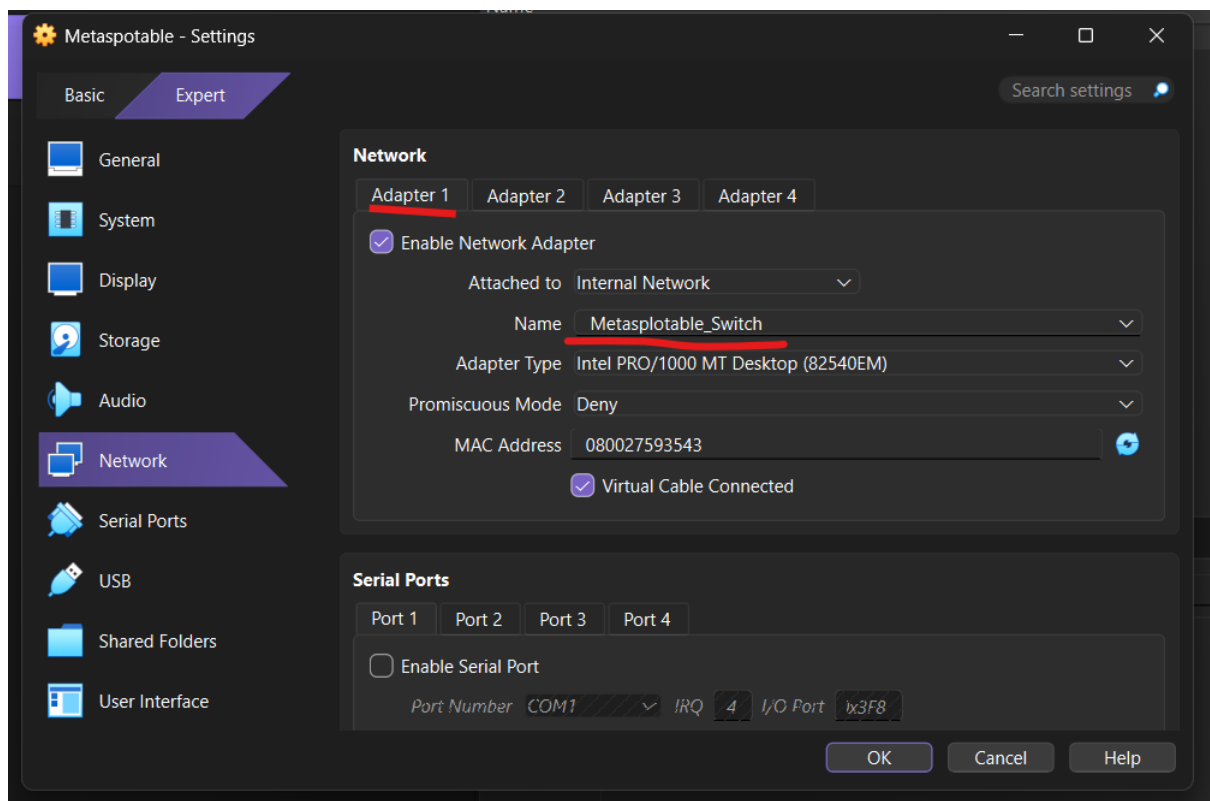


Obbiettivo:

