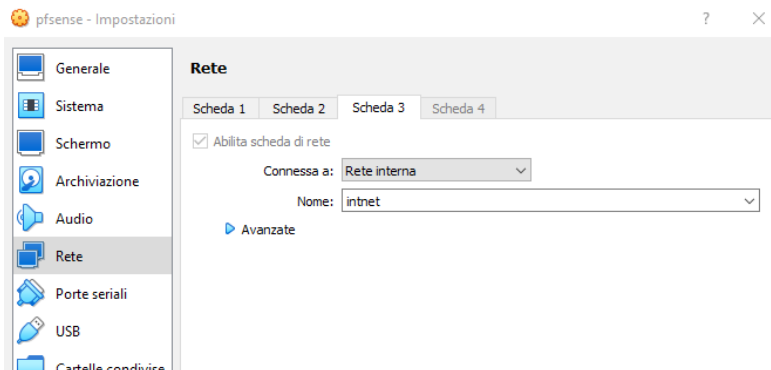TASK:

Scopo dell'esercizio di oggi è mettere la macchina kali e la macchina metasploitable su 2 reti divere 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 Metasplotable:

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

Enable	☑ Enable interface
Description	LAN1
	Enter a description (name) for the interface here.
IPv4 Configuration Type	Static IPv4
IPv6 Configuration Type	None
MAC Address	xx:xx:xx:xx:xx:xx
	This field can be used to modify ("spoof") the MAC address of this interface.
	Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx 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	Default (no preference, typically autoselect)
	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	192.168.50.103 / 24
IPv4 Upstream gateway	None ➕ Add a new gateway

Enable	☑ Enable interface
Description	LAN2
	Enter a description (name) for the interface here.
IPv4 Configuration Type	Static IPv4
IPv6 Configuration Type	None
MAC Address	xx:xx:xx:xx:xx:xx
	This field can be used to modify ("spoof") the MAC address of this interface.
	Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx 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	Default (no preference, typically autoselect)
	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	192.168.90.100 / 24
IPv4 Upstream gateway	LAN2GW - 192.168.90.1 ➕ 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 dall' immagine 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 ⌄
	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 ⌄	192.168.90.100 / ⌄
Destination Port Range	HTTP (80) ⌄	Custom	HTTP (80) ⌄	Custom
	From		To	

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: