

Obbiettivo: Configurare il firewall psfsense in VM, per la comunicazione di due VM su reti diverse (Kali 192.168.50.100 – Metasploitable 192.168.90.100)

Nell'esercitazione di oggi siamo andati a settare come firewall psfsense, per prima cosa abbiamo impostato le reti sia su metasploitable sia su kali con reti differenti e su quest'ultimo il gateway su 192.168.50.102 dove psfsense fungerà da router come vediamo nelle immagini seguenti:

```
# This file describes the network
# and how to activate them. For mo

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 192.168.50.100/24
gateway 192.168.50.102

# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.90.100
netmask 255.255.255.0
network 192.168.90.0
broadcast 192.168.90.255
gateway 192.168.90.1
```

Dopo di che da browser siamo entrati nel settaggio di psfsense, da li abbiamo inserito una seconda lan per collegare metasploitable (LAN2) e settato l'altra LAN con i relativi indirizzi ip.

Static IPv4 Configuration	
IPv4 Address	192.168.90.100
IPv4 Upstream gateway	OPT1GW - 192.168.90.1
If this interface is an Internet connection, select an existing Gateway from the list.	

Static IPv4 Configuration	
IPv4 Address	192.168.50.102
IPv4 Upstream gateway	None
If this interface is an Internet connection, select an existing Gateway from the list.	

Dopodiche abbiamo impostato le nostre rules per la funzione firewall, per impedire l'ingresso sulla nostra DVWA di metasploitable e quindi impostiamo l'action in block e indichiamo la porta 80 con

servizi http.

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) 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/UDP

Choose which IP protocol this rule should match.

Destination

Destination

☐ Invert match

any

Destination Address

/

Destination Port Range

HTTP (80)

From

Custom

To

HTTP (80)

Custom

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

Infine effettuiamo una scansione nmap prima con il nostro firewall disattivato e poi attivo, possiamo notare come nella prima scansione ci trova le relative porte aperte. Con il nostro firewall attivo invece troviamo la dicitura filtered sulla porta 80 che ci indica l'impedimento nel raggiungerla e anche da browser la pagina non viene caricata.

```
(kali@kali) [~]
$ sudo nmap -sS 192.168.90.100
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-21 10:47 EST
Nmap scan report for 192.168.90.100
Host is up (0.0026s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https
Nmap done: 1 IP address (1 host up) scanned in 5.16 seconds
```

```
(kali@kali) [~]
$ sudo nmap -p80 192.168.90.100
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-21 12:11 EST
Nmap scan report for 192.168.90.100
Host is up (0.0024s latency).
PORT      STATE SERVICE
80/tcp    filtered http
Nmap done: 1 IP address (1 host up) scanned in 0.41 seconds
```

