

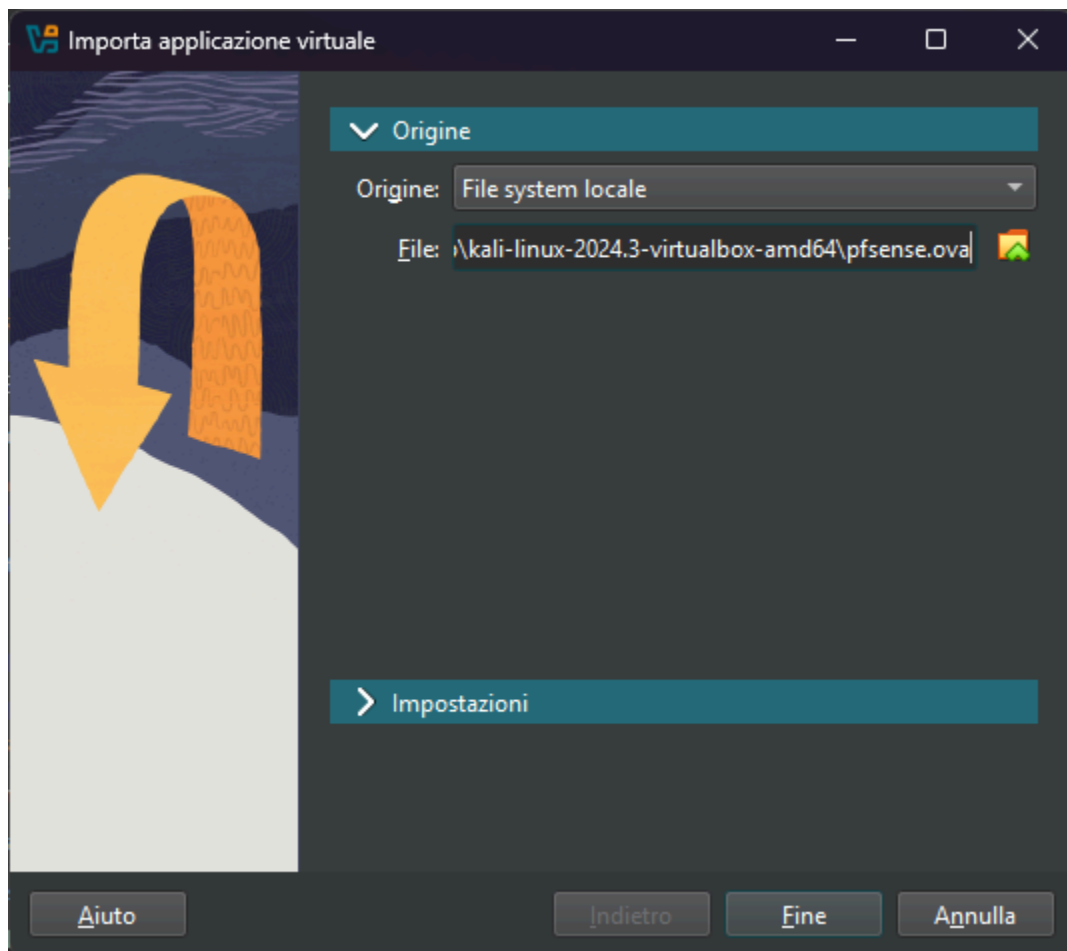
PRATICA S3L5

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.

