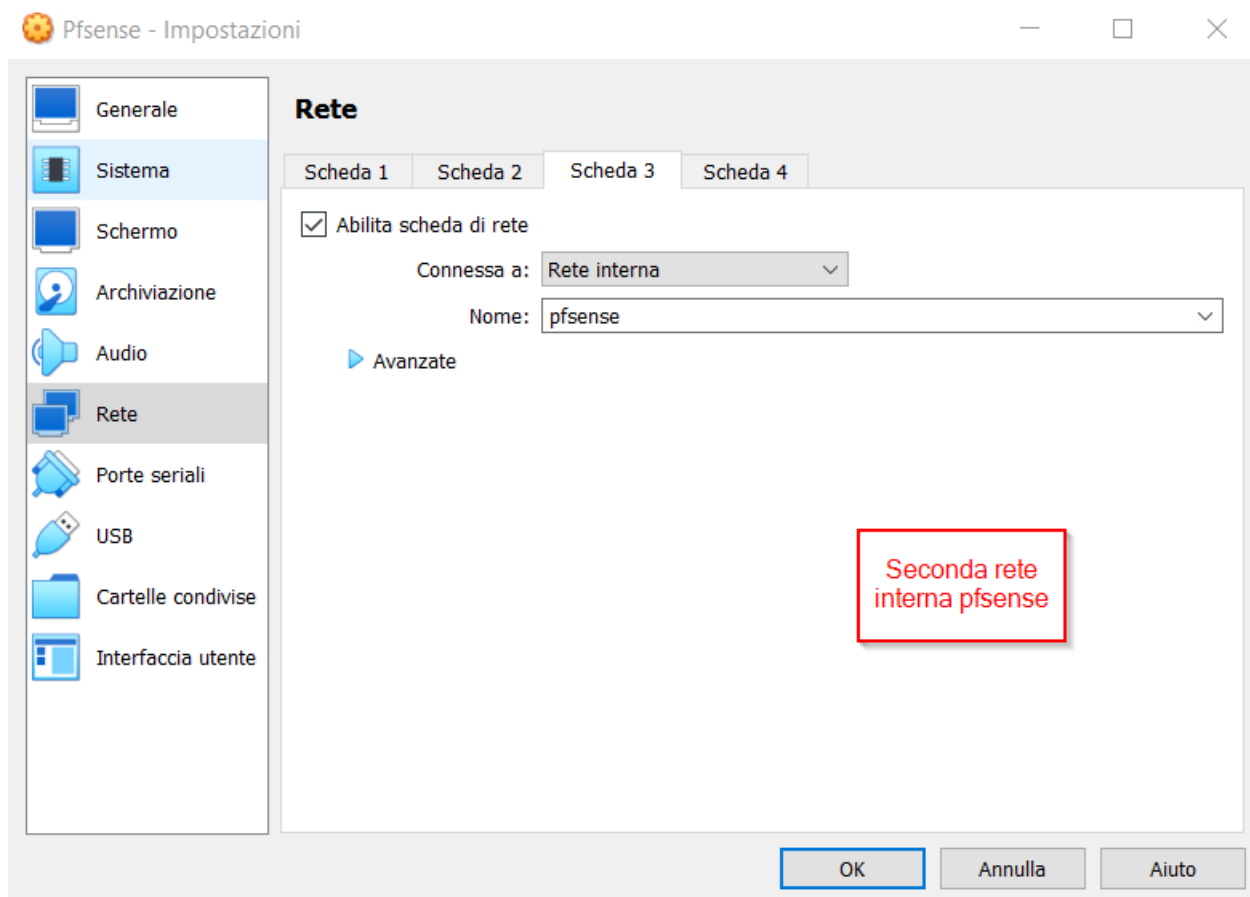


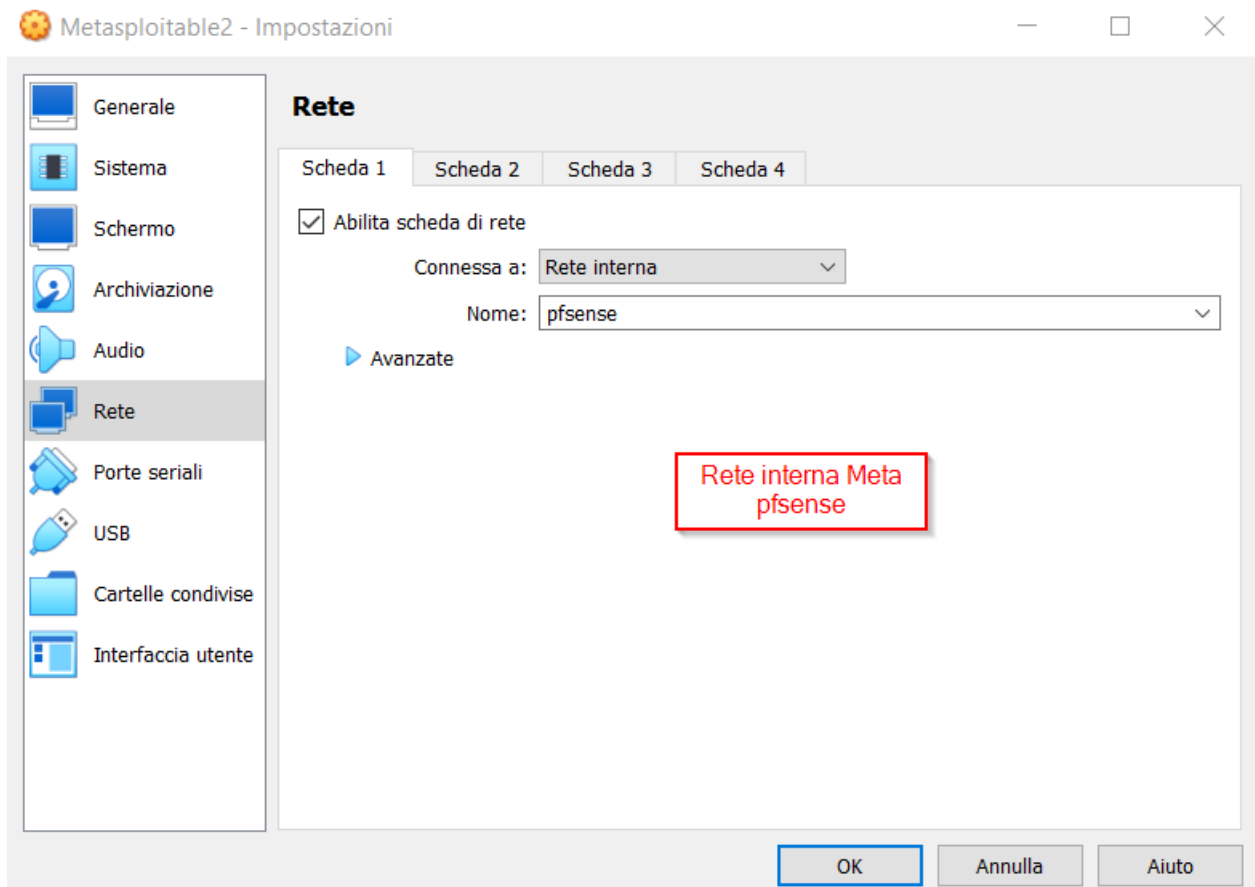
## ESERCIZIO W9D4

L'esercizio seguente ci porterà a creare un'eccezione nel policy set di pfsense, il nostro firewall. Negheremo lo scambio di pacchetti in partenza da Kali verso Meta.

