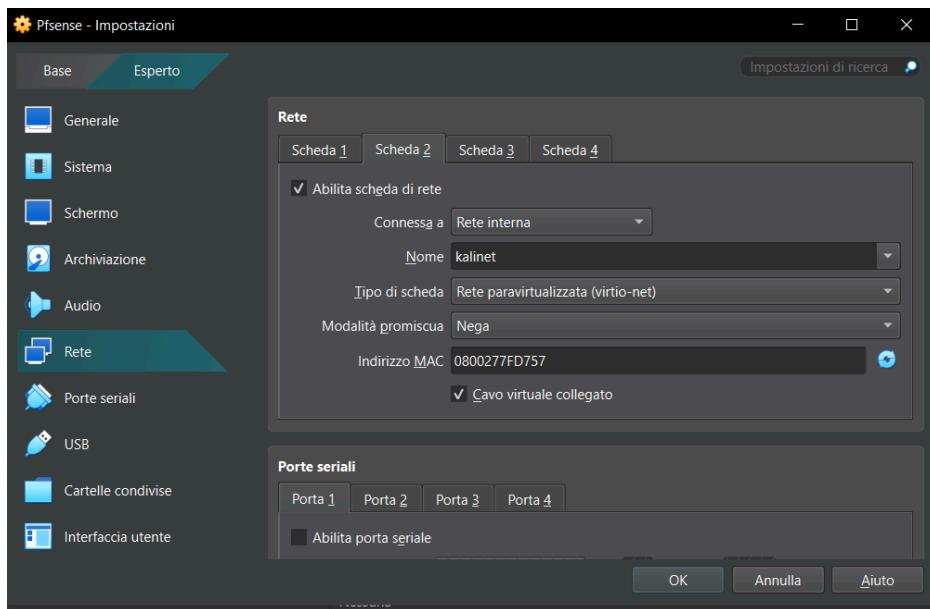
Configurazioni

Come prima cosa ho configurato sulle impostazioni di Virtualbox le tre schede di rete della PFsense

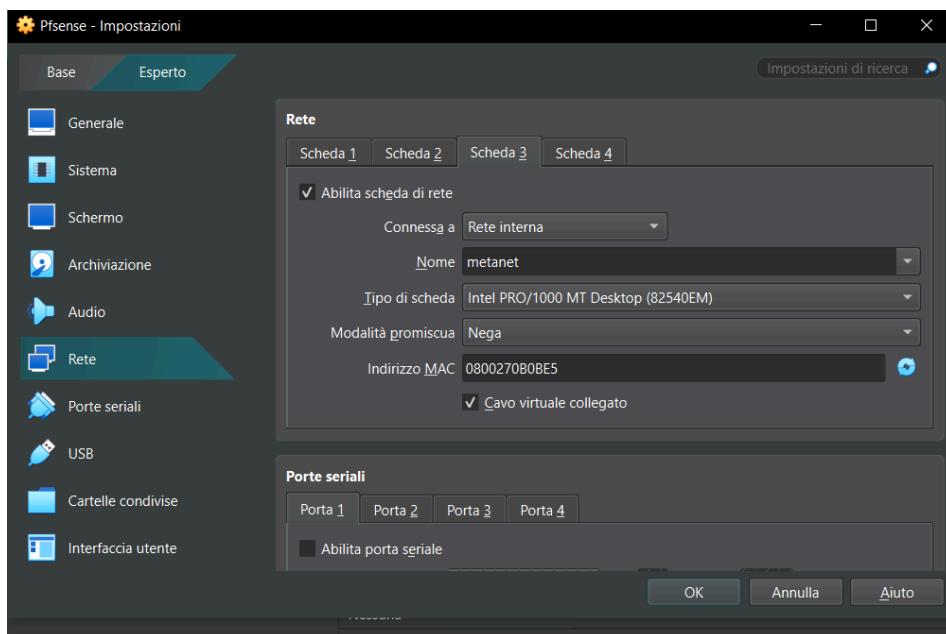
Prima scheda di rete :



Seconda scheda di rete :



Terza scheda di rete :



Da notare come la prima scheda di rete sia impostata su **Scheda con Bridge** per permettere il collegamento verso l'esterno; mentre le altre 2 siano impostate su rete interna.

