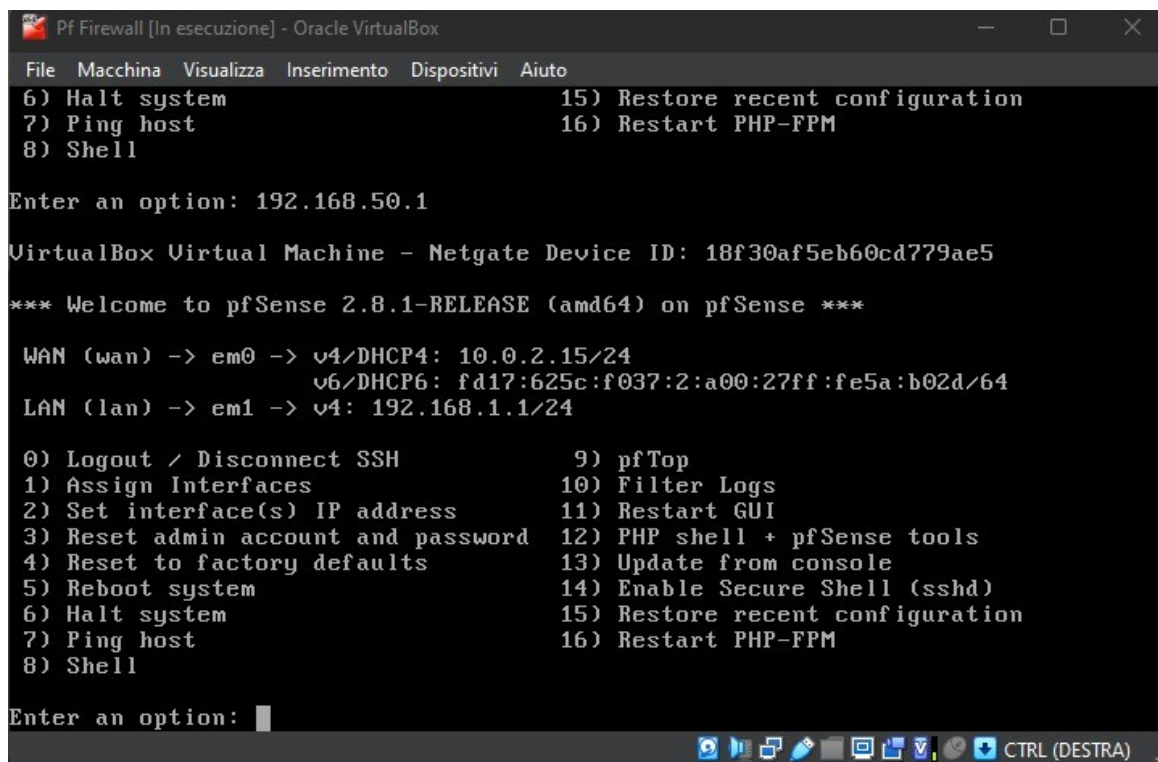
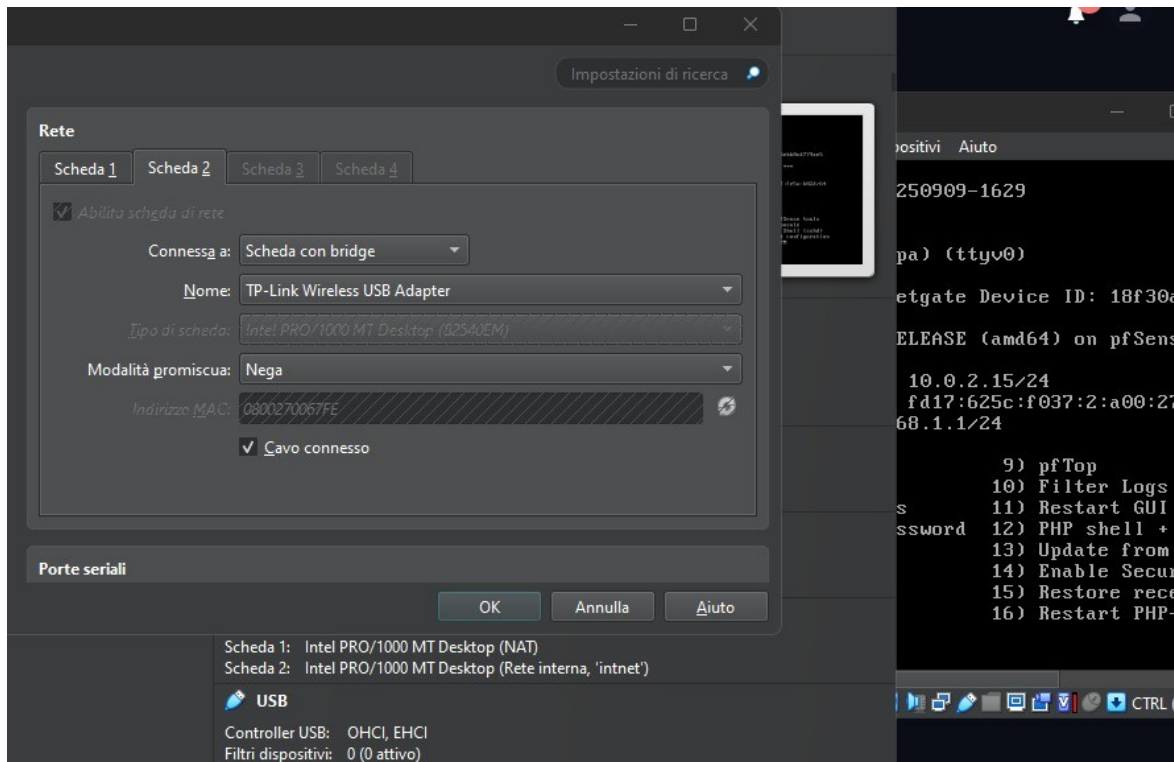