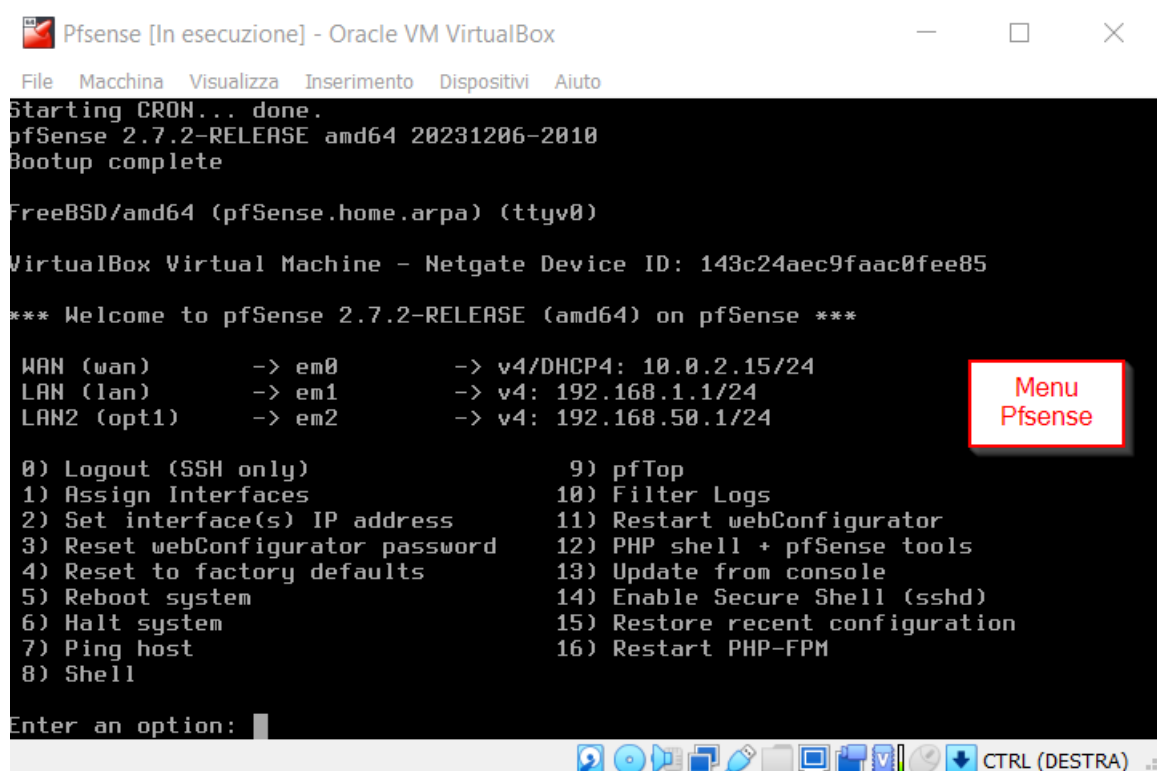
### Configurazione macchine

Iniziamo con il preparare pfsense andando ad aggiungere un secondo indirizzo LAN. Se avremo aperto la terza rete su VM, ci basterà seguire le opzioni di settaggio di set interface ed attivare così il nuovo servizio avente come IP 192.168.50.100. Ricordiamoci anche di cambiare la spunta nome per Meta in pfsense, altrimenti non sarà possibile per Meta ricevere un indirizzo dal DHCP.





Per fare in modo che pfsense assegni un certo range di indirizzi alla macchina, modifichiamo inoltre l'interfaccia di rete di Meta.



Metasploitable2 [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

GNU nano 2.0.7 File: interfaces Modified

```
# 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
iface eth0 inet dhcp
#address 192.168.50.101
#netmask 255.255.255.0
#network 192.168.50.0
#broadcast 192.168.50.255
#gateway 192.168.50.1
```

Meta interfaces configuration

Get Help WriteOut Read File Prev Page Cut Text Cur Pos  
Exit Justify Where Is Next Page UnCut Text To Spell

CTRL (DESTRA)

Su pfsense invece ci muoviamo come segue. Assicuriamoci di rendere operativa la nuova rete grazie ai dati essenziali. Attivazione interfacce, servizio DHCP, range utilizzabili, etc.

General Configuration

Enable ☒ Enable interface

Description  Creazione LAN2  
Enter a description (name) for the interface here.

IPv4 Configuration Type

IPv6 Configuration Type

MAC Address   
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   
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  / 24

IPv4 Upstream gateway  + 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"

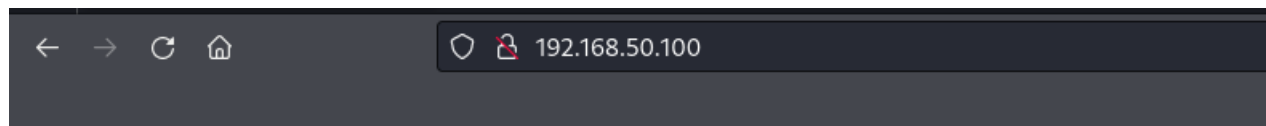
General DHCP Options	
DHCP Backend	ISC DHCP <span style="float: right; border: 1px solid red; padding: 2px;">Lan2 attivato</span>
Enable	<input checked="" type="checkbox"/> Enable DHCP server on LAN2 interface
BOOTP	<input type="checkbox"/> Ignore BOOTP queries
Deny Unknown Clients	<div>Allow all clients <span style="float: right;">▼</span></div> <p>When set to <b>Allow all clients</b>, any DHCP client will get an IP address within this scope/range on this interface. If set to <b>Allow known clients from any interface</b>, any DHCP client with a MAC address listed in a static mapping on <b>any</b> scope(s)/interface(s) will get an IP address. If set to <b>Allow known clients from only this interface</b>, only MAC addresses listed in static mappings on this interface will get an IP address within this scope/range.</p>
Ignore Denied Clients	<input type="checkbox"/> Ignore denied clients rather than reject <small>This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.</small>
Ignore Client Identifiers	<input type="checkbox"/> Do not record a unique identifier (UID) in client lease data if present in the client DHCP request <small>This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.</small>
Primary Address Pool	
Subnet	192.168.50.0/24
Subnet Range	192.168.50.1 - 192.168.50.254
Address Pool Range	<div>192.168.50.100</div> <div>192.168.50.200</div>