La seconda scheda di rete è impostata su **rete interna** e sullo switch "**kalinet**" mentre la terza scheda di rete è impostata su **rete interna** ma sullo switch "**metanet**", ciò fa sì che le due macchine siano su reti differenti e non sulla stessa rete.

Una volta settate le schede di rete ho settato le varie impostazioni della Pfsense, prima da interfaccia web **aggiungendo la OPT1** e poi tramite terminale mettendo le varie impostazioni.

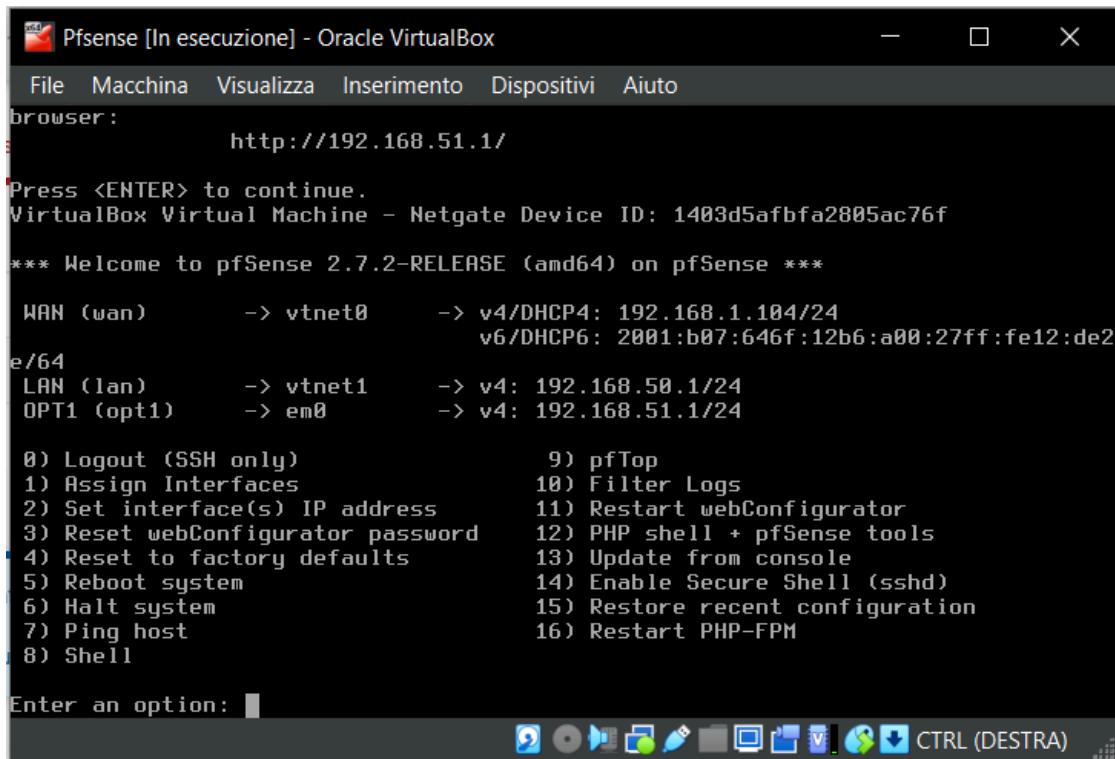
- **IpV4** : 192.168.51.1 Indirizzo Gateway
- **Range Minimo** : 192.168.51.10
- **Range Massimo** : 192.168.51.100
- **Disattivo e non impostato l'Ipv6**
- **Attivo il DHCP non manualmente ma in maniera automatica**

Così da avere impostato la rete WAN / LAN / Opt 1

Interfaccia Web con creazione OPT1:

The screenshot shows the Pfsense web interface under the 'Interfaces / Interface Assignments' tab. A warning message at the top states: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below this, the 'Interface Assignments' tab is selected. A table lists three interfaces: WAN (assigned to vtne0), LAN (assigned to vtne1), and OPT1 (assigned to em0). Each row has a 'Delete' button. At the bottom left is a 'Save' button. A note at the bottom says: "Interfaces that are configured as members of a lagg(4) interface will not be shown. Wireless interfaces must be created on the Wireless tab before they can be assigned."

