# 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.

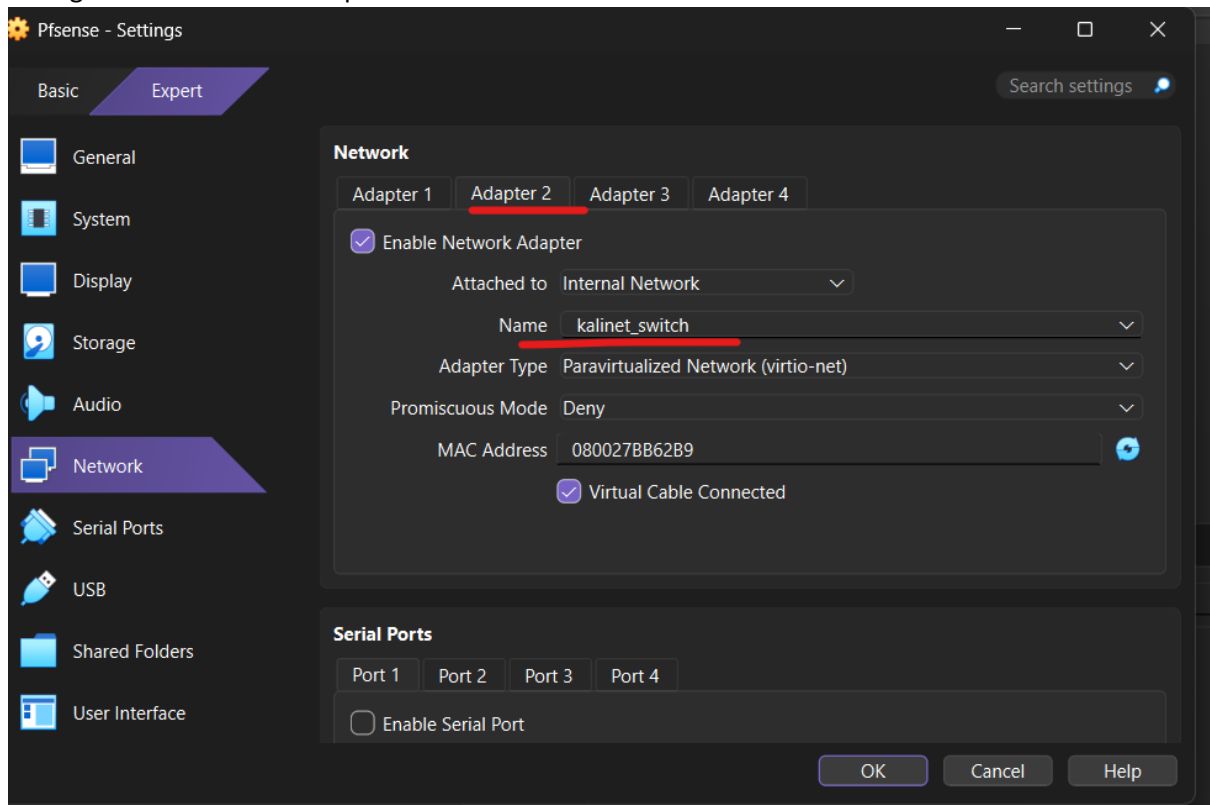# Configurazione Network delle tre macchine Virtuali

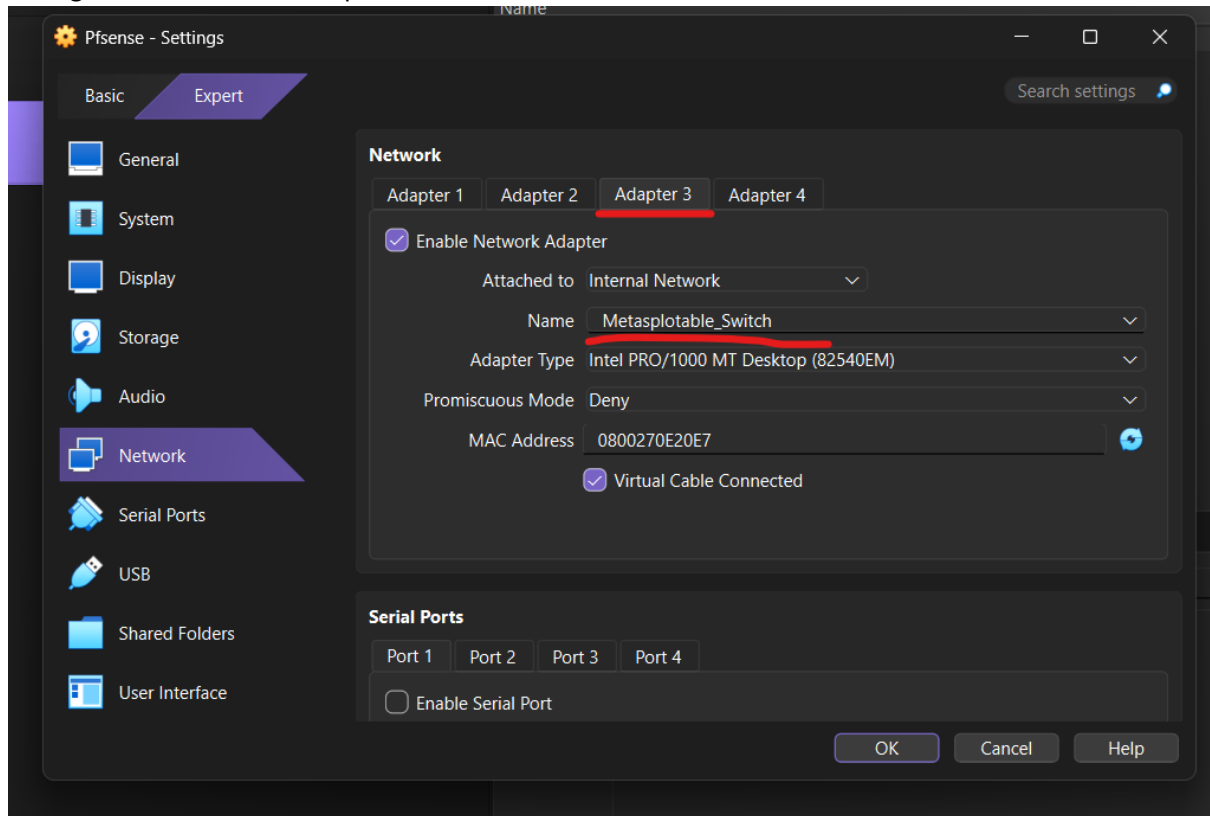Configurazione **Mtasploitable** Adapter1
