



Progetto S3/L5

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.


Ho impostato le schede di rete di kali, pfsense e metasploitable in questo modo:

 **Rete**
Scheda 1: Intel PRO/1000 MT Desktop (Rete interna, 'intnet')

kali

 **Rete**
Scheda 1: Intel PRO/1000 T Server (NAT)
Scheda 2: Rete paravirtualizzata (Rete interna, 'intnet')
Scheda 3: Rete paravirtualizzata (Rete interna, 'intnet')

pfsens

 **Rete**
Scheda 1: Intel PRO/1000 MT Desktop (Rete interna, 'intnet')

metasploitable

Sono andato a controllare l'indirizzo ip di metasploitable

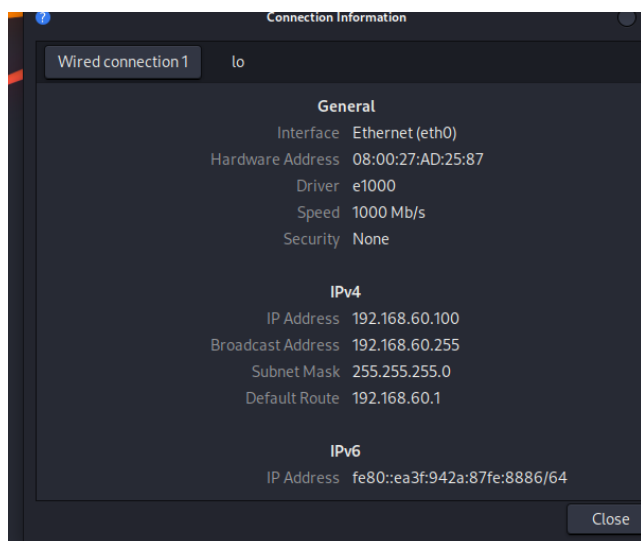
```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:6d:84:56
          inet addr:192.168.50.155  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe6d:8456/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:21 errors:0 dropped:0 overruns:0 frame:0
          TX packets:48 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1344 (1.3 KB)  TX bytes:3836 (3.7 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:104 errors:0 dropped:0 overruns:0 frame:0
          TX packets:104 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:20581 (20.0 KB)  TX bytes:20581 (20.0 KB)

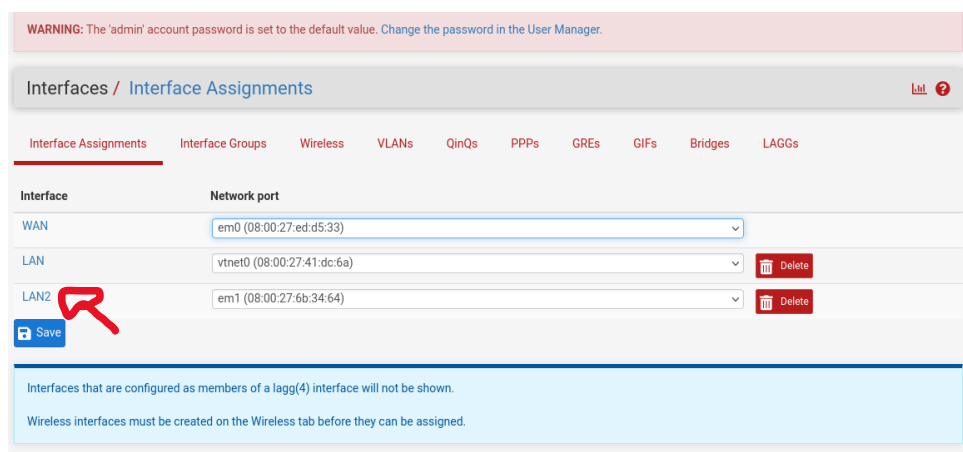
msfadmin@metasploitable:~$
```

Poi sono andato a modificare l'indirizzo IP di kali in modo che potesse comunicare con pfsense (192.168.60.5)

Ho scelto l'indirizzo 192.168.60.100 per kali



Una volta fatto questo ho aperto la gui di pfsense tramite kali, mettendo l'indirizzo IP di pfsense nel browser in kali, sono entrato dentro e sono andato a configurare la nuova interfaccia di rete per metasploitable.



l'ho chiamata LAN2

Interfaces / LAN2 (em1)

General Configuration

Enable ☒ Enable interface

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

IPv4 Configuration Type

IPv6 Configuration Type

MAC Address
This field can be used to modify ("spoof") the MAC address of this interface.
Enter a MAC address in the following format: xxxxxxxx:xxxx:xxxx 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) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.

Speed and Duplex
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 forced.