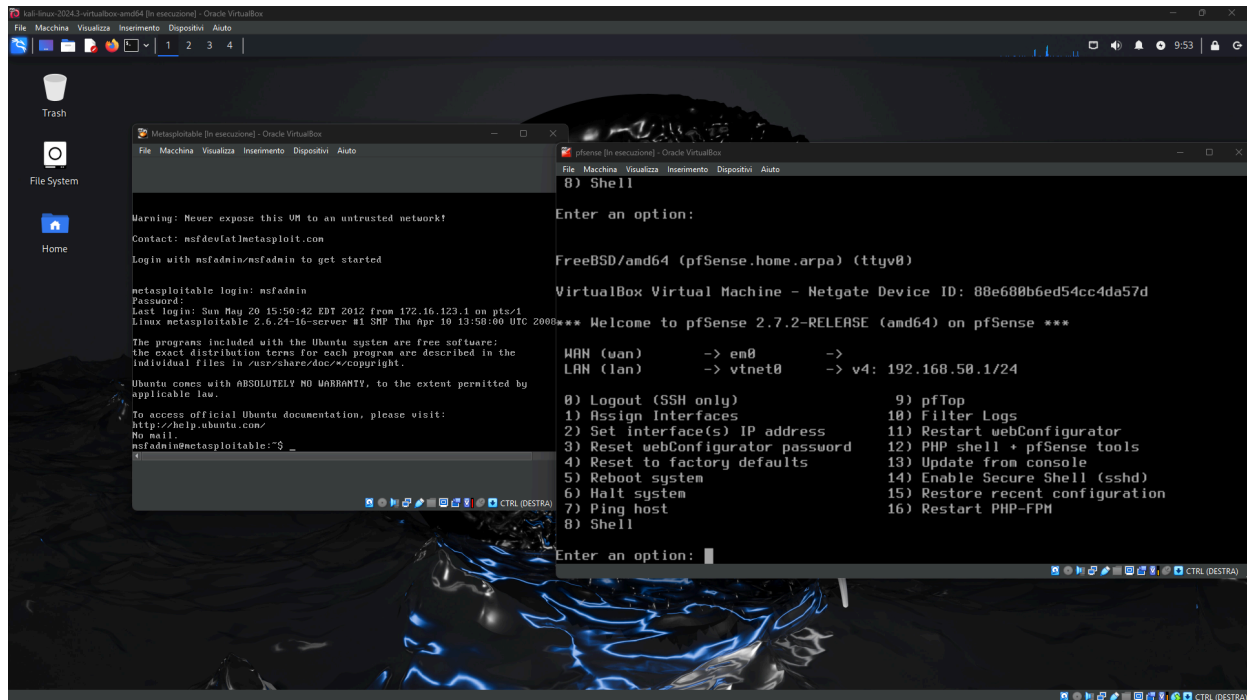
Assumiamo che le macchine Kali Linux e Metasploitable siano già su reti separate e che sia necessario aggiungere una nuova interfaccia di rete in pfSense.

1. Importazione di pfSense e avvio macchine

Importiamo pfSense su VirtualBox.