Terminale PfSense con conferma delle impostazioni:



```
Pfsense [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
browser:
http://192.168.51.1/

Press <ENTER> to continue.
VirtualBox Virtual Machine - Netgate Device ID: 1403d5afbf2805ac76f

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> vtnet0      -> v4/DHCP4: 192.168.1.104/24
                      v6/DHCP6: 2001:b07:646f:12b6:a00:27ff:fe12:de2
e/64
LAN (lan)      -> vtnet1      -> v4: 192.168.50.1/24
OPT1 (opt1)    -> em0        -> v4: 192.168.51.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults   13) Update from console
5) Reboot system               14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: ■
```

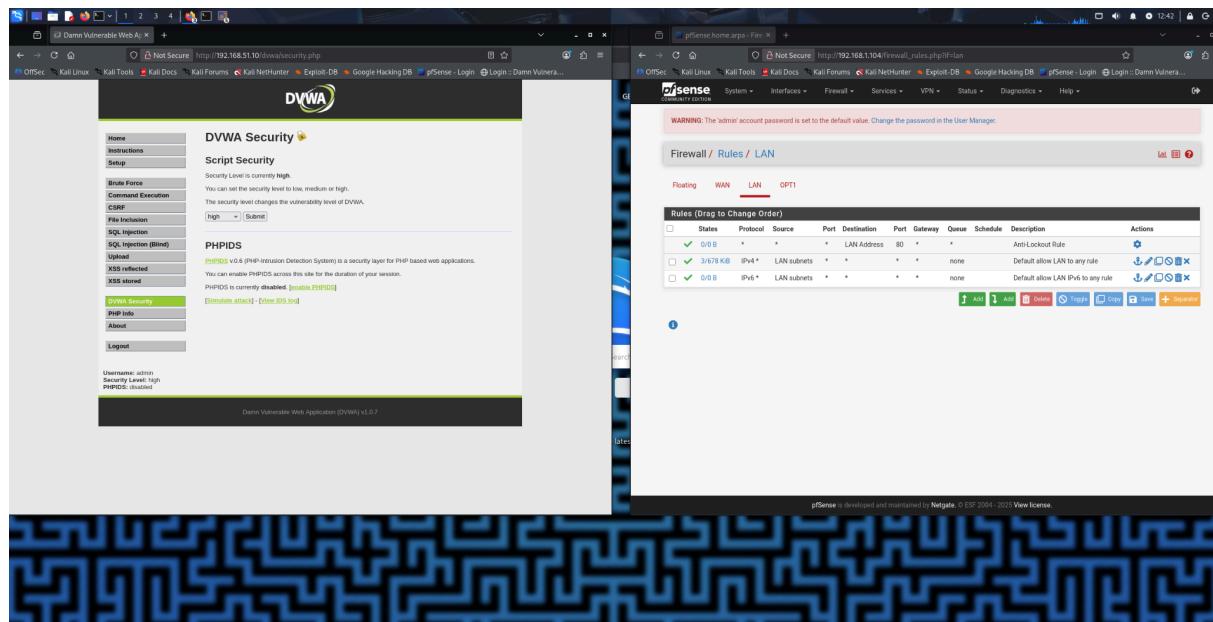
Avvio la Metasploitable con l'ip per collegarmi :

```
* debian-helper-scripts
* sysvconfig
try: sudo apt-get install <selected package>
-bash: service: command not found
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:6b:7d:f2
          inet addr:192.168.51.10  Bcast:192.168.51.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe6b:7df2/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
            RX packets:7 errors:0 dropped:0 overruns:0 frame:0
            TX packets:58 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:1296 (1.2 KB)  TX bytes:6668 (6.5 KB)
            Base address:0xd020 Memory:f0200000-f0220000

lo       Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
            UP LOOPBACK RUNNING  MTU:16436  Metric:1
            RX packets:113 errors:0 dropped:0 overruns:0 frame:0
            TX packets:113 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:29705 (29.0 KB)  TX bytes:29705 (29.0 KB)

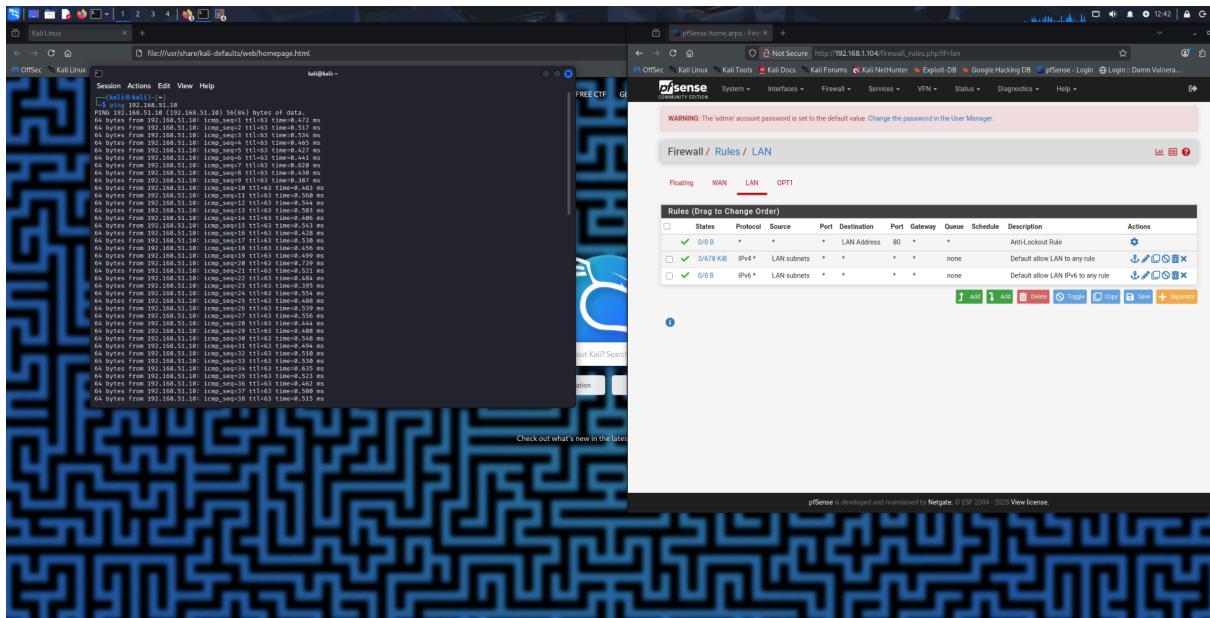
msfadmin@metasploitable:~$ _
```

L'ip sarà **192.168.51.10** con il quale dal Browser della kali cercherò di collegarmi riuscendo ad arrivare alla pagina Login di DVWA per poi una volta fatto il login accedere alle varie impostazioni del Database.



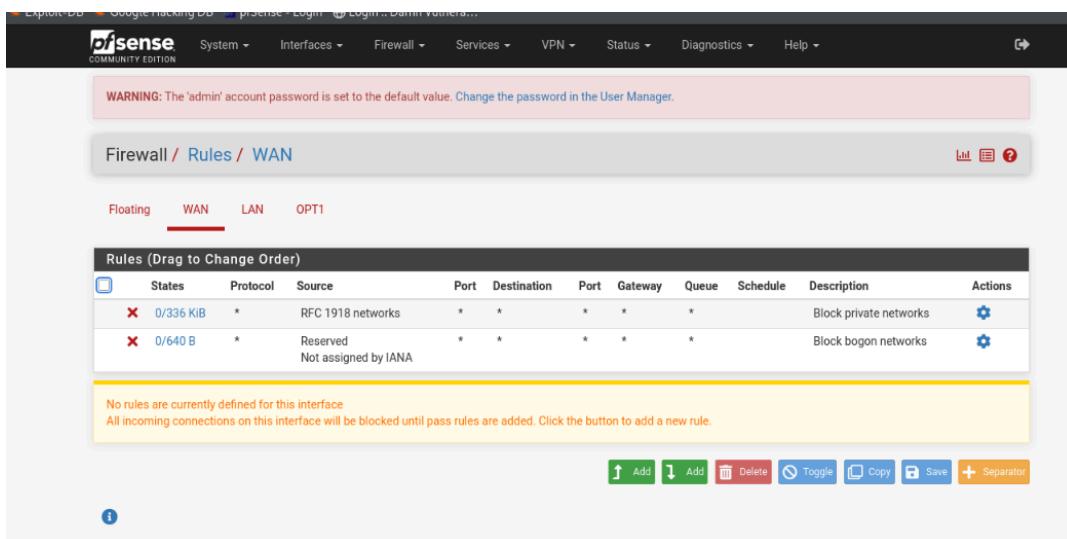
Come si può vedere dallo screen senza regole aggiuntive nella LAN il sito è **comodamente raggiungibile**.

Inoltre per maggiore controllo decido di fare un tentativo cercando di **pingare dalla Kali alla Metasploitable avente esito positivo**.



Dallo screen si può notare come senza regole aggiuntive il ping **sia possibile e dia esito positivo**.

In allegato i 3 screen (WAN , LAN , OPT1) con relative regole, compresa la regola aggiunta nella LAN che andrà a vietare ogni tipo di accesso verso la Metasploitable.



WZCNSC COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Firewall / Rules / LAN

Floating WAN LAN OPT1

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0/0 B	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	X 0/2 KIB	IPv4 TCP	192.168.50.151	*	192.168.51.10	80 (HTTP)	*	none			
<input type="checkbox"/>	✓ 1/5.74 MIB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>	✓ 0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Add Add Delete Toggle Copy Save Separator

pfSense COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Firewall / Rules / OPT1

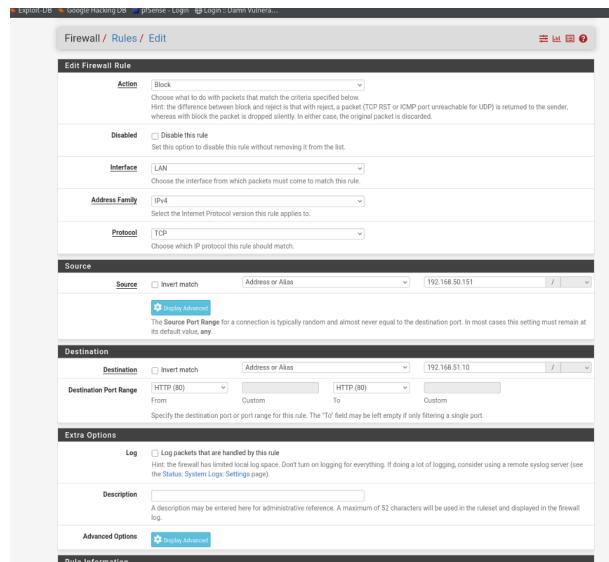
Floating WAN LAN OPT1

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
No rules are currently defined for this interface All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.											

Add Add Delete Toggle Copy Save Separator

Successivamente ho infatti creato la regola richiesta, **che vada a bloccare ogni tipo di accesso verso la Metasploitable dalla macchina Kali**.

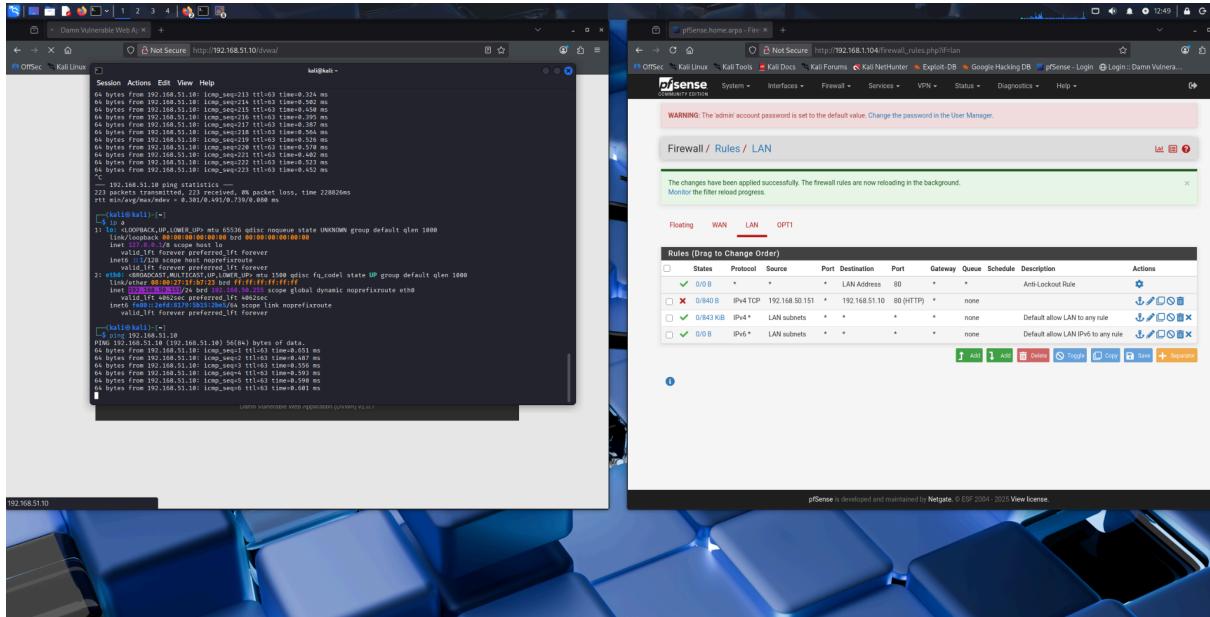


Con questa regola si va a **bloccare qualsiasi accesso dalla Kali (Source) con IP 192.168.50.151 alla Metasploitable (Destination) con IP 192.168.51.10 andando a bloccare anche la porta 80 (HTTP) su cui girano tutti i servizi riferiti al Web.**

Una volta salvata la regola e applicati i cambiamenti allego gli screen dei test effettuati che fanno vedere come l'accesso alla Meta venga bloccato ma continui comunque la possibilità di effettuare il ping.

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 0/2 B	*	*	*	LAN Address	80	*	*	*	Anti-Lockout Rule	
✗ 0/2 KB	IPv4 TCP	192.168.50.151	*	192.168.51.10	*	(HTTP)	*	*	none	
✓ 16/589 MB	IPv4 *	LAN subnets	*	*	*	*	*	*	Default allow LAN to any rule	
✓ 0/0 B	IPv6 *	LAN subnets	*	*	*	*	*	*	Default allow LAN IPv6 to any rule	

Come si può vedere dallo screen, grazie alla regola messa nella PfSense in Lan l'**accesso alla Meta viene bloccato**.



Come si vede dallo screen il ping continua a funzionare anche con la presenza della regola.

Descrizione dettagliata della regola creata:

- Action** : Block (Scarta il pacchetto silenziosamente).
- Interface**: LAN (Il punto di ingresso del traffico).
- Address Family**: IPv4.
- Protocol** : TCP cioè il protocollo usato per trasportare il pacchetto dal server web di DVW).
- Source** : Indirizzo IP della kali .
- Destination** : Indirizzo IP della Meta.
- Destination Port Range** : 80 (http) poichè tutti i server web viaggiano su quella determinata porta.

In conclusione :

La regola implementata impedisce lo sfruttamento delle vulnerabilità web di DVWA da parte della macchina Kali, senza compromettere la raggiungibilità della macchina Metasploitable per altre attività.