Static IPv4 Configuration

IPv4 Address /

IPv4 Upstream gateway [+ Add a new gateway](#)
If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.
On local area network interfaces the upstream gateway should be "none".
Selecting an upstream gateway causes the firewall to treat this interface as a WAN type interface.
Gateways can be managed by [clicking here](#).

Reserved Networks

Fatto questo sono andato a controllare in pfSense se fosse andato a buon fine

```

1 - WAN (em0 - dhcp)
2 - LAN (vtnet0 - static)
3 - LAN2 (em1 - static)

Enter the number of the interface you wish to configure: esc
VirtualBox Virtual Machine - Netgate Device ID: fde7a180875782b169a7

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

WAN (wan)      -> em0      -> v4/DHCP4: 10.0.2.15/24
LAN (lan)      -> vtnet0   -> v4: 192.168.60.5/24
LAN2 (opt1)    -> em1      -> v4: 192.168.50.155/24

0) Logout (SSH only)
1) Assign Interfaces
2) Set interface(s) IP address
3) Reset webConfigurator password
4) Reset to factory defaults
5) Reboot system
6) Halt system
7) Ping host
8) Shell

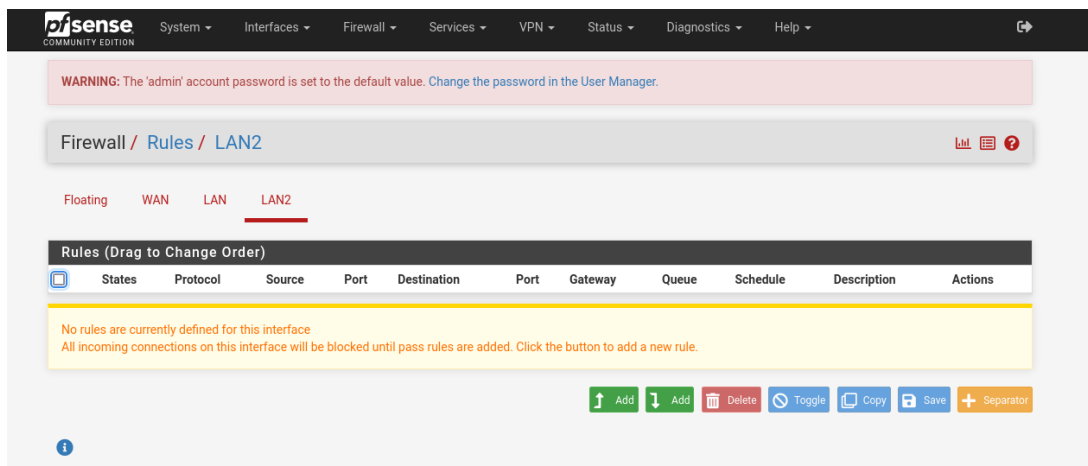
9) pfTop
10) Filter Logs
11) Restart webConfigurator
12) PHP shell + pfSense tools
13) Update from console
14) Enable Secure Shell (sshd)
15) Restore recent configuration
16) Restart PHP-FPM

Enter an option:

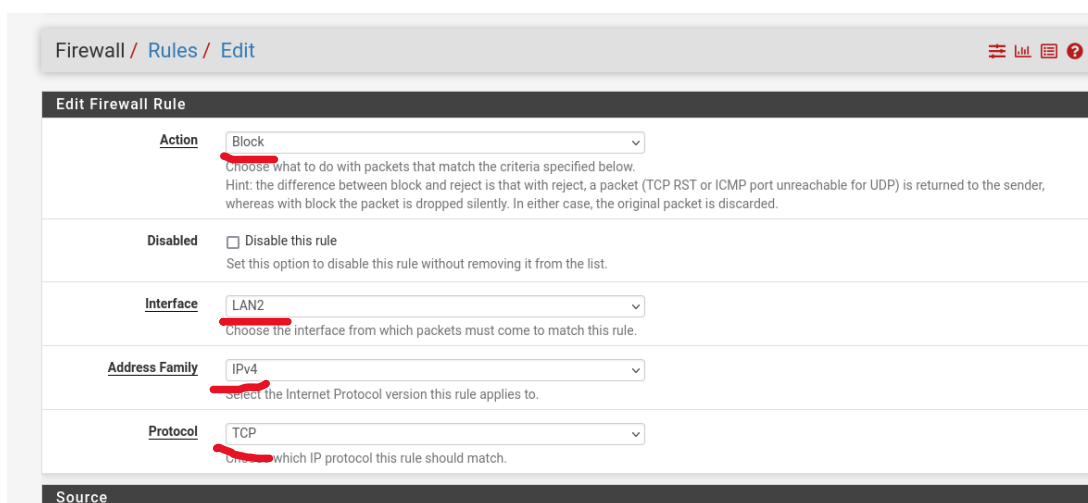
```

Sono ritornato nella gui di pfSense e ho cominciato ad impostare le regole per il firewall

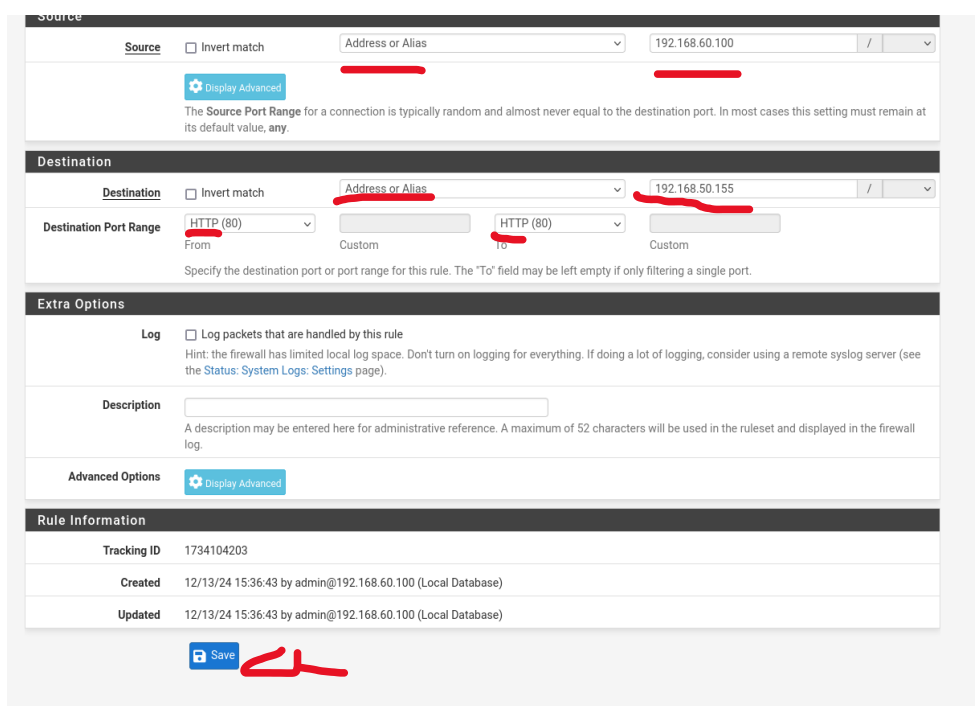
Firewall---->rules---->LAN2



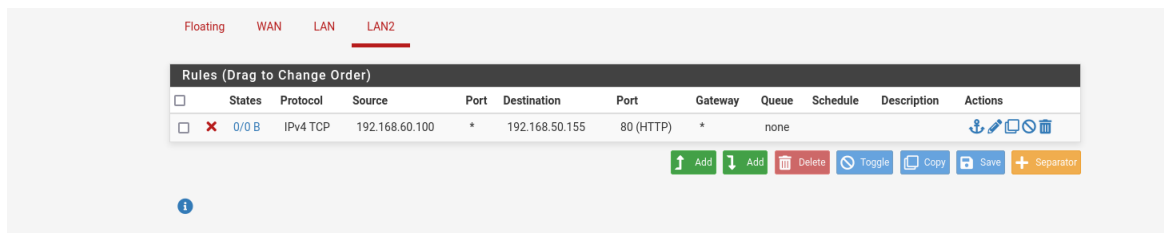
Clicchiamo su add e configuriamo la regola:



Come azione mettiamo block, interfaccia sarà quella di LAN2 e come address famiglia ipv4, infine, mettiamo il protocollo TCP poichè è il protocollo progettato per l'invio dei pacchetti.



Proseguiamo e mettiamo l'indirizzo source che sarà quello di kali e l'indirizzo di destinazione che sarà quello di metasploitable. Scegliamo la porta 80 che appartiene al protocollo HTTP e salviamo.



Questa è la regola.

Purtroppo, mi sono fermato qui, non sono riuscito a verificare che la regola di blocco funzioni, non ho abbastanza tempo per continuare a fare prove e venire a capo del problema, purtroppo ho perso tantissimo tempo questa mattina con la macchina metasploitable (sono il ragazzo che l'ha tartassata su discord, mi scusi).

Mi scusi anche per la pochezza del report, sono stato fino alla fine a cercare di capire se la regola di blocco abbia funzionato e gli ultimi 15mn mi sono dedicato al report.