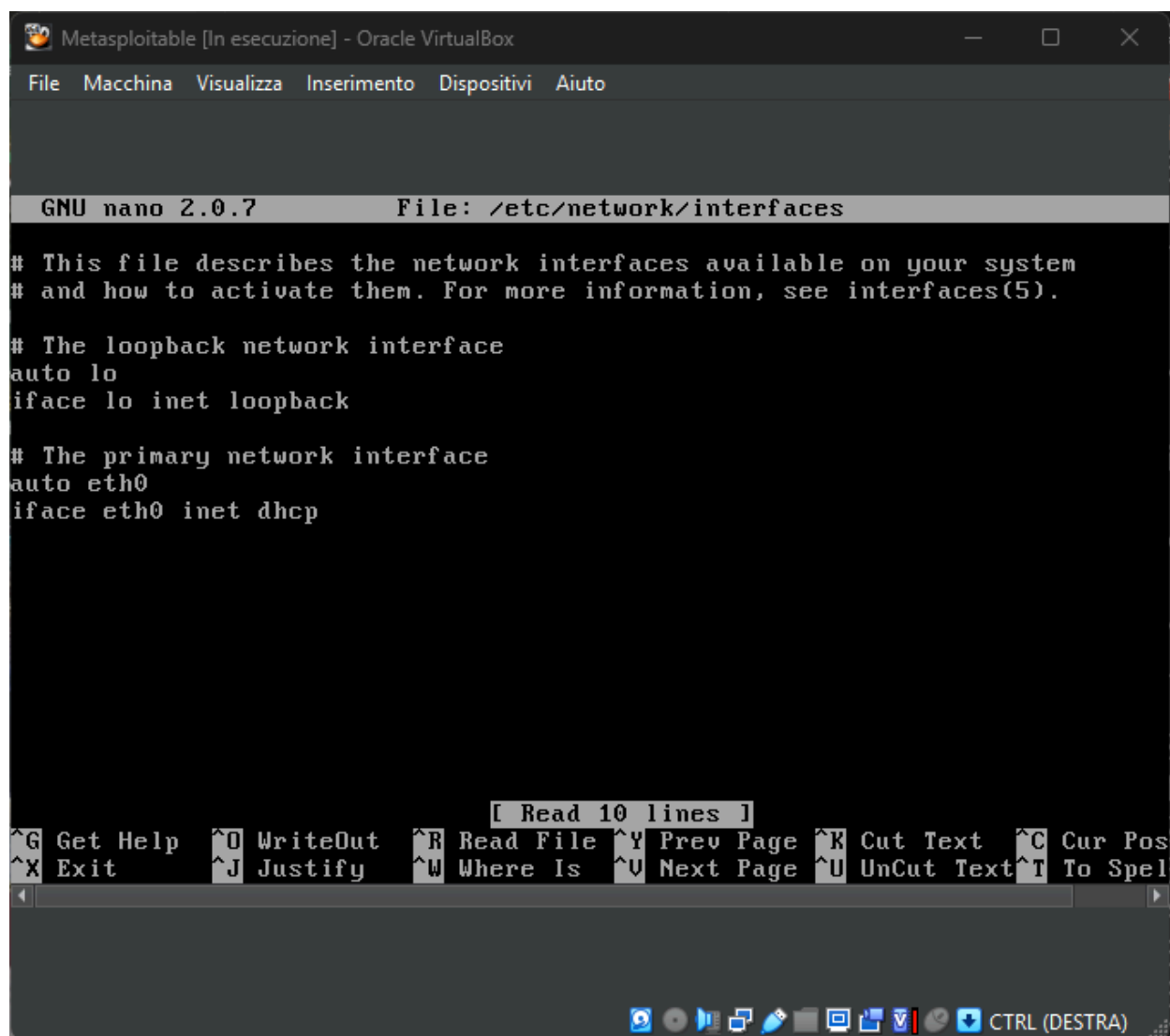


Tramite VirtualBox avvio le pfSense, Kali e Metasploitable.



2. Modifica della rete di Metasploitable

Metasploitable e PfSense devono trovarsi su reti diverse, quindi vado a modificare la rete di Metasploitable attraverso il comando "sudo nano /etc/network/interfaces".



```
Metasploitable [In esecuzione] - Oracle VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

GNU nano 2.0.7      File: /etc/network/interfaces

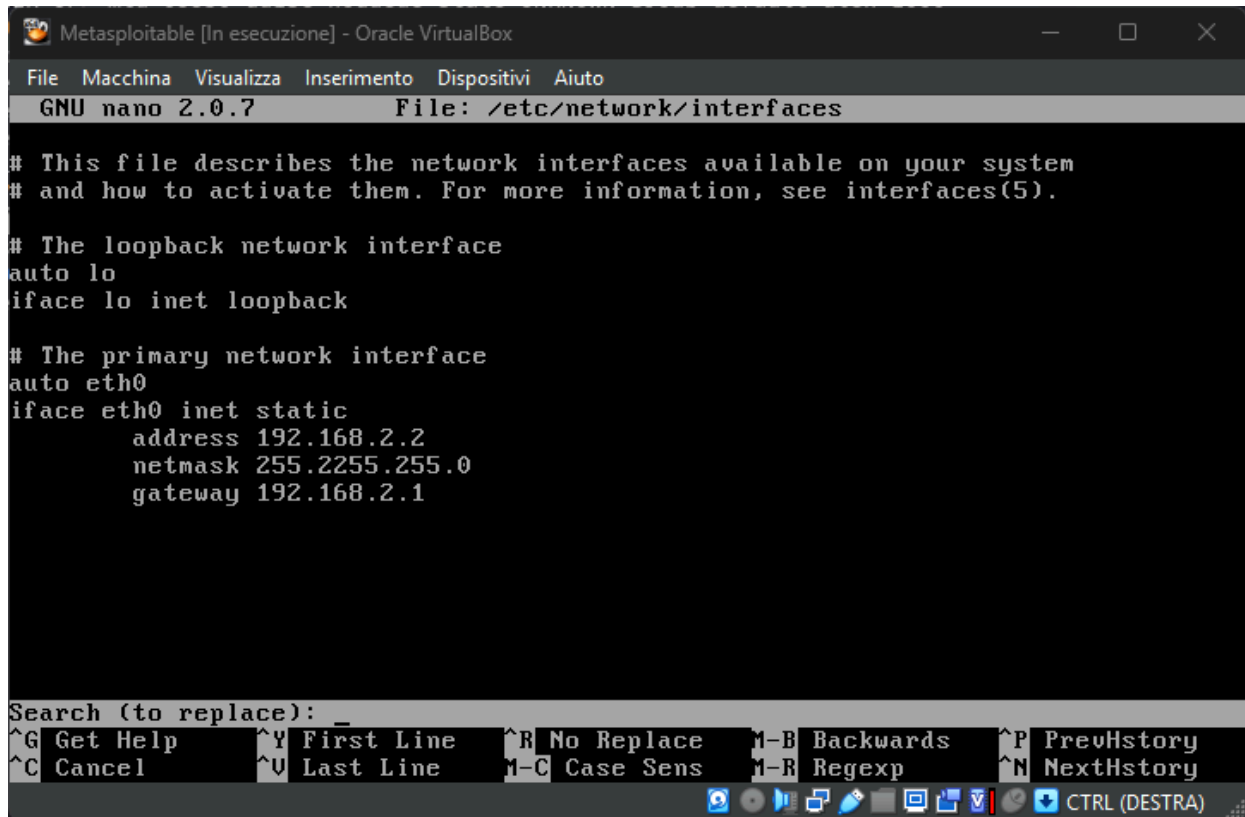
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet dhcp

[ Read 10 lines ]
^G Get Help  ^O WriteOut  ^R Read File  ^Y Prev Page  ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is   ^U Next Page  ^U UnCut Text ^T To Spel
```

Metasploitable è impostato su dhcp, il che non è quello che vogliamo dato che dobbiamo controllarlo quindi imposto su static e configuro a mio piacimento. Kali ha una sottorete 192.168.1.0, quindi ne imposto una con 192.168.2.0.



The screenshot shows a terminal window titled "Metasploitable [In esecuzione] - Oracle VirtualBox". The window displays the GNU nano 2.0.7 text editor editing the file /etc/network/interfaces. The file content is as follows:

```
# 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 192.168.2.2
    netmask 255.2255.255.0
    gateway 192.168.2.1
```

At the bottom of the terminal, there is a search bar with the text "Search (to replace): _" and a list of keyboard shortcuts for nano editor:

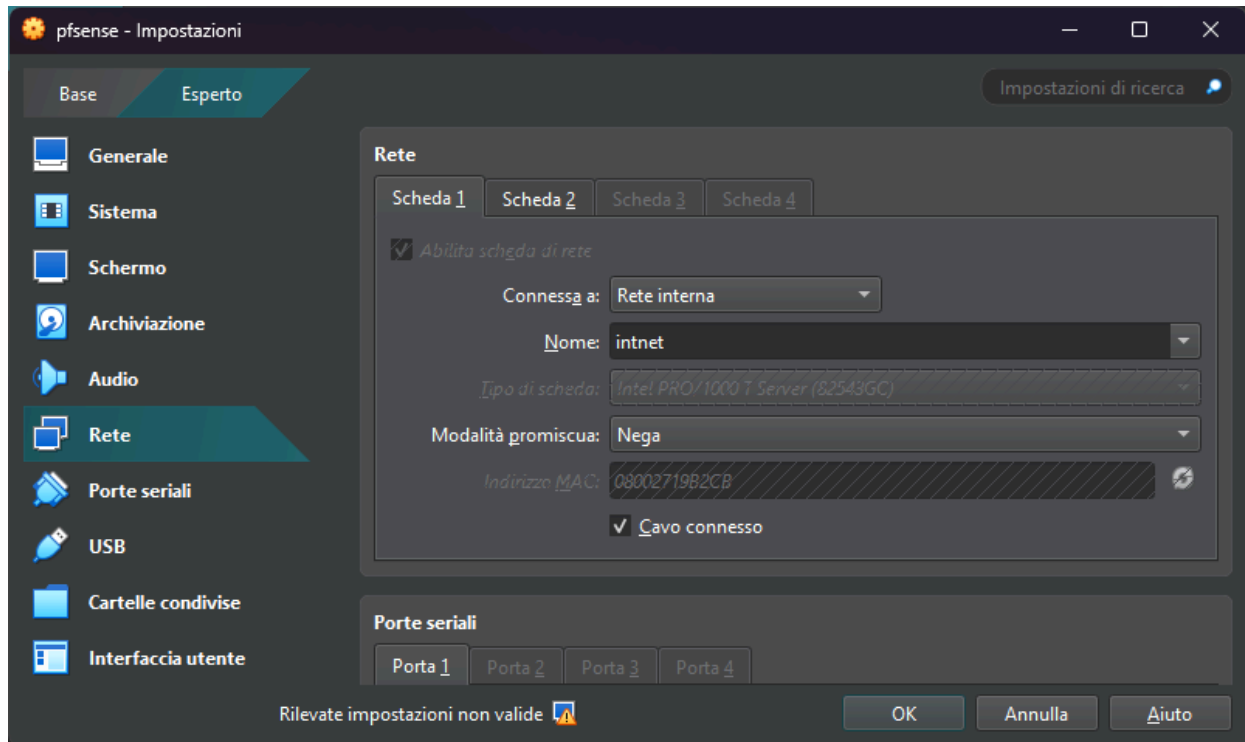
^G Get Help	^Y First Line	^R No Replace	M-B Backwards	^P PrevHistory
^C Cancel	^U Last Line	M-C Case Sens	M-R Regexp	^N NextHistory

The bottom of the window shows the Oracle VM VirtualBox taskbar with various icons and the text "CTRL (DESTRA)".

Riavvio Metasploitable e verifico il cambiamento di rete. Ora Metasploitable si trova in una sottorete diversa da quella di Kali.

3. Setup della Web GUI di pfSense

Dalle impostazioni di virtualbox aggiungo una nuova scheda di rete a Pfsense.



Entro nell'interfaccia web di PfSense su Firefox Kali e aggiungo la nuova interfaccia da assegnare a Metasploitable.

Interface	Network port
WAN	em0 (08:00:27:2d:53:25)
LAN	vtnet0 (08:00:27:96:49:83) Delete
OPT1	vtnet1 (08:00:27:1b:c2:e3) Delete

Dopodiché abilito l'interfaccia e la configuro.

Interfaces / OPT1 (vtnet1)

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) 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

Static IPv4 Configuration

IPv4 Address /

4. Testare le connessioni

Per testare le connessioni tra le macchine inizio eseguendo un comando di ping da Kali verso Pfense.

```
(kali@kali)-[~]
$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=0.253 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=0.208 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=0.228 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=64 time=0.219 ms
64 bytes from 192.168.1.1: icmp_seq=5 ttl=64 time=0.261 ms
64 bytes from 192.168.1.1: icmp_seq=6 ttl=64 time=0.254 ms
^C
— 192.168.1.1 ping statistics —
6 packets transmitted, 6 received, 0% packet loss, time 5113ms
rtt min/avg/max/mdev = 0.208/0.237/0.261/0.019 ms
```

