

venerdì 13 dicembre 2024

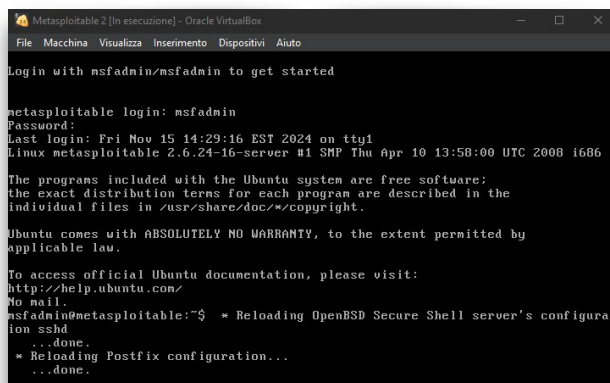
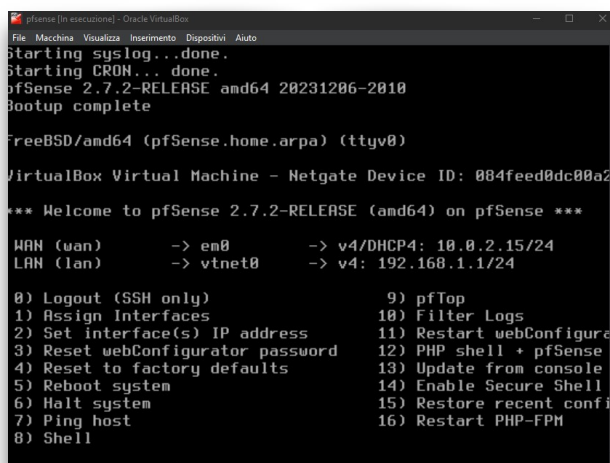
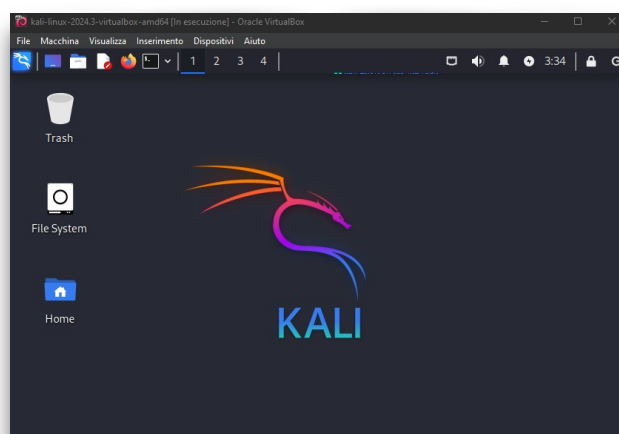
## PROGETTO S3/L5

Il progetto di questa settimana prevede la creazione di una policy con **Pfsense**.

Andremo quindi a creare una regola Firewall. In particolare la regola Firewall deve **bloccare l'accesso alla DVWA di Metasploitable** dalla macchina Kali Linux e ne deve impedire quindi lo Scan. Kali e Pfsense devono essere su reti diverse, quindi si aggiunge una nuova interfaccia di rete a Pfsense.

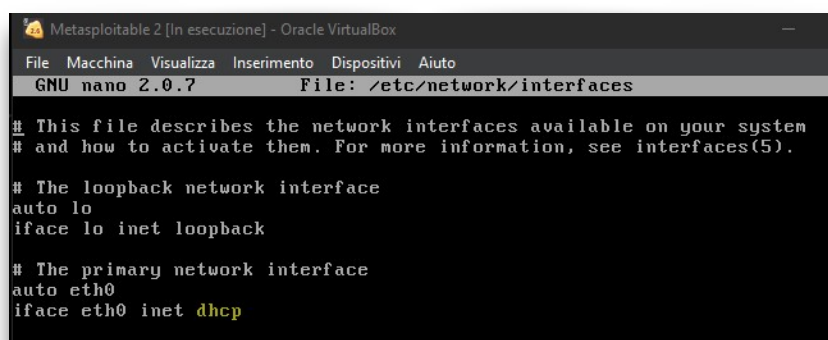
### 1. AVVIO DELLE MACCHINE KALI, Pfsense e METASPLOITABLE