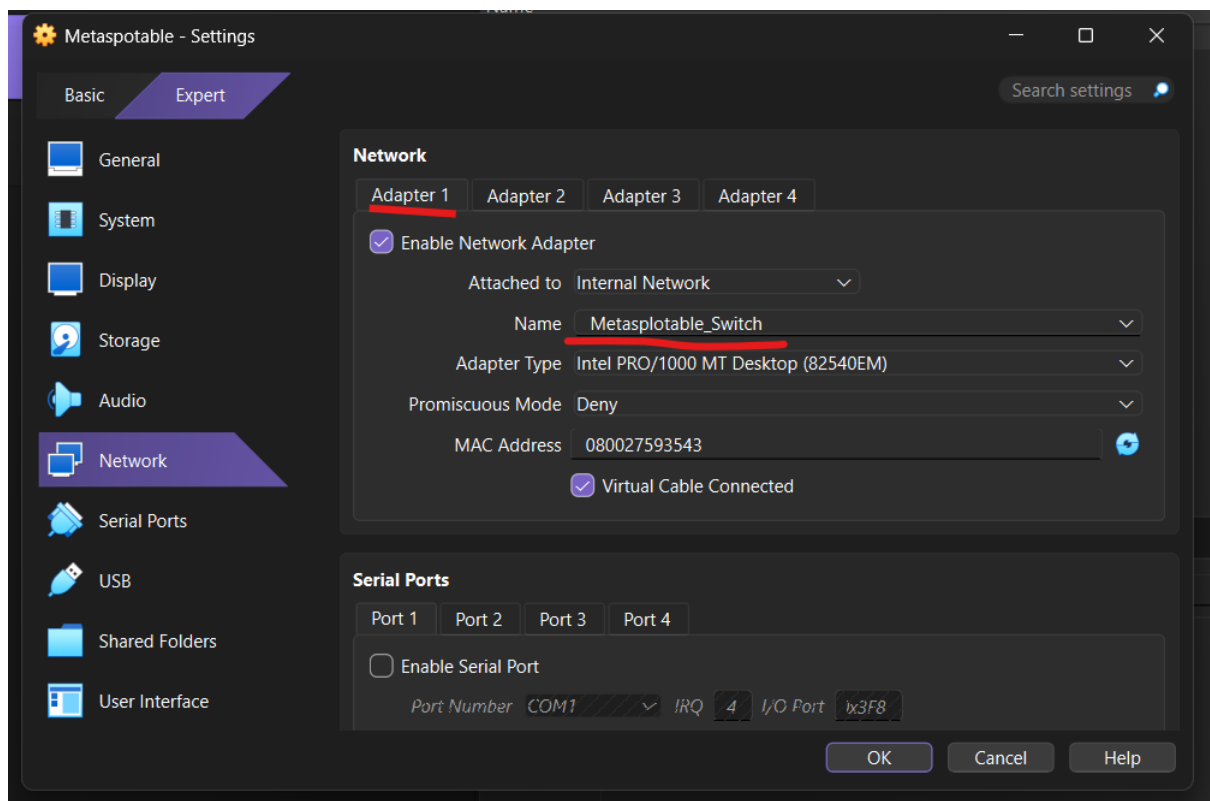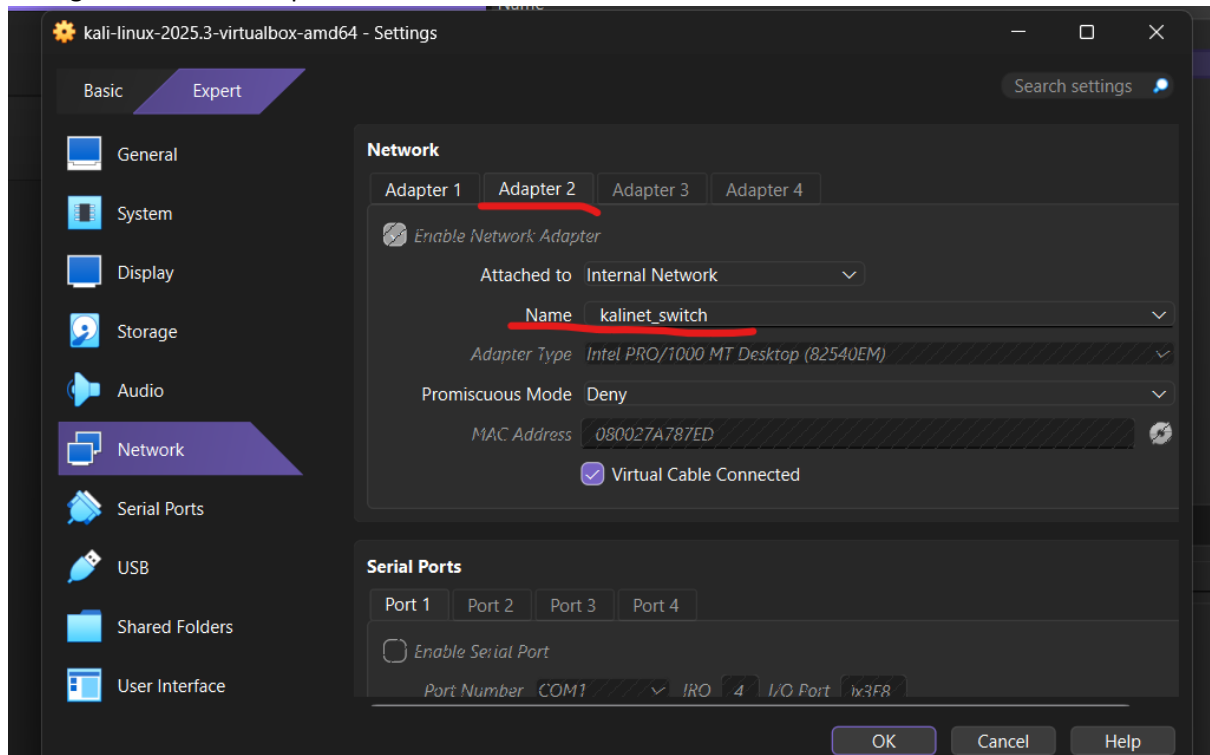
Configurazione **PsSense** Adapter 01
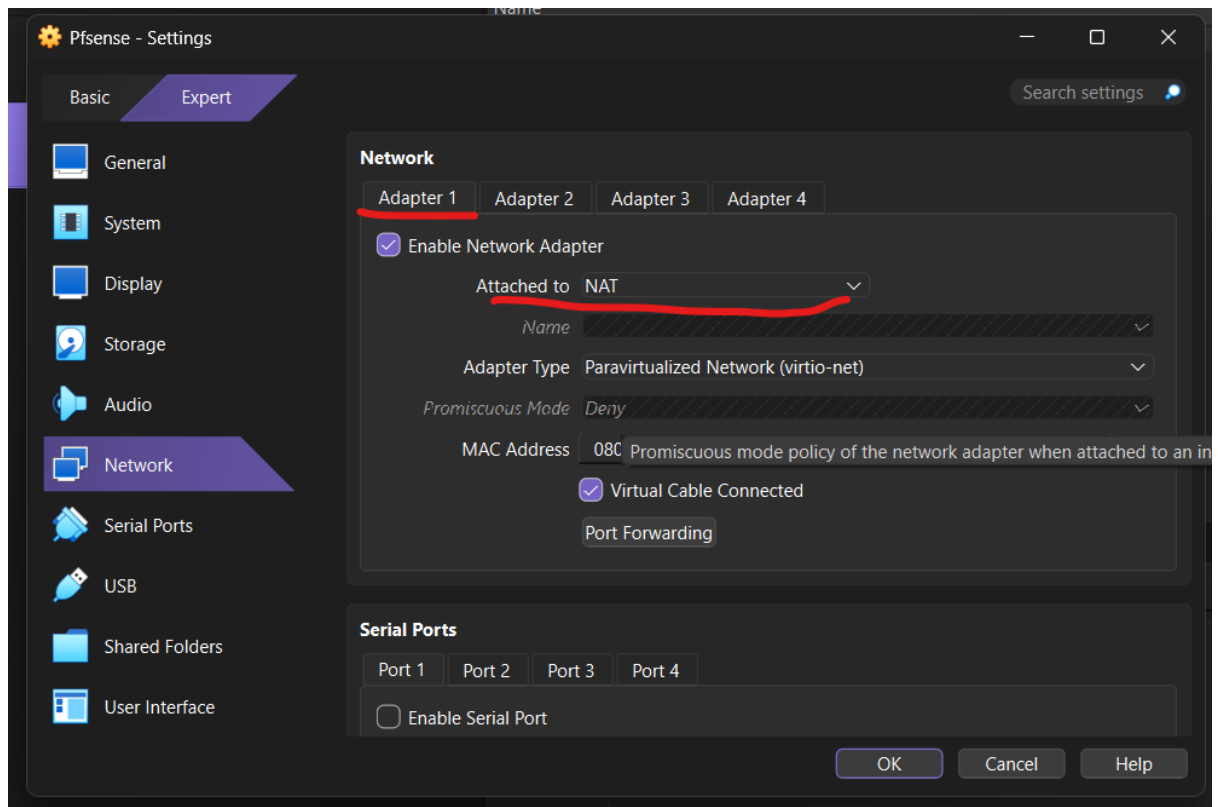
Configurazione **PsSense** Adapter 02

Configurazione **PsSense** Adapter 03