Poi sempre da Kali eseguo un ping verso Metasploitable.

```
(kali㉿kali)-[~]  
$ ping 192.168.2.2  
PING 192.168.2.2 (192.168.2.2) 56(84) bytes of data.  
64 bytes from 192.168.2.2: icmp_seq=1 ttl=63 time=0.507 ms  
64 bytes from 192.168.2.2: icmp_seq=2 ttl=63 time=0.421 ms  
64 bytes from 192.168.2.2: icmp_seq=3 ttl=63 time=0.472 ms  
64 bytes from 192.168.2.2: icmp_seq=4 ttl=63 time=0.347 ms  
64 bytes from 192.168.2.2: icmp_seq=5 ttl=63 time=0.367 ms  
64 bytes from 192.168.2.2: icmp_seq=6 ttl=63 time=0.444 ms  
^C  
— 192.168.2.2 ping statistics —  
6 packets transmitted, 6 received, 0% packet loss, time 5104ms  
rtt min/avg/max/mdev = 0.347/0.426/0.507/0.055 ms
```

Infine da metasploitable eseguo un ping verso Kali e poi verso Pfsense.

```
msfadmin@metasploitable:~$ ping 192.168.1.5  
PING 192.168.1.5 (192.168.1.5) 56(84) bytes of data.  
  
--- 192.168.1.5 ping statistics ---  
4 packets transmitted, 0 received, 100% packet loss, time 3006ms  
  
msfadmin@metasploitable:~$ ping 192.168.1.1  
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.  
  
--- 192.168.1.1 ping statistics ---  
43 packets transmitted, 0 received, 100% packet loss, time 42006ms
```

Le connessioni funzionano correttamente.

5. Creazione regola firewall

Ora che ho configurato correttamente la rete devo bloccare l'accesso alla DVWA di Metasploitable da Kali. Per farlo, apro le regole del firewall dall'interfaccia web di Pfsense e seleziono la porta LAN, dove Kali si collega.

Firewall / Rules / LAN

Floating

WAN

LAN

OPT1

Rules (Drag to Change Order)

<div><div></div></div>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<div><div><div></div></div></div>	<div><div></div><div>✓</div><div>1/167 KiB</div></div>	<div>*</div>	<div>*</div>	<div>*</div>	<div>LAN Address</div>	<div>80</div>	<div>*</div>	<div>*</div>		<div>Anti-Lockout Rule</div>	<div><div></div></div>
<div><div><div></div></div></div>	<div><div></div><div>✓</div><div>0/1008 B</div></div>	<div>IPv4 *</div>	<div>LAN subnets</div>	<div>*</div>	<div>*</div>	<div>*</div>	<div>*</div>	<div>none</div>		<div>Default allow LAN to any rule</div>	<div><div></div><div></div><div></div><div></div><div></div><div></div></div>
<div><div><div></div></div></div>	<div><div></div><div>✓</div><div>0/0 B</div></div>	<div>IPv6 *</div>	<div>LAN subnets</div>	<div>*</div>	<div>*</div>	<div>*</div>	<div>*</div>	<div>none</div>		<div>Default allow LAN IPv6 to any rule</div>	<div><div></div><div></div><div></div><div></div><div></div><div></div></div>

Add

Add

Delete

Toggle

Copy

Save

Separator

Aggiungo una nuova regola in cima alla lista perché la regola di blocco deve venire necessariamente prima delle altre di accettazione, e inizio a configurarla. Su action seleziono Block, perché voglio bloccare una specifica connessione.

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 R

Come protocollo seleziono TCP, perché DVWA è una applicazione web, e HTTP utilizza il protocollo TCP.

Protocol

TCP

Choose which IP protocol this rule should match.

Alla sorgente indico la voce Address or Alias in modo da specificare l'indirizzo IP sorgente della richiesta.

Source			
Source	<input type="checkbox"/> Invert match	Address or Alias	192.168.1.5

Alla destinazione indico invece l'IP di metasploitable e come porta inserisco 80 dato che voglio bloccare l'accesso alla DVWA (applicazione web).

