

## Progetto S3L5

### Esercizio:

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.

### Step1:

Dalle impostazioni della **macchina virtuale** su **Router Pfsense** collego **Pfsense** alla mia rete e successivamente creo **2 Reti locali** distinte: **kalinet** e **metanet**.

La rete **kalinet** è la rete di **Kali-linux** e **metanet** di **Metasploitable2**

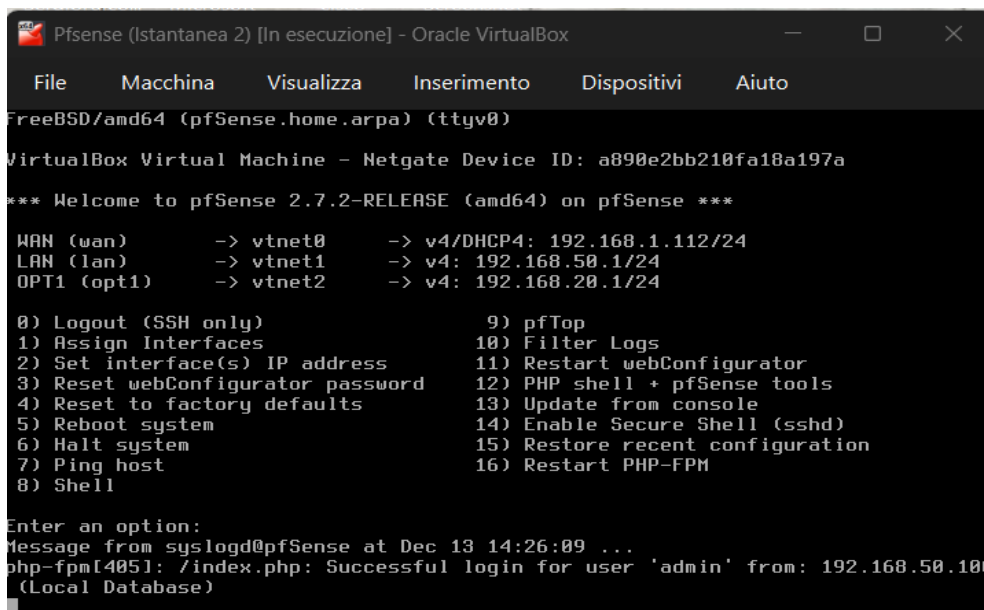
### Step2:

Avvio **Pfsense** e imposto manualmente le reti.

WAN assegnato alla rete

**LAN** di **Kali-linux** con **Ip192.168.50.1**

**OPT1** di **Metasploitable2** con **Ip192.168.20.20**



```
Pfsense (Istantanea 2) [In esecuzione] - Oracle VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)
VirtualBox Virtual Machine - Netgate Device ID: a890e2bb210fa18a197a
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

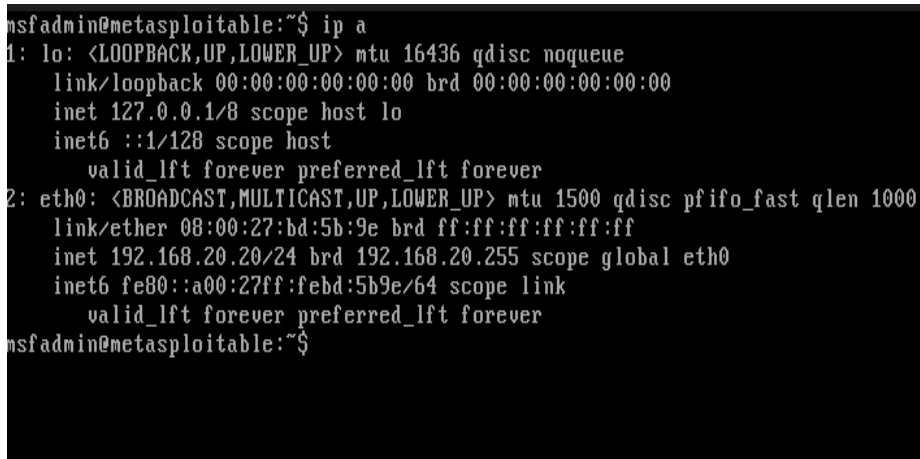
WAN (wan)      -> vtnet0      -> v4/DHCP4: 192.168.1.112/24
LAN (lan)      -> vtnet1      -> v4: 192.168.50.1/24
OPT1 (opt1)    -> vtnet2      -> v4: 192.168.20.1/24

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:
Message from syslogd@pfSense at Dec 13 14:26:09 ...
php-fpm[4051]: /index.php: Successful login for user 'admin' from: 192.168.50.10
(Local Database)
```