- Tramite VirtualBox avvio le tre macchine in modo da potermi poi muovere velocemente:

A terminal window titled 'Metasploitable 2 [In esecuzione] - Oracle VM VirtualBox'. It shows the login process for 'msfadmin' with password 'msfadmin'. The system is Ubuntu 2.6.24-16-server. It displays the last login time and the system uptime. It also shows the Ubuntu warranty disclaimer and the official documentation URL. The terminal prompt is 'msfadmin@metasploitable:~\$'.A terminal window titled 'pfSense [In esecuzione] - Oracle VM VirtualBox'. It shows the bootup process of pfSense 2.7.2-RELEASE (amd64). It displays the system configuration, including the WAN (wan) and LAN (lan) interfaces. The terminal prompt is 'FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)'. It also shows the VirtualBox Virtual Machine - Netgate Device ID: 084feed0dc08a2. The terminal prompt is '\*\*\* Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense \*\*\*'.

## 2. MODIFICO LA RETE DI METASPLOITABLE

- Come da indicazioni, Metasploitable e Pfsense devono trovarsi su reti diverse, quindi vado a modificare la rete di Metasploitable attraverso il comando “**sudo nano /etc/network/interfaces**”:



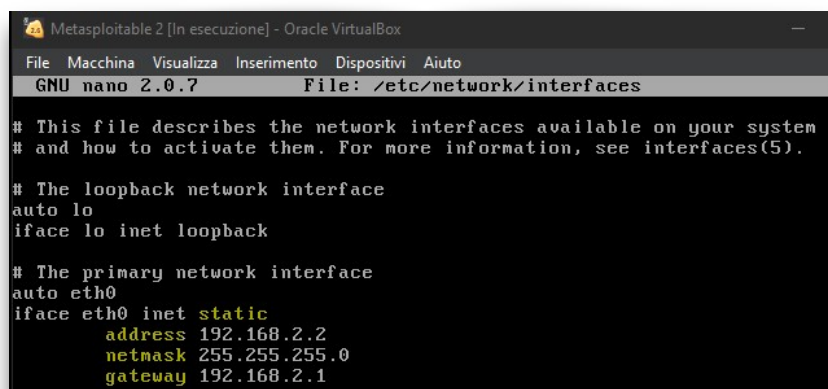
```
Metasploitable 2 [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
GNU nano 2.0.7 File: /etc/network/interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet dhcp
```

- È impostato su **dhcp**, significa che viene assegnato in automatico ma io voglio controllarlo quindi imposto su **static** e configuro a mio piacimento:



```
Metasploitable 2 [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
GNU nano 2.0.7 File: /etc/network/interfaces M

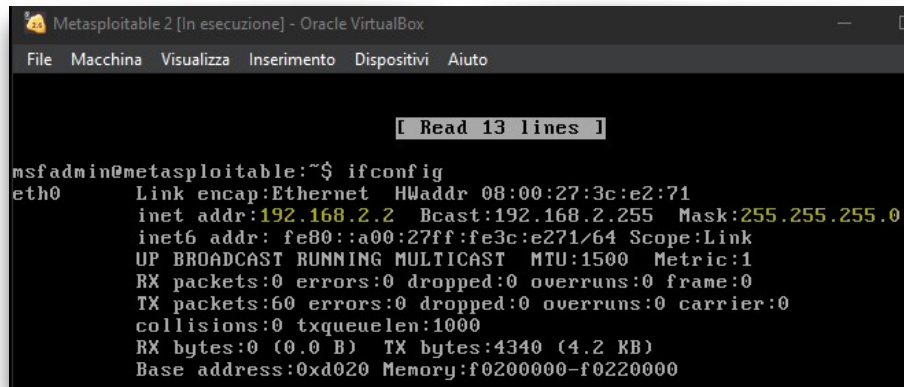
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
    address 192.168.2.2
    netmask 255.255.255.0
    gateway 192.168.2.1
```