Destination				
Destination	<input type="checkbox"/> Invert match	Address or Alias	192.168.2.2	
Destination Port Range	HTTP (80)		HTTP (80)	
	From	Custom	To	Custom

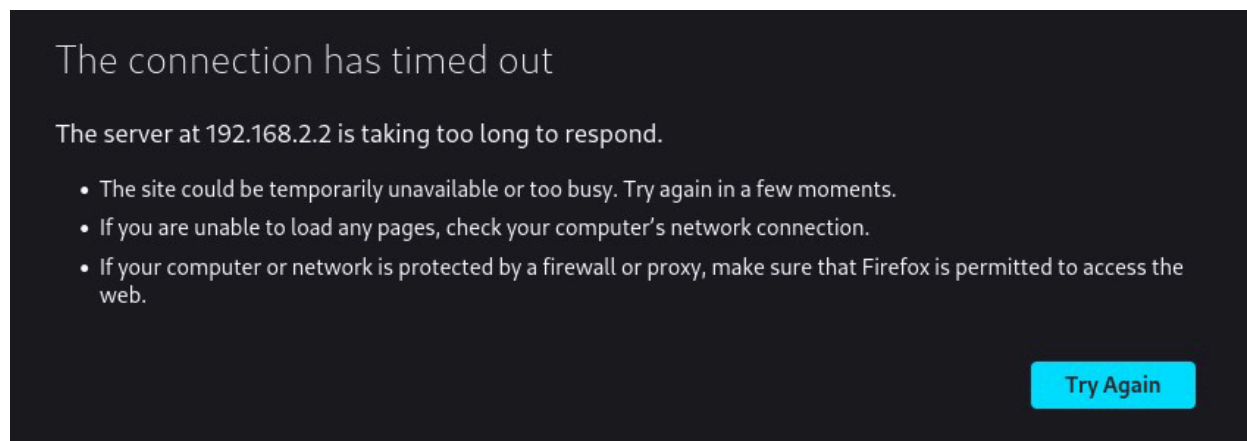
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Infine salvo e applico le modifiche. In cima alla lista troviamo la regola che abbiamo creato.

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	✓ 1/217 KiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	✗ 0/0 B	IPv4 TCP	192.168.1.5	*	192.168.2.2	80 (HTTP)	*	none			
<input type="checkbox"/>	✓ 0/1008 B	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>	✓ 0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

6. Verifica della regola

Per verificare che la regola applicata funzioni correttamente possiamo fare diverse cose. Ad esempio, cerco 192.168.2.2 sul web.



Come si vede il server non risponde quindi la richiesta è "timed out".

Oltre a questo possiamo eseguire un comando "nmap" da Kali per scansionare le porte di Metasploitable e vedere cosa succede con la porta 80.

```
(kali㉿kali)-[~]
$ nmap 192.168.2.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-13 07:22 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
th --dns-servers
Nmap scan report for 192.168.2.2
Host is up (0.021s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE    SERVICE
21/tcp    open    ftp
22/tcp    open    ssh
23/tcp    open    telnet
25/tcp    open    smtp
53/tcp    open    domain
80/tcp    filtered http
111/tcp   open    rpcbind
139/tcp   open    netbios-ssn
445/tcp   open    microsoft-ds
512/tcp   open    exec
513/tcp   open    login
514/tcp   open    shell
1099/tcp  open    rmiregistry
1524/tcp  open    ingreslock
2049/tcp  open    nfs
2121/tcp  open    ccproxy-ftp
3306/tcp  open    mysql
5432/tcp  open    postgresql
5900/tcp  open    vnc
6000/tcp  open    X11
6667/tcp  open    irc
8009/tcp  open    ajp13
8180/tcp  open    unknown

Nmap done: 1 IP address (1 host up) scanned in 1.32 seconds
```

Come si vede la porta 80 ci da stato “filtered”, significa che la regola del firewall funziona perfettamente.

7. Conclusione

Abbiamo visto come configurare una rete funzionante tra le varie macchine e che facesse in modo che la comunicazione passasse per pfsense. Abbiamo configurato pfsense e aggiunto una regola al firewall che andasse a bloccare una determinata e specifica comunicazione tra kali e metasploitable senza interferire con il resto del traffico. Saper applicare le regole del firewall può all’inizio sembrare difficile, ma una volta capito il senso di ogni singolo parametro diventa fluido e intuitivo.