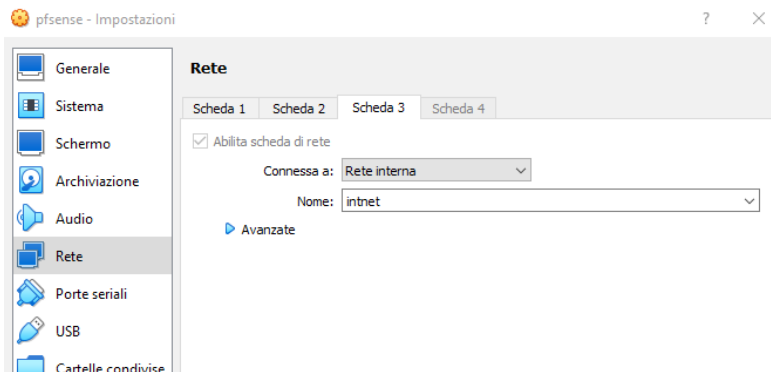


## TASK:

Scopo dell'esercizio di oggi è mettere la macchina kali e la macchina metasploitable su 2 reti diverse ma capaci di comunicare tra loro. Fatto ciò andremo ad introdurre le policy firewall tramite Pfsense in modo che kali non possa accedere a DVWA.

Per prima cosa siamo andati a modificare le impostazioni di Pfsense aggiungendo una terza scheda di rete in modo da poterlo mettere in comunicazione con Metasploitable:



Dopo ciò ho configurato le connessioni di Kali e Metasploitable:

```
source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
#iface eth0 inet dhcp

# dhcp

# static

address 192.168.50.100/24
gateway 192.168.50.103
```

```
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 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
```

A questo punto sono ho aperto la GUI di Pfsense e ho configurato le 2 LAN nel seguente modo:

|                         |                                                                                                                                                                                                                                                                                                          |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Enable                  | <input checked="" type="checkbox"/> Enable interface                                                                                                                                                                                                                                                     |
| Description             | <input type="text" value="LAN1"/><br><small>Enter a description (name) for the interface here.</small>                                                                                                                                                                                                   |
| IPv4 Configuration Type | <input type="text" value="Static IPv4"/>                                                                                                                                                                                                                                                                 |
| IPv6 Configuration Type | <input type="text" value="None"/>                                                                                                                                                                                                                                                                        |
| MAC Address             | <input type="text" value="xxxxxxxxxxxx"/><br><small>This field can be used to modify ("spoof") the MAC address of this interface.<br/>Enter a MAC address in the following format: xxxxxxxx:xx:xx or leave blank.</small>                                                                                |
| MTU                     | <input type="text" value=""/><br><small>If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.</small>                                                                                                                         |
| MSS                     | <input type="text" value=""/><br><small>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.</small>                                           |
| Speed and Duplex        | <input type="text" value="Default (no preference, typically autoselect)"/><br><small>Explicitly set speed and duplex mode for this interface.<br/>WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.</small> |

**Static IPv4 Configuration**

|                       |                                             |                                                    |                                 |
|-----------------------|---------------------------------------------|----------------------------------------------------|---------------------------------|
| IPv4 Address          | <input type="text" value="192.168.50.103"/> | /                                                  | <input type="text" value="24"/> |
| IPv4 Upstream gateway | <input type="text" value="None"/>           | <input type="button" value="+ Add a new gateway"/> |                                 |

|                         |                                                                                                                                                                                                                                                                                                          |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Enable                  | <input checked="" type="checkbox"/> Enable interface                                                                                                                                                                                                                                                     |
| Description             | <input type="text" value="LAN2"/><br><small>Enter a description (name) for the interface here.</small>                                                                                                                                                                                                   |
| IPv4 Configuration Type | <input type="text" value="Static IPv4"/>                                                                                                                                                                                                                                                                 |
| IPv6 Configuration Type | <input type="text" value="None"/>                                                                                                                                                                                                                                                                        |
| MAC Address             | <input type="text" value="xxxxxxxxxxxx"/><br><small>This field can be used to modify ("spoof") the MAC address of this interface.<br/>Enter a MAC address in the following format: xxxxxxxx:xx:xx or leave blank.</small>                                                                                |
| MTU                     | <input type="text" value=""/><br><small>If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.</small>                                                                                                                         |
| MSS                     | <input type="text" value=""/><br><small>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.</small>                                           |
| Speed and Duplex        | <input type="text" value="Default (no preference, typically autoselect)"/><br><small>Explicitly set speed and duplex mode for this interface.<br/>WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.</small> |

**Static IPv4 Configuration**

|                       |                                                    |                                                    |                                 |
|-----------------------|----------------------------------------------------|----------------------------------------------------|---------------------------------|
| IPv4 Address          | <input type="text" value="192.168.90.100"/>        | /                                                  | <input type="text" value="24"/> |
| IPv4 Upstream gateway | <input type="text" value="LAN2GW - 192.168.90.1"/> | <input type="button" value="+ 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](#).

Sono andato a vedere che le macchine potessero comunicare tramite il comando ping:

```
(kali㉿kali)-[~]
└─$ ping -c2 192.168.90.100
PING 192.168.90.100 (192.168.90.100) 56(84) bytes of data:
64 bytes from 192.168.90.100: icmp_seq=1 ttl=64 time=0.467 ms
64 bytes from 192.168.90.100: icmp_seq=2 ttl=64 time=0.437 ms

— 192.168.90.100 ping statistics —
2 packets transmitted, 2 received, 0% packet loss, time 1020ms
rtt min/avg/max/mdev = 0.437/0.452/0.467/0.015 ms
```

Sono poi passato a fare la scansione SYN tramite NMAP ottenendo questo risultato:

```
(kali㉿kali)-[~]
$ sudo nmap -sS 192.168.90.100
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-21 10:03 EST
Nmap scan report for 192.168.90.100
Host is up (0.00062s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 17.22 seconds
```

Dopodichè sono passato a configurare le Firewall policy come si può vedere dalle immagini qui sotto:

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

LAN1

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.

Source

Source

☐ Invert match

any

Source Address

/

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

any

Destination Address

/

Destination Port Range

any

From

Custom

To

any

Custom

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

**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** LAN2

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

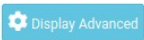
Choose which IP protocol this rule should match.

---

**Source**

**Source** ☐ Invert match any Source Address /

---

 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 any Destination Address /

---

**Destination Port Range** any any

From Custom 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.

Per avere conferma che le regole fossero effettivamente attive sono quindi andato a fare una nuova scansione SYN ottenendo questo risultato:

```
(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.90.100
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-21 10:11 EST
Nmap scan report for 192.168.90.100
Host is up (0.00058s latency).
All 1000 scanned ports on 192.168.90.100 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 34.44 seconds
```