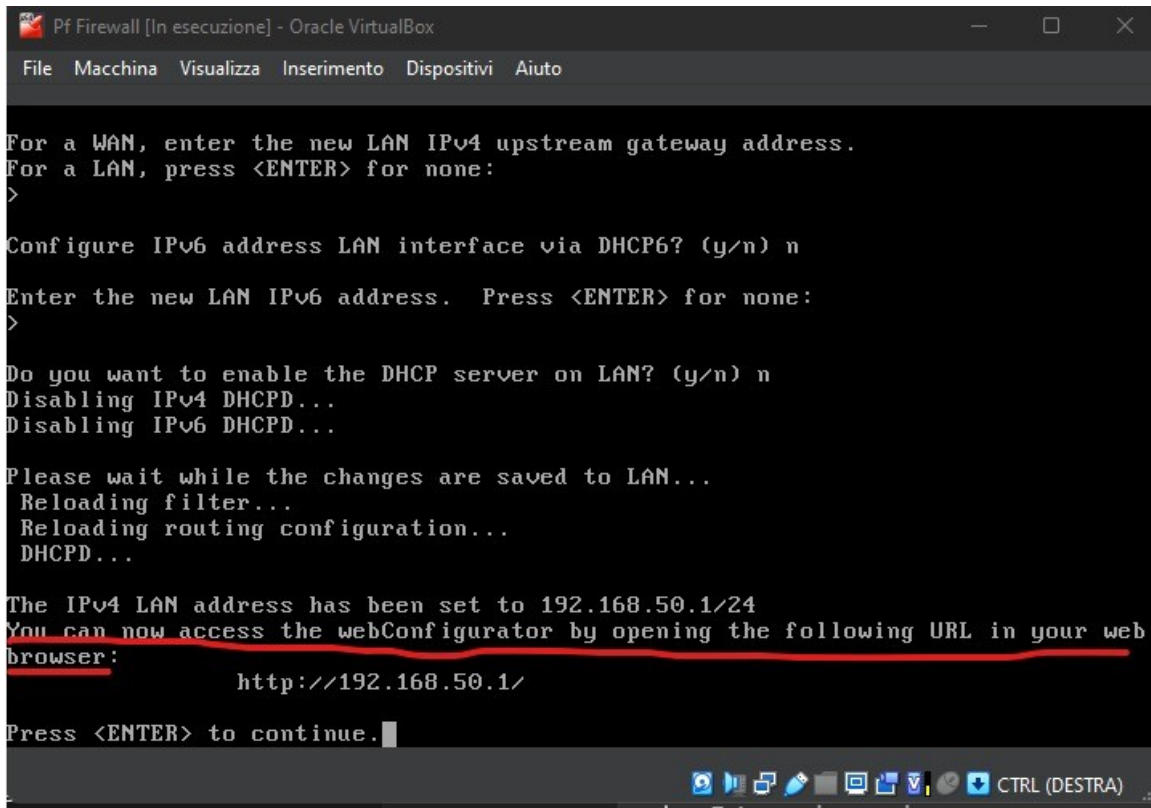