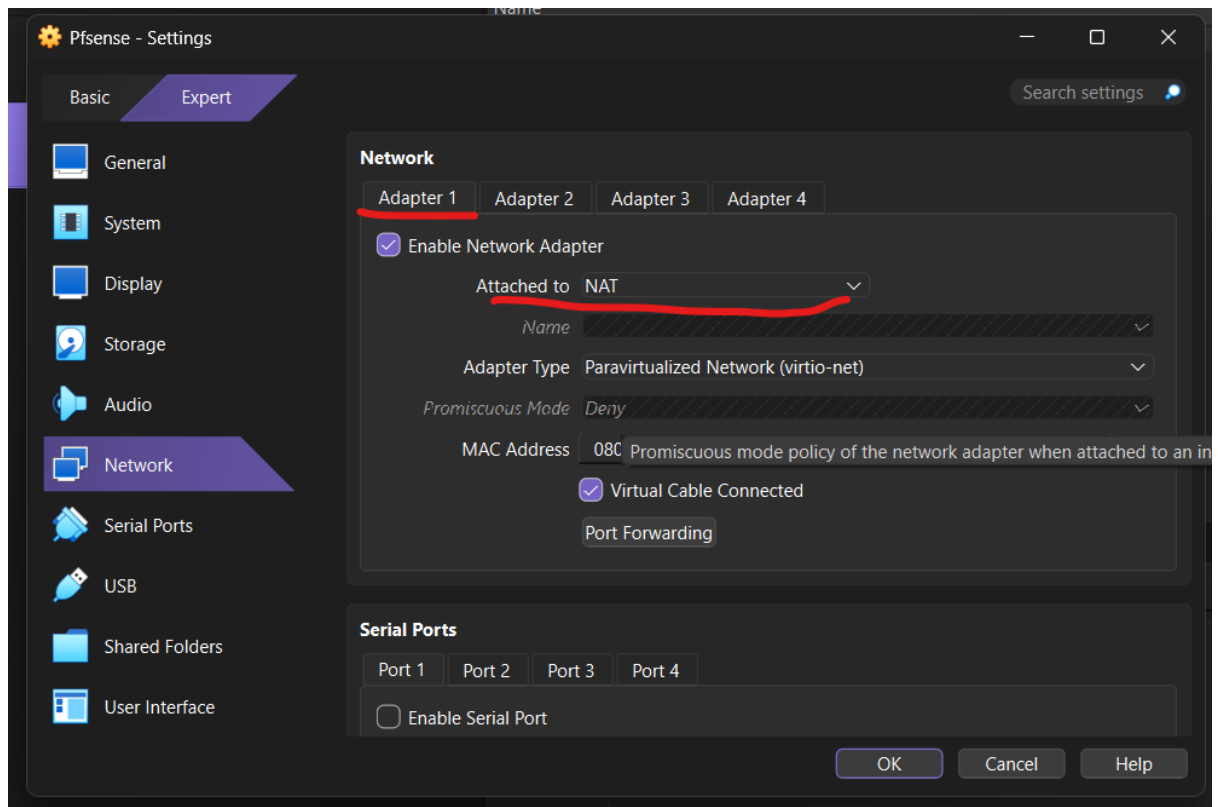
Creare una regola firewall che **blocchi** l'accesso alla DVWA (su metasploitable) dalla macchina Kali Linux e ne impedisca di conseguenza lo scan. Un requisito fondamentale dell'esercizio è che le macchine Kali e Metasploitable siano su reti diverse, potete aggiungere una nuova interfaccia di rete a PfSense in modo tale da gestire una ulteriore rete. Connettetevi poi in Web Gui per attivare la nuova interfaccia e configurarla.

Configurazione Network delle tre macchine Virtuali

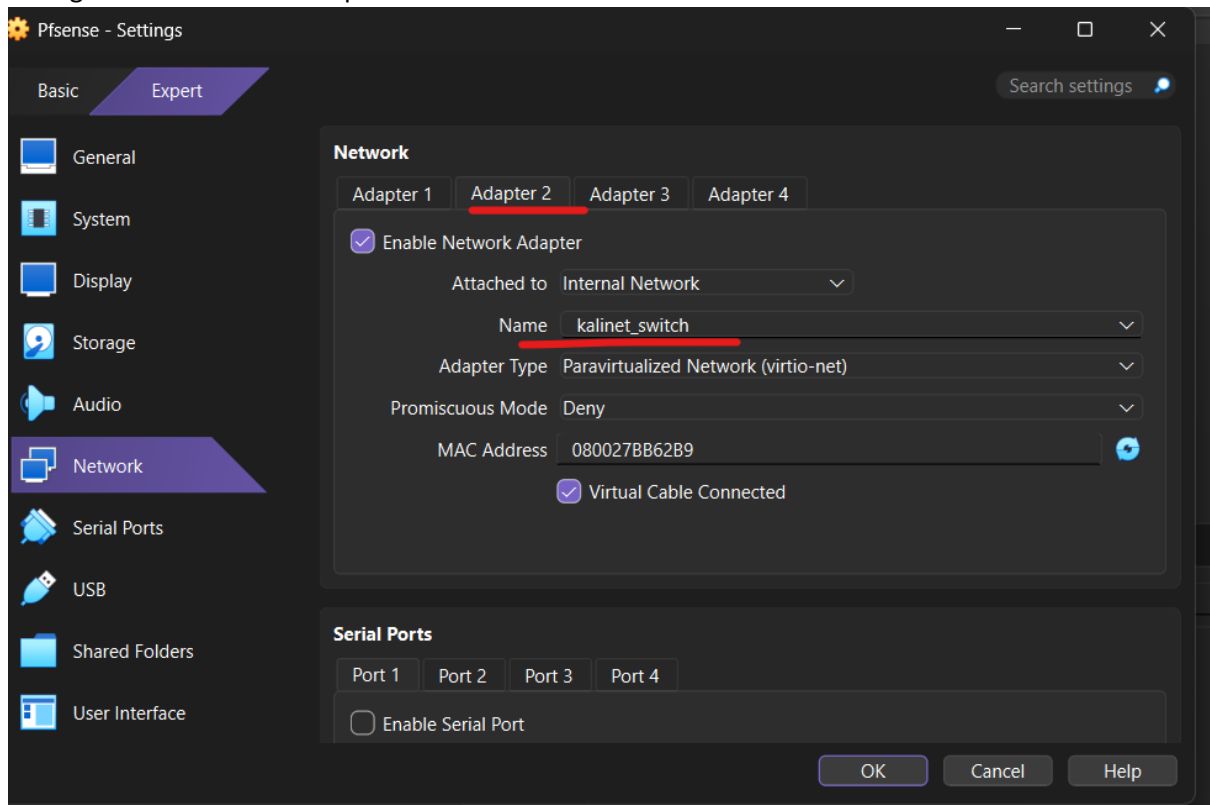
Configurazione **Metasploitable** Adapter1