- Ho impostato una sottorete diversa rispetto a kali che ha 192.168.1.0

- A questo punto riavvio metasploitable e verifico il cambiamento di rete:



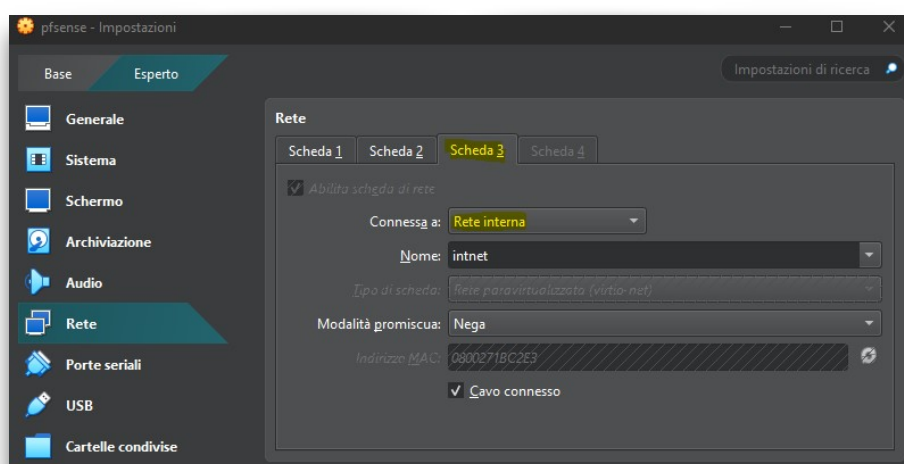
```

msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:3c:e2:71
          inet addr:192.168.2.2  Bcast:192.168.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe3c:e271/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:60 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:4340 (4.2 KB)
          Base address:0xd020  Memory:f0200000-f0220000
  
```

- Come si vede le impostazioni sono state salvate e ora metasploitable si trova in una sottorete diversa da quella di kali.

### 3. AGGIUNGO UN'INTERFACCIA A PfSense

- Dalle impostazioni di virtualbox aggiungo una **nuova scheda di rete a PfSense**:



- Dall'interfaccia web di Pfsense su kali **aggiungo la nuova interfaccia da assegnare a metasploitable**:

Interface	Network port
WAN	em0 (08:00:27:2d:53:25)
LAN	vtnet0 (08:00:27:96:49:83)
OPT1	vtnet1 (08:00:27:1b:c2:e3)

- Dopodiché **abilito l'interfaccia e la configuro**:

Interfaces / OPT1 (vtnet1)

### General Configuration

Enable ☒ **Enable interface**

Description   
Enter a description (name) for the interface here.

IPv4 Configuration Type **Static IPv4**

IPv6 Configuration Type **None**

MAC Address   
This field can be used to modify ("spoof") the MAC address of this interface.  
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.

MTU   
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

MSS   
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.

Speed and Duplex **Default (no preference, typically autoselect)**  
Explicitly set speed and duplex mode for this interface.  
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex

### Static IPv4 Configuration

IPv4 Address  /

## 4. TESTO LE CONNESSIONI

- Per testare le connessioni tra le macchine inizio eseguendo un comando di **ping** da Kali verso Pfsense:

```
(kali㉿kali)-[~]  
$ ping 192.168.1.1  
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.  
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=0.253 ms  
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=0.208 ms  
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=0.228 ms  
64 bytes from 192.168.1.1: icmp_seq=4 ttl=64 time=0.219 ms  
64 bytes from 192.168.1.1: icmp_seq=5 ttl=64 time=0.261 ms  
64 bytes from 192.168.1.1: icmp_seq=6 ttl=64 time=0.254 ms  
^C  
— 192.168.1.1 ping statistics —  
6 packets transmitted, 6 received, 0% packet loss, time 5113ms  
rtt min/avg/max/mdev = 0.208/0.237/0.261/0.019 ms
```