W9D4 – FRANCESCO MONTALTO

1. Innanzitutto ho cambiato la scheda di Rete 2 in “scheda con Bridge”, ed ho riavviato PFSense.



2. Tramite la procedura al tasto 2 (quella di assegnazione di interfacce ed IP), ho cambiato l'IP in Lan in "192.168.50.1", come visibile dall'immagine. Poi ho verificato, tramite procedura ping, l'effettiva connessione tra le mie due macchine PFSense e Kali.



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

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

Configure IPv6 address LAN interface via DHCP6? (y/n) n

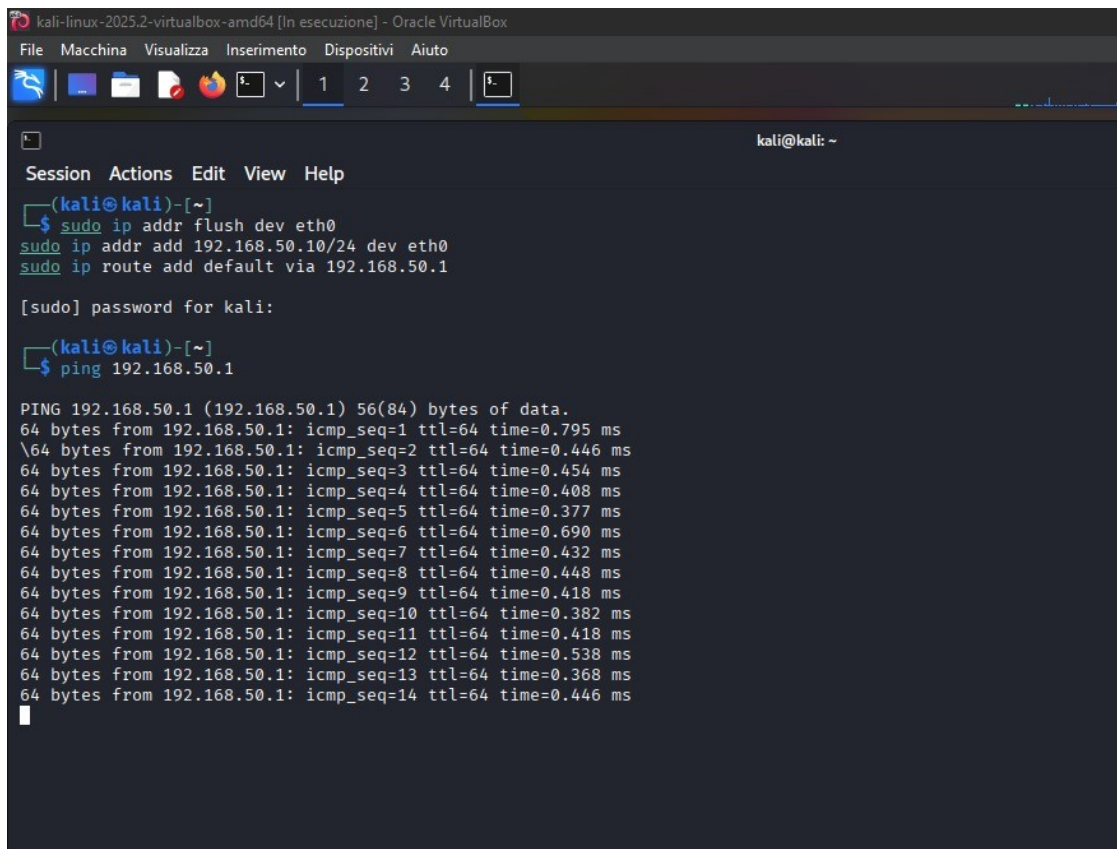
Enter the new LAN IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) n
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

Please wait while the changes are saved to LAN...
Reloading filter...
Reloading routing configuration...
DHCPD...