Configurazione **Kali** Adapter 01

PSense 3 schede di rete e gli ip associati:


```
*** 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 Rage: 192.268.10.254
Network 2:
Start Address Range: 192.268.20.2
End Address Rage: 192.268.20.254


```
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
```
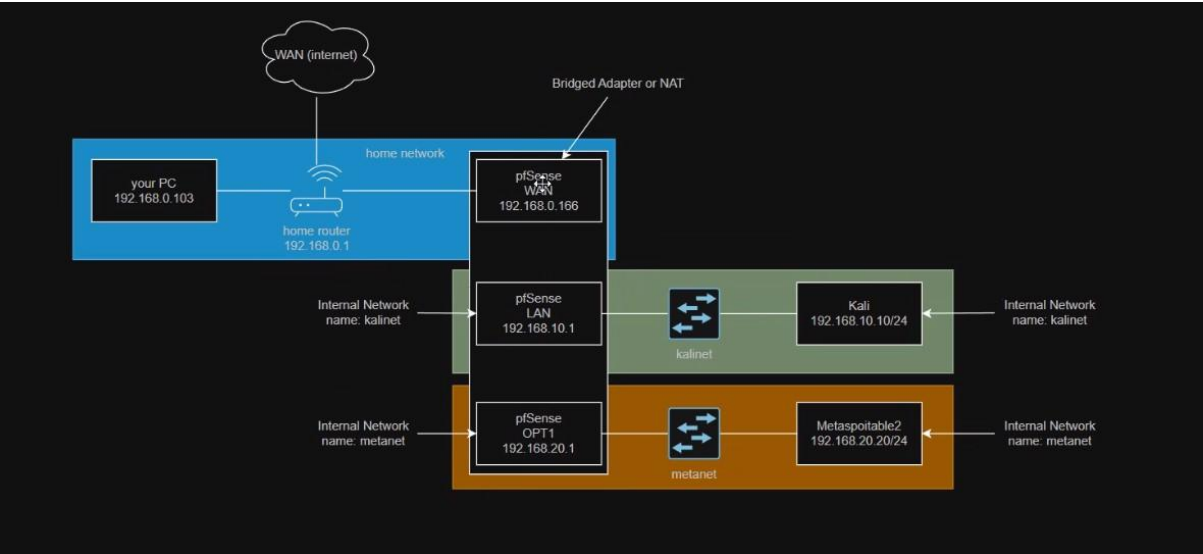
Topologico Ottenuto:

ScreenshotFirewall rules **WAN**:

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**