## Test connettività tra Kali e Meta

Prima di passare al policy set, controlliamo che le macchine riescano a comunicare tra di loro nonostante si trovino su reti diverse. Pinghiamo Meta con Kali e cerchiamo di accedere con il browser al server Metasploitable2.

```
(kali㉿kali)-[~]
$ ping 192.168.50.100
PING 192.168.50.100 (192.168.50.100) 56(84) bytes of data:
64 bytes from 192.168.50.100: icmp_seq=1 ttl=63 time=1.03 ms
64 bytes from 192.168.50.100: icmp_seq=2 ttl=63 time=2.06 ms
64 bytes from 192.168.50.100: icmp_seq=3 ttl=63 time=0.748 ms
64 bytes from 192.168.50.100: icmp_seq=4 ttl=63 time=2.09 ms
^C
— 192.168.50.100 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3069ms
rtt min/avg/max/mdev = 0.748/1.483/2.093/0.601 ms
```

Kali ping  
Meta



Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

Kali find Meta

- [TWiki](#)
- [phpMyAdmin](#)
- [Mutillidae](#)
- [DVWA](#)
- [WebDAV](#)

Tutto funziona. Ora, non ci resta che inserire l'eccezione usando pfsense.

## Negazione pacchetti

Andiamo a specificare porta e indirizzi interessanti nella regola del policy set riguardante la rete LAN1. In questo modo Kali non sarà in grado di connettersi al server web Metasploitable2. Nel caso vogliamo un'ulteriore conferma, Wireshark ci fornisce, nelle sue analisi numerosi tentativi di connessione falliti, come nell'ultima figura sottostante.

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.

Creazione regola

Source

Source

☐ Invert match

Address or Alias

192.168.1.100

/

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

Address or Alias

192.168.50.100

/

Destination Port Range

HTTP (80)

From

Custom

HTTP (80)

To

Custom

The connection has timed out

The server at 192.168.50.100 is taking too long to respond.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the web.

Kali and Meta connection blocked

Try Again

eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port == 80

Time	Source	Destination	Protocol	Length	Info
69.2678156	192.168.1.100	92.123.106.16	TCP	54	41352 → 80 [ACK] Seq=1661 Ack=3555
97.0134260	192.168.1.100	192.168.50.100	TCP	74	50544 → 80 [SYN] Seq=0 Win=64240 Len=0
221.174543	192.168.1.100	192.168.50.100	TCP	74	50550 → 80 [SYN] Seq=0 Win=64240 Len=0
99.7151456	192.168.1.100	192.168.50.100	TCP	74	[TCP Retransmission] 50544 → 80 [SYN] Seq=0 Win=64240 Len=0
253.006767	192.168.1.100	192.168.50.100	TCP	74	[TCP Retransmission] 50550 → 80 [SYN] Seq=0 Win=64240 Len=0
008.998908	192.168.1.100	192.168.50.100	TCP	74	[TCP Retransmission] 50544 → 80 [SYN] Seq=0 Win=64240 Len=0
269.420986	192.168.1.100	192.168.50.100	TCP	74	[TCP Retransmission] 50550 → 80 [SYN] Seq=0 Win=64240 Len=0
752.940749	192.168.1.100	92.123.106.16	TCP	54	[TCP Keep-Alive] 41352 → 80 [ACK] Seq=1661 Ack=3555
754.189674	92.123.106.16	192.168.1.100	TCP	60	[TCP Keep-Alive ACK] 80 → 41352 [ACK] Seq=1661 Ack=3555
270.602828	192.168.1.100	192.168.50.100	TCP	74	[TCP Retransmission] 50544 → 80 [SYN] Seq=0 Win=64240 Len=0

Frame 42: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0

Ethernet II, Src: 08:00:27:53:0c:ba (08:00:27:53:0c:ba), Dst: 08:00:27:6d:2a:19 (08:00:27:6d:2a:19)

Internet Protocol Version 4, Src: 192.168.1.100, Dst: 92.123.106.16

Transmission Control Protocol, Src Port: 41352, Dst Port: 80, Seq: 416, Ack: 889, Len: 0

Wireshark testing

wireshark\_eth06L3JG2.pcapng

Packets: 264 · Displayed: 59 (22.3%) · Dropped: 0 (0.0%) · Profile: Default