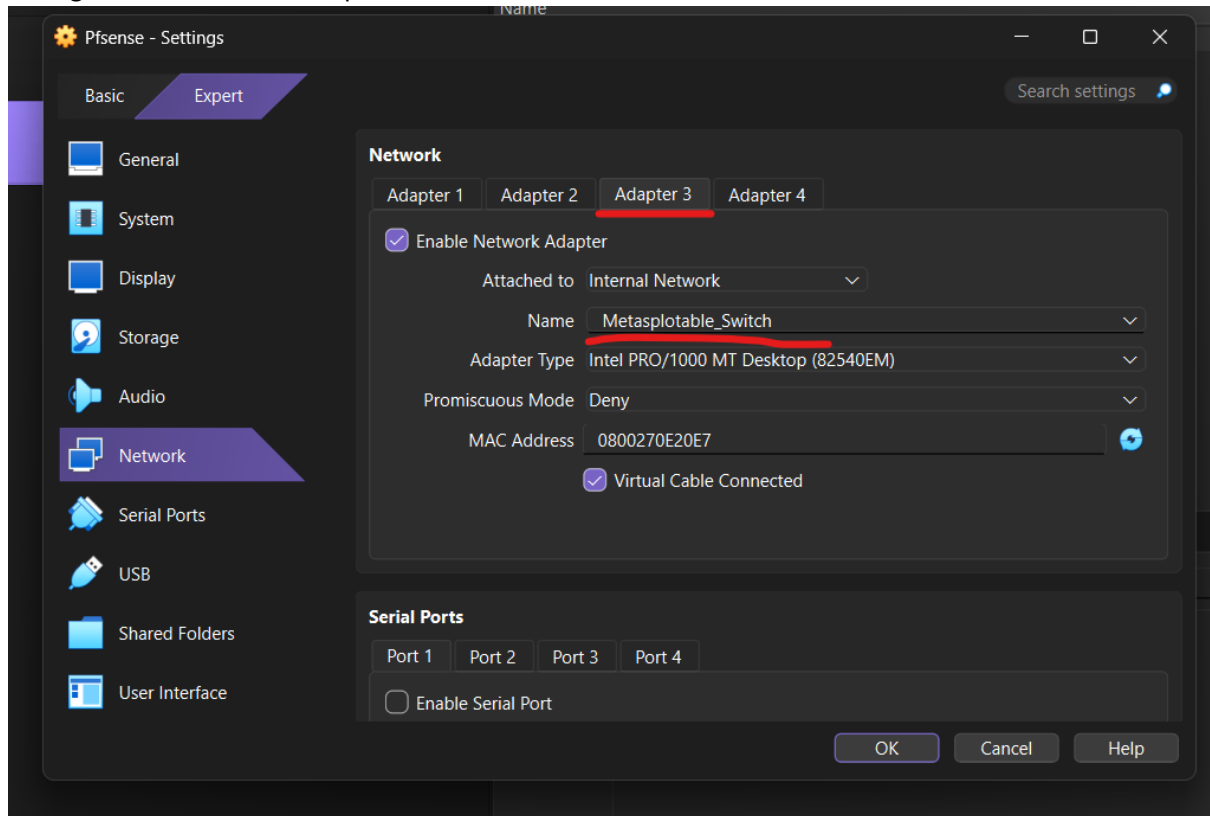
Configurazione PsSense Adapter 01



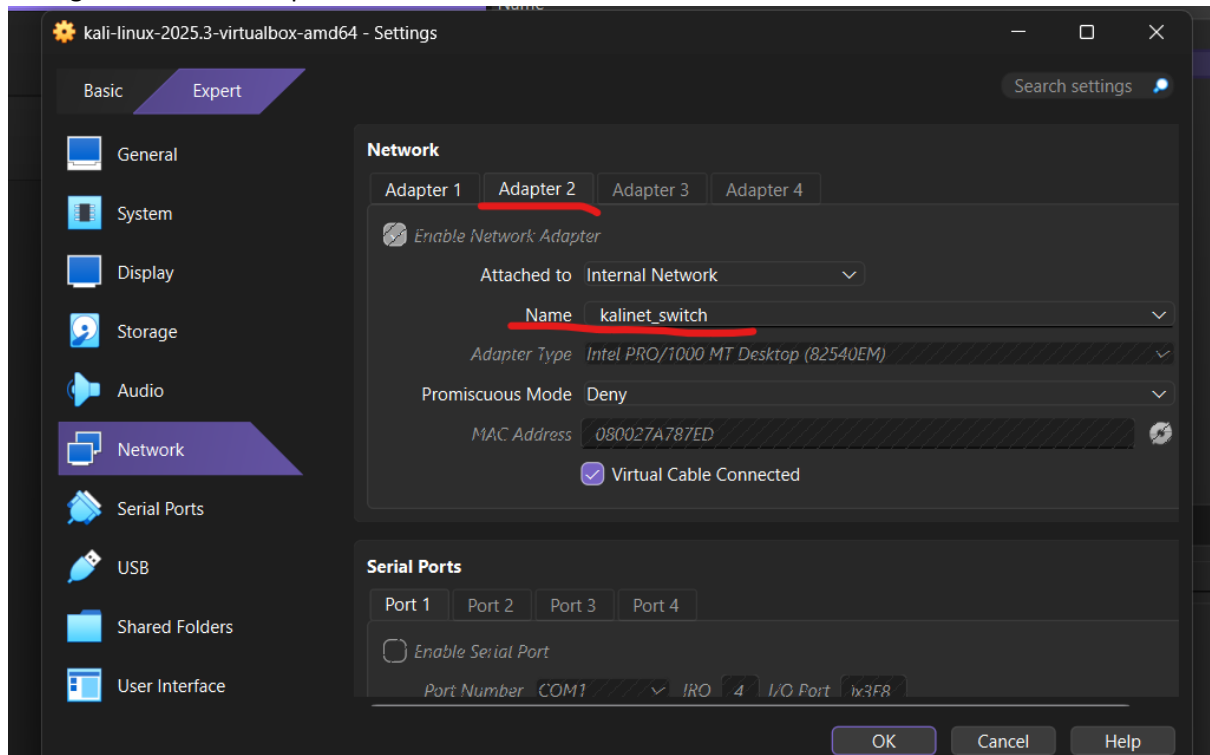
Configurazione PsSense Adapter 02



Configurazione PsSense Adapter 03



Configurazione Kali Adapter 01



PfSense 3 schede di rete e gli ip associati:

```
Pfsense [Running] - Oracle VirtualBox
File Machine View Input Devices Help

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> vtnet0      -> v4/DHCP4: 10.0.2.15/24
LAN (lan)      -> vtnet1      -> v4: 192.168.10.1/24
OPT1 (opt1)    -> em0         -> v4: 192.168.20.1/24
```

PfSense Configuration gateway range

Network 1:

Start Address Range: 192.268.10.2

End Address Range: 192.268.10.254

Network 2:

Start Address Range: 192.268.20.2

End Address Range: 192.268.20.254

```
Pfsense [Running] - Oracle VirtualBox
Configure IPv4 address OPT1 interface via DHCP? (y/n) n
Enter the new OPT1 IPv4 address. Press <ENTER> for none:
> 192.168.20.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
    255.255.0.0   = 16
    255.0.0.0     = 8

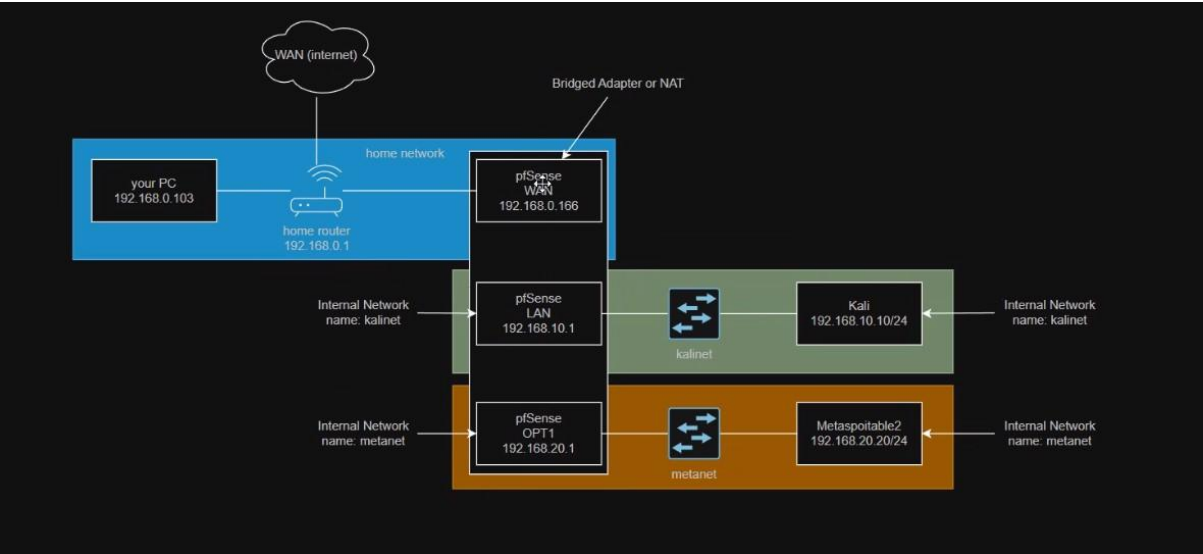
Enter the new OPT1 IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new OPT1 IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address OPT1 interface via DHCP6? (y/n) n
Enter the new OPT1 IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on OPT1? (y/n) y
Enter the start address of the IPv4 client address range: 192.168.20.2
Enter the end address of the IPv4 client address range: 192.168.20.254
```

Topologico Ottenuto:



ScreenshotFirewall rules WAN:

Interfaces / WAN (vtnet0)

General Configuration

Enable ☒ Enable interface

Description
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.




DHCP Client Configuration

Options ☐ Advanced Configuration ☐ Configuration Override
Use advanced DHCP configuration options. Override the configuration from this file.

Hostname
The value in this field is sent as the DHCP client identifier and hostname when requesting a DHCP lease. Some ISPs may require this (for client identification).

Alias IPv4 address / 32

Screenshot Firewall rules LAN

Interfaces / LAN (vtnet1)   

General Configuration

Enable

☒ Enable interface

Description

LAN

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

192.168.10.1

/ 24

IPv4 Upstream gateway

None

+ 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](#).

Screenshot Firewall rules **OPT1**

Interfaces / **OPT1 (em0)**

General Configuration

Enable ☒ Enable interface

Description
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.