- Poi sempre da Kali eseguo un **ping** verso Metasploitable:

```
(kali㉿kali)-[~]  
$ ping 192.168.2.2  
PING 192.168.2.2 (192.168.2.2) 56(84) bytes of data.  
64 bytes from 192.168.2.2: icmp_seq=1 ttl=63 time=0.507 ms  
64 bytes from 192.168.2.2: icmp_seq=2 ttl=63 time=0.421 ms  
64 bytes from 192.168.2.2: icmp_seq=3 ttl=63 time=0.472 ms  
64 bytes from 192.168.2.2: icmp_seq=4 ttl=63 time=0.347 ms  
64 bytes from 192.168.2.2: icmp_seq=5 ttl=63 time=0.367 ms  
64 bytes from 192.168.2.2: icmp_seq=6 ttl=63 time=0.444 ms  
^C  
— 192.168.2.2 ping statistics —  
6 packets transmitted, 6 received, 0% packet loss, time 5104ms  
rtt min/avg/max/mdev = 0.347/0.426/0.507/0.055 ms
```

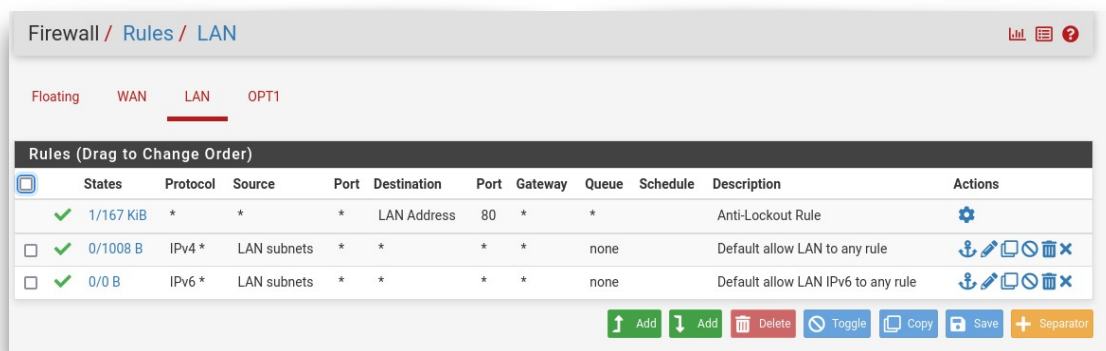
- Infine da metasploitable eseguo un **ping** verso Kali e poi verso Pfsense:

```
msfadmin@metasploitable:~$ ping 192.168.1.5  
PING 192.168.1.5 (192.168.1.5) 56(84) bytes of data.  
  
--- 192.168.1.5 ping statistics ---  
4 packets transmitted, 0 received, 100% packet loss, time 3006ms  
  
msfadmin@metasploitable:~$ ping 192.168.1.1  
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.  
  
--- 192.168.1.1 ping statistics ---  
43 packets transmitted, 0 received, 100% packet loss, time 42006ms
```

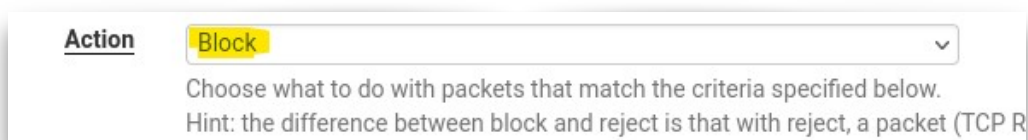
- Le connessioni funzionano correttamente!

## 5. CREAZIONE REGOLA FIREWALL

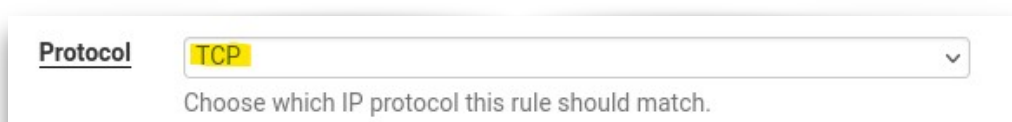
- Ora che ho configurato correttamente la rete devo **bloccare l'accesso alla DVWA di Metasploitable** da Kali.
- Per farlo, sempre dall'interfaccia web di Pfsense, apro le regole del firewall e seleziono la porta LAN, dove Kali si collega:



- Aggiungo una nuova regola in cima alla lista perché la regola di blocco deve venire necessariamente prima delle altre di accettazione, e inizio a configurarla.
- Su **action** seleziono **Block**, perché voglio bloccare una specifica connessione:



- Come protocollo seleziono **TCP**, perché DVWA è una applicazione web, e **HTTP** utilizza il protocollo **TCP**:



- Alla sorgente indico la voce **Address or Alias** in modo da specificare l'indirizzo IP sorgente della richiesta:

Source configuration panel showing the 'Source' dropdown set to 'Address or Alias' and the 'Address or Alias' field containing '192.168.1.5'.

- Alla destinazione indico invece l'**IP di metasploitable** e come porta inserisco **80** dato che voglio bloccare l'accesso alla DVWA (applicazione web):

Destination configuration panel showing the 'Destination' dropdown set to 'Address or Alias' and the 'Address or Alias' field containing '192.168.2.2'. The 'Destination Port Range' is set to 'HTTP (80)' with 'From' and 'To' fields both containing '80'.

- Infine salvo e applico le modifiche:

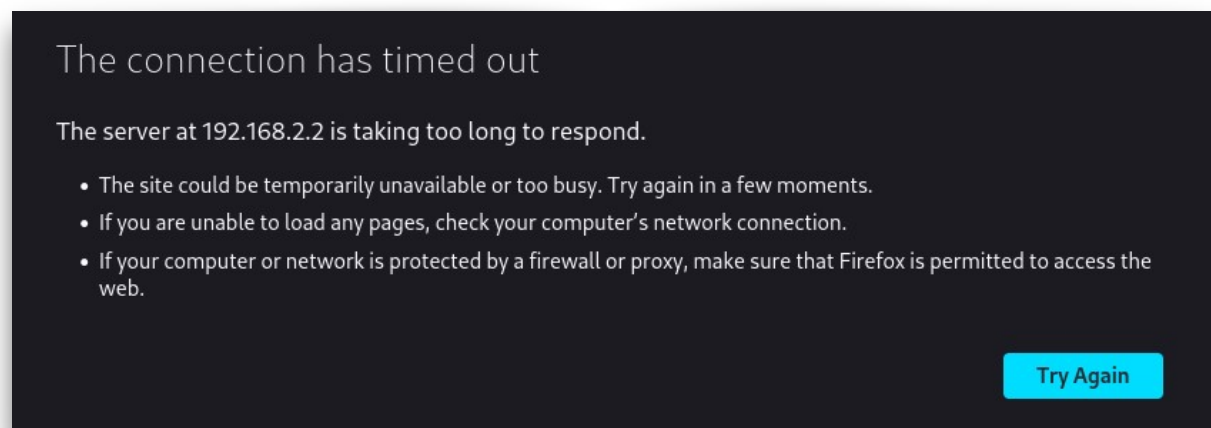
Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	✓ 1/217 KiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	✗ 0/0 B	IPv4 TCP	192.168.1.5	*	192.168.2.2	80 (HTTP)	*	none			
<input type="checkbox"/>	✓ 0/1008 B	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	

- Come si vede la regola è stata aggiunta in cima alla lista.



## 6. VERIFICA DELLA REGOLA

- Per verificare che la regola applicata funzioni correttamente possiamo fare diverse cose:
- Cerco **192.168.2.2** sul web:



- Come si vede il server non risponde quindi la richiesta viene definita **“timed out”**.
- Oltre a questo possiamo eseguire un comando **“nmap”** da Kali per scansionare le porte di Metasploitable e vedere cosa succede con la **porta 80**:

```
(kali@kali)-[~]
$ nmap 192.168.2.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-13 07:22 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
th --dns-servers
Nmap scan report for 192.168.2.2
Host is up (0.021s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    filtered http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 1.32 seconds
```



- Come si vede la porta **80** ci da stato **“filtered”**, significa che la regola del firewall funziona perfettamente!

## 7. CONCLUSIONE

- Abbiamo visto come configurare una rete funzionante tra le varie macchine e che facesse in modo che la comunicazione passasse per pfsense. Abbiamo configurato pfsense e aggiunto una regola al firewall che andasse a bloccare una determinata e specifica comunicazione tra kali e metasploitable senza interferire con il resto del traffico.
- Saper applicare le regole del firewall può all'inizio sembrare difficile, ma una volta capito il senso di ogni singolo parametro diventa fluido e intuitivo.

## Esercizio bonus

## Impostare una regola su Pfsense per bloccare da Kali il telnet verso Metasploitable.

## 1.1 TEST DELLA COMUNICAZIONE

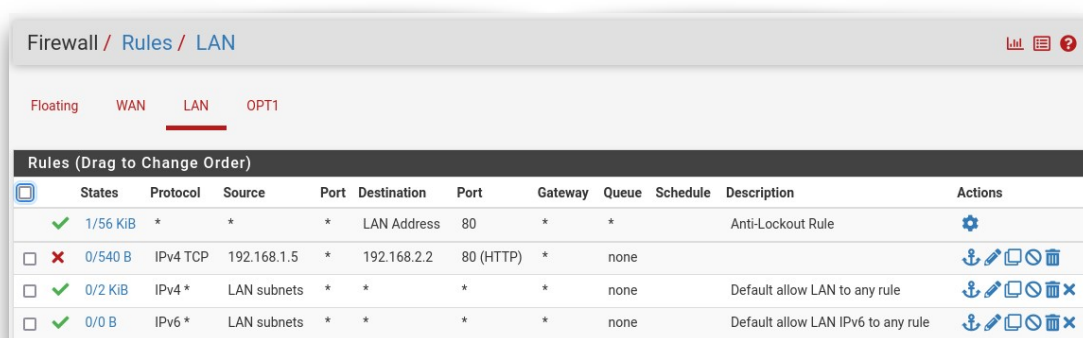
- Prima di impostare la regola su Pfsense, verifico che la connessione con **telnet** verso Metasploitable sia possibile, attraverso il comando **“telnet 192.168.2.2 23”**, dove 23 indica la porta telnet (vedi punto 6):

```
kali@kali: ~  
File Actions Edit View Help  
zsh: corrupt history file /home/kali/.zsh_history  
[kali@kali]~]  
$ telnet 192.168.2.2 23  
Trying 192.168.2.2 ...  
Connected to 192.168.2.2.  
Escape character is '^['.  
  
Warning: Never expose this VM to an untrusted network!  
Contact: msfdev[at]metasploit.com  
Login with msfadmin/msfadmin to get started  
  
metasploitable login: 
```