### Step3:

Imposto rete su **Metasploitable2**



```
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:bd:5b:9e brd ff:ff:ff:ff:ff:ff
    inet 192.168.20.20/24 brd 192.168.20.255 scope global eth0
    inet6 fe80::a00:27ff:febd:5b9e/64 scope link
        valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$
```

Con queste impostazioni “**kalinet**” ha **accesso** a “**metanet**” poiché stanno utilizzando lo stesso **Router PfSense**.

#### Step4:

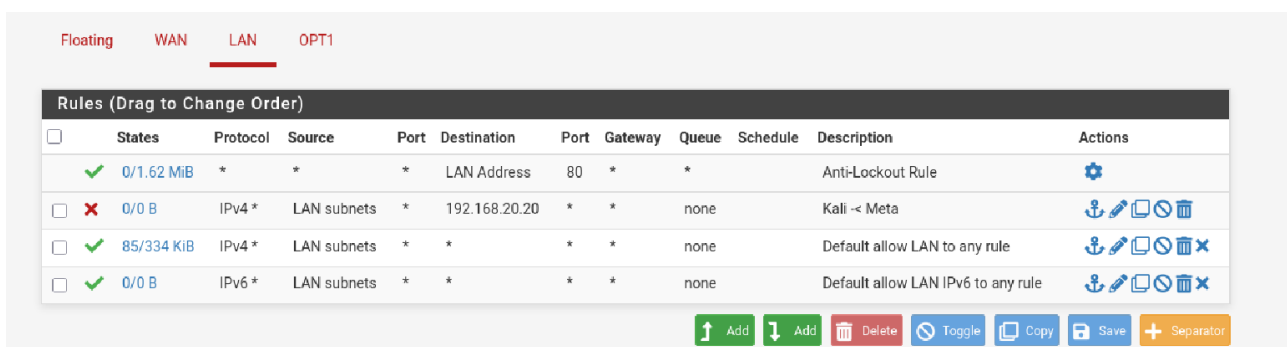
Testo attraverso il comando **ping** dal **Terminale** di **Kali-Linux**, richiamando **Metasploitable2** col suo Ip **192.168.20.20**

```
Session Actions Edit View Help
(kali㉿kali)-[~]
$ ping 192.168.20.20
PING 192.168.20.20 (192.168.20.20) 56(84) bytes of data.
64 bytes from 192.168.20.20: icmp_seq=1 ttl=63 time=9.80 ms
64 bytes from 192.168.20.20: icmp_seq=2 ttl=63 time=1.04 ms
64 bytes from 192.168.20.20: icmp_seq=3 ttl=63 time=1.47 ms
^C
— 192.168.20.20 ping statistics —
3 packets transmitted, 3 received, 0% packet loss, time 2033ms
rtt min/avg/max/mdev = 1.036/4.102/9.797/4.030 ms
(kali㉿kali)-[~]
$
```

#### Step5:

Dal **Browser** visito **192.168.50.1** per cambiare le impostazioni **Firewall** di **PfSense** e per bloccare l’accesso alla **rete metanet** da **kalinet**.

Vado su **Firewall/Rules/** e aggiungo **una regola che blocchi metanet** per Kali-Linux e **kalinet** per **OPT1 (Metasploitable2)** specificando i rispettivi Ip.



Attraverso queste regole **sul Firewall** di **PfSense**, nonostante le due reti siano sullo stesso **Router**, **blocco l’accesso** e quindi la loro comunicazione.

### Step6:

Dal Terminale attraverso il comando **ping** provo a comunicare con **Metasploitable2** per testare che la regola sia stata efficace.

```
(kali㉿kali)-[~]  
$ ping 192.168.20.20  
PING 192.168.20.20 (192.168.20.20) 56(84) bytes of data.  
^C  
— 192.168.20.20 ping statistics —  
9 packets transmitted, 0 received, 100% packet loss, time 8213ms  
  
(kali㉿kali)-[~]  
$
```