The IPv4 LAN address has been set to 192.168.50.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
    http://192.168.50.1/

Press <ENTER> to continue.
```



```
kali-linux-2025.2-virtualbox-amd64 [In esecuzione] - Oracle VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

kali@kali: ~
Session  Actions  Edit  View  Help

(kali@kali)-[~]
└─$ sudo ip addr flush dev eth0
sudo ip addr add 192.168.50.10/24 dev eth0
sudo ip route add default via 192.168.50.1

[sudo] password for kali:

(kali@kali)-[~]
└─$ ping 192.168.50.1

PING 192.168.50.1 (192.168.50.1) 56(84) bytes of data.
64 bytes from 192.168.50.1: icmp_seq=1 ttl=64 time=0.795 ms
64 bytes from 192.168.50.1: icmp_seq=2 ttl=64 time=0.446 ms
64 bytes from 192.168.50.1: icmp_seq=3 ttl=64 time=0.454 ms
64 bytes from 192.168.50.1: icmp_seq=4 ttl=64 time=0.408 ms
64 bytes from 192.168.50.1: icmp_seq=5 ttl=64 time=0.377 ms
64 bytes from 192.168.50.1: icmp_seq=6 ttl=64 time=0.690 ms
64 bytes from 192.168.50.1: icmp_seq=7 ttl=64 time=0.432 ms
64 bytes from 192.168.50.1: icmp_seq=8 ttl=64 time=0.448 ms
64 bytes from 192.168.50.1: icmp_seq=9 ttl=64 time=0.418 ms
64 bytes from 192.168.50.1: icmp_seq=10 ttl=64 time=0.382 ms
64 bytes from 192.168.50.1: icmp_seq=11 ttl=64 time=0.418 ms
64 bytes from 192.168.50.1: icmp_seq=12 ttl=64 time=0.538 ms
64 bytes from 192.168.50.1: icmp_seq=13 ttl=64 time=0.368 ms
64 bytes from 192.168.50.1: icmp_seq=14 ttl=64 time=0.446 ms
```

3. Sono entrato ed ho potuto iniziare la configurazione Web Gui.



SIGN IN

Username

Password

SIGN IN

pfSense is developed and maintained by Netgate. © ESF 2004 - 2025 [View license](#).

Status / Dashboard

System Information

Name	pfSense.home.arpa
User	admin@192.168.50.10 (Local Database)
System	VirtualBox Virtual Machine Netgate Device ID: 18f30af5eb60cd779ae5
BIOS	Vendor: innotek GmbH Version: VirtualBox Release Date: Fri Dec 1 2006 Boot Method: BIOS
Version	2.8.1-RELEASE (amd64) built on Tue Sep 9 16:29:00 UTC 2025 FreeBSD 15.0-CURRENT The system is on the latest version. Version information updated at Fri Sep 12 20:40:36 UTC 2025
CPU Type	Intel(R) Core(TM) i7-3770 CPU @ 3.40GHz AES-NI CPU Crypto: Yes (inactive)

Netgate Services And Support

Contract type Community Support
Community Support Only

NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES

If you purchased your pfSense gateway firewall appliance from Netgate and elected **Community Support** at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the [NETGATE RESOURCE LIBRARY](#).

You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.

[Upgrade Your Support](#)

[Community Support Resources](#)

[Netgate Global Support FAQ](#)

[Official pfSense Training by Netgate](#)

4. Poi ho proceduto alla creazione della policy. Per creare la regola del Firewall, dall'interfaccia sopracitata, sono andato su "Firewall", "Rules", "LAN", e poi "Add", quel tasto verde con la freccia all'insù.

Firewall / Rules / LAN

Floating WAN LAN

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	5/1.43 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
<input checked="" type="checkbox"/>