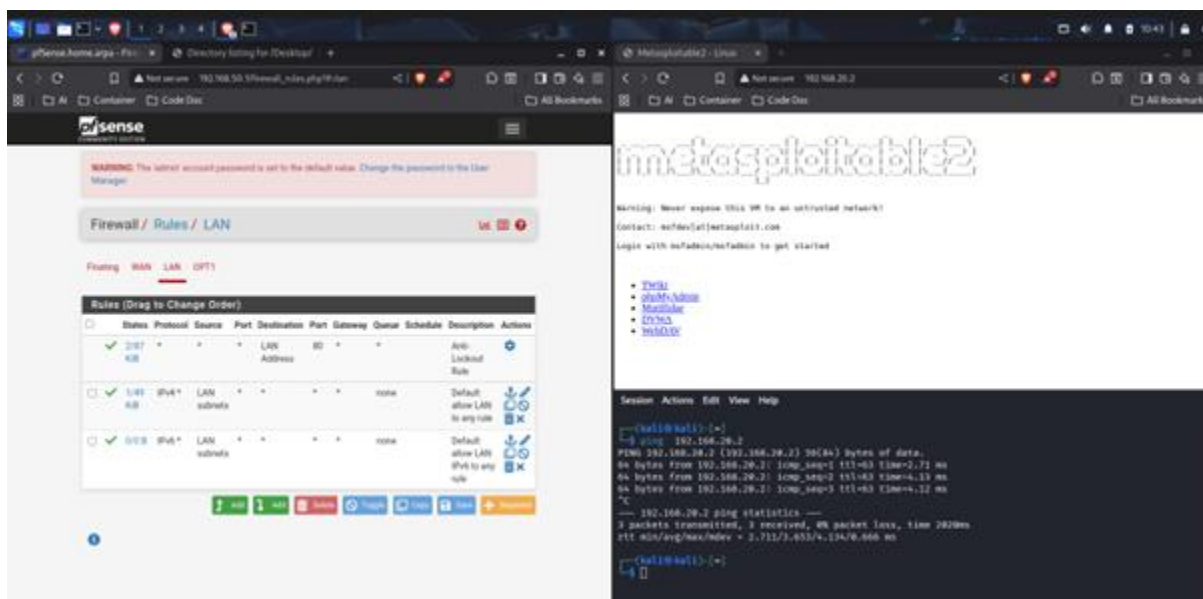
Speed and Duplex
Explicitly set speed and duplex mode for this interface.
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

Static IPv4 Configuration

IPv4 Address /

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".
Selecting an upstream gateway causes the firewall to treat this interface as a [WAN type interface](#).
Gateways can be managed by [clicking here](#).

Screenshot browser della Kali che apre la pagina servita della Metasploitable2 + il protocollo ICMP raggiungibile.



Screenshot browser della Kali che non riesce più ad aprire la pagina servita dalla Metasploitable2 (dopo l'applicazione della regola) + il protocollo ICMP ancora funzionante

The image shows two side-by-side screenshots. The left screenshot is a web browser displaying the pfSense Firewall Rules configuration page for the LAN interface. A warning message at the top states: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below this, a green message indicates: "The changes have been applied successfully. The firewall rules are now reloading in the background. Monitor the filter reload progress." The "Rules (Drag to Change Order)" table is visible, showing four rules:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0/948 KB	*	*	LAN Address	80	*	*	*	Anti-Lockout Rule	[Settings]
<input type="checkbox"/>	0/240 B	192.168.50.11	TCP	192.168.20.2	80 (HTTP)	*	none	*		[Add] [Edit] [Delete]
<input checked="" type="checkbox"/>	0/97 KB	IPv4 *	*	LAN subnets	*	*	*	*	Default allow LAN to any rule	[Add] [Edit] [Delete]
<input checked="" type="checkbox"/>	0/0 B	IPv6 *	*	LAN subnets	*	*	*	*	Default allow LAN IPv6 to any rule	[Add] [Edit] [Delete]

The right screenshot shows a Kali Linux terminal window. The top part displays a browser error message: "This site can't be reached. 192.168.20.2 refused to connect." Below this, the terminal shows the execution of the following commands:

```
ip net 192.168.50.11/24 brd 192.168.50.255 scope global dynamic noprefixroute eth0
valid_lft 6742sec preferred_lft 6742sec
ip net 192.168.50.11/24 brd 192.168.50.255 scope link noprefixroute
valid_lft forever preferred_lft forever
```

The terminal output shows the results of a ping command to 192.168.20.2:

```
PING 192.168.20.2 (192.168.20.2) 56(84) bytes of data:
64 bytes from 192.168.20.2: icmp_seq=1 ttl=63 time=3.41 ms
64 bytes from 192.168.20.2: icmp_seq=2 ttl=63 time=3.19 ms
64 bytes from 192.168.20.2: icmp_seq=3 ttl=63 time=2.03 ms
^C
- 192.168.20.2 ping statistics -
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 2.025/2.873/3.408/0.686 ms
```