

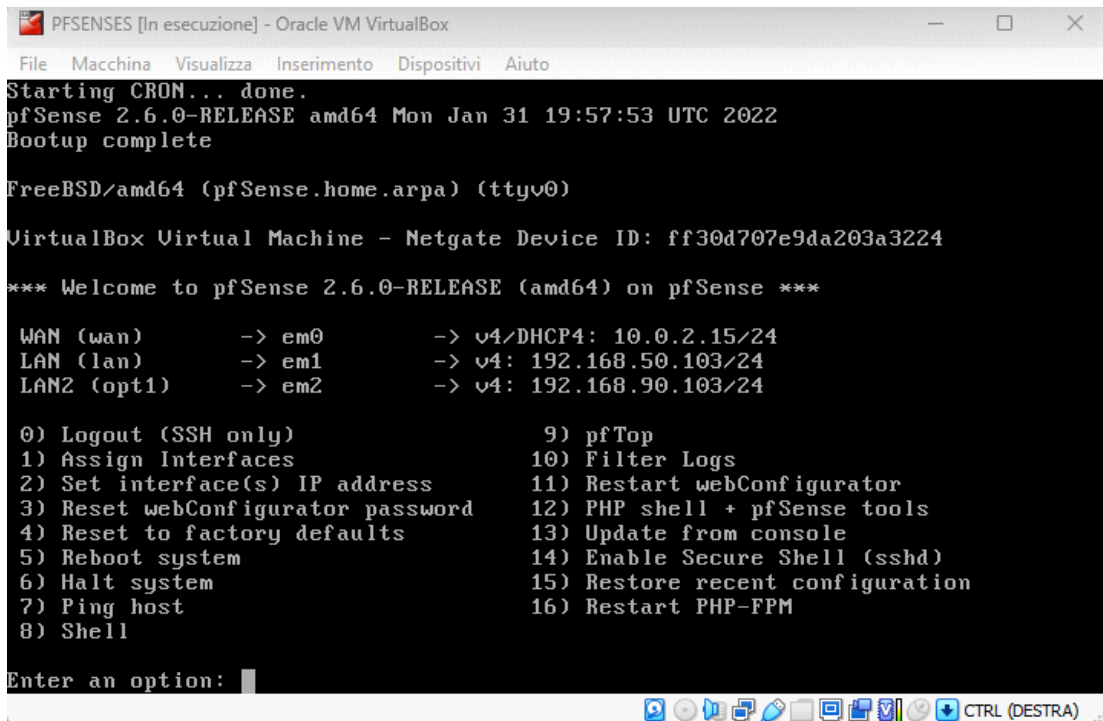
PFSENSE BLOCCO SERVIZI PORTA 80 SU MACCHINA KALI LINUX

Come da traccia abbiamo suddiviso i network della macchina metasploitable e kali linux, con i rispettivi:

Linux - 192.168.50.0

Metasploit - 192.168.90.0

Successivamente abbiamo configurato la nostra macchina PFSense aggiungendo i Gateway che ci serviranno per la corretta comunicazione delle 2 macchine.



```
PFSENSES [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
Starting CRON... done.
pfSense 2.6.0-RELEASE amd64 Mon Jan 31 19:57:53 UTC 2022
Bootup complete

FreeBSD/amd64 (pfSense.home.arp) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: ff30d707e9da203a3224

*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 10.0.2.15/24
LAN (lan)      -> em1      -> v4: 192.168.50.103/24
LAN2 (opt1)    -> em2      -> v4: 192.168.90.103/24

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: 
```

Dopo la configurazione si è svolto un test di ping e di scansione per controllare la corretta comunicazione delle due macchine, da cui abbiamo riscontrato esito positivo.

```

(kali㉿kali)-[~]
$ ping 192.168.90.101
PING 192.168.90.101 (192.168.90.101) 56(84) bytes of data.
64 bytes from 192.168.90.101: icmp_seq=1 ttl=63 time=1.07 ms
64 bytes from 192.168.90.101: icmp_seq=2 ttl=63 time=0.662 ms
64 bytes from 192.168.90.101: icmp_seq=3 ttl=63 time=0.762 ms
^C
— 192.168.90.101 ping statistics —
3 packets transmitted, 3 received, 0% packet loss, time 2016ms
rtt min/avg/max/mdev = 0.662/0.832/1.074/0.175 ms

(kali㉿kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:c6:5f:7e brd ff:ff:ff:ff:ff:ff
    inet 192.168.50.100/24 brd 192.168.50.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fec6:5f7e/64 scope link
        valid_lft forever preferred_lft forever

```

```

(kali㉿kali)-[~]
$ sudo nmap -sS 192.168.90.101
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-21 11:22 EST
Nmap scan report for 192.168.90.101
Host is up (0.00056s latency).
Not shown: 977 closed tcp ports (reset)
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    open  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

```

Infine abbiamo configurato le regole di firewall per bloccare le richieste di tipo TCP da parte della macchina kali, sulla porta 80 della macchina metasploitable

Edit Firewall Rule

Action

Block

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled

☐ Disable this rule

Set this option to disable this rule without removing it from the list.

Interface

LAN

Choose the interface from which packets must come to match this rule.

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

TCP

Choose which IP protocol this rule should match.


Source

Source

☐ Invert match

Single host or alias

192.168.50.100 /

 Display Advanced

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Destination

Destination

☐ Invert match

Single host or alias

192.168.90.101 /

Destination Port Range

HTTP (80)

From

Custom

HTTP (80)

To

Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

```
(kali㉿kali)-[~]  
$ sudo nmap -sS 192.168.90.101  
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-21 11:28 EST  
Nmap scan report for 192.168.90.101  
Host is up (0.00061s latency).  
Not shown: 977 closed tcp ports (reset)  
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
```