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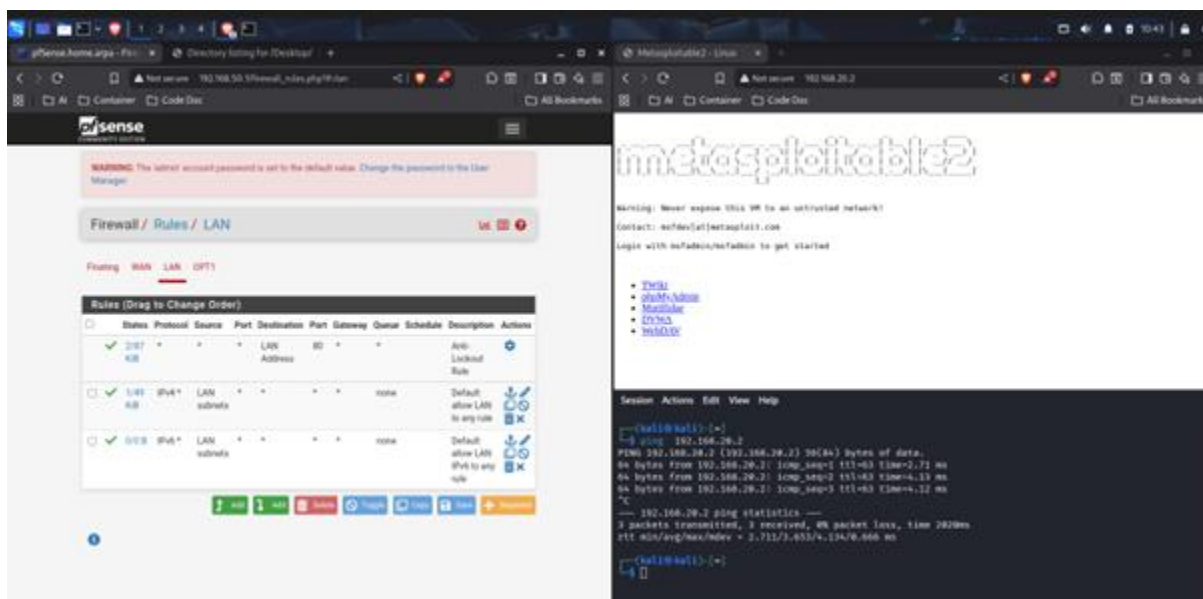
Screeenshot browser della Kali che non riesce più ad aprire la pagina servita della Metasploitable2 (dopo l'applicazione della regola) + il protocollo ICMP ancora funzionante