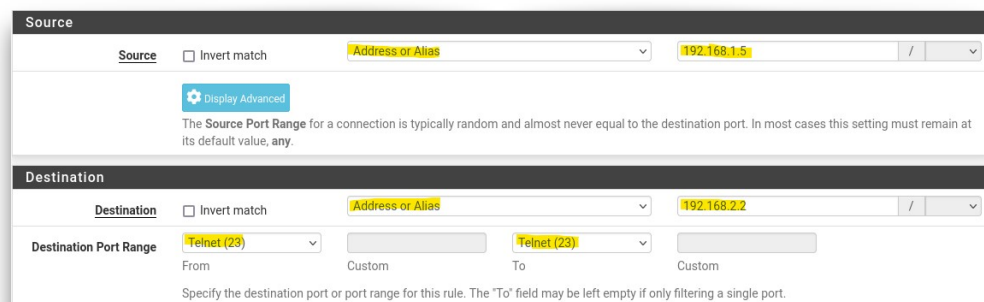
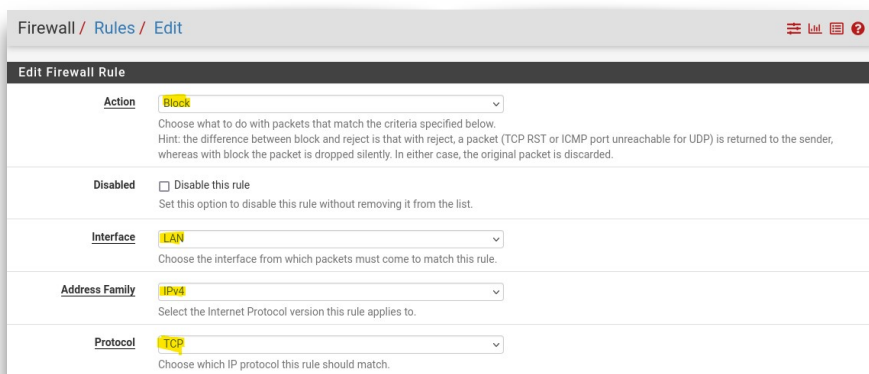
- Come si vede la connessione è possibile.

## 1.2 CONFIGURAZIONE DELLA REGOLA

- Come prima vado nella sezione **Rules** del **Firewall** da Kali:



- Aggiungo una regola sempre **in cima alla lista** e la configuro come segue:



- Ora salvo e applico:

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	✓ 1/106 KiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	✗ 0/0 B	IPv4 TCP	192.168.1.5	*	192.168.2.2	23 (Telnet)	*	none			
<input type="checkbox"/>	✗ 0/540 B	IPv4 TCP	192.168.1.5	*	192.168.2.2	80 (HTTP)	*	none			
<input type="checkbox"/>	✓ 0/2 KiB	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	

### 1.3 VERIFICA DELLA REGOLA

- Per verificare se la regola è stata appresa provo ad eseguire di nuovo il comando di prima:

```
(kali@kali)-[~]
$ telnet 192.168.2.2 23
Trying 192.168.2.2 ...
telnet: Unable to connect to remote host: Connection timed out
```

- La connessione non va a buon fine il che ci suggerisce di aver impostato correttamente la regola.
- Faccio un'ulteriore verifica attraverso “nmap”:

- Risultano chiuse le porte **80** dell'esercizio precedente e la **23**, quindi le regole sono state applicate correttamente!

```
(kali@kali)-[~]
$ nmap 192.168.2.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-13 09:37 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
--dns-servers
Nmap scan report for 192.168.2.2
Host is up (0.013s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE      SERVICE
21/tcp    open       ftp
22/tcp    open       ssh
23/tcp    filtered  telnet
25/tcp    open       smtp
53/tcp    open       domain
80/tcp    filtered  http
111/tcp   open       rpcbind
139/tcp   open       netbios-ssn
445/tcp   open       microsoft-ds
512/tcp   open       exec
513/tcp   open       login
514/tcp   open       shell
1099/tcp  open       rmiregistry
1524/tcp  open       ingreslock
2049/tcp  open       nfs
2121/tcp  open       ccproxy-ftp
3306/tcp  open       mysql
5432/tcp  open       postgresql
5900/tcp  open       vnc
6000/tcp  open       X11
6667/tcp  open       irc
8009/tcp  open       ajp13
8180/tcp  open       unknown

Nmap done: 1 IP address (1 host up) scanned in 1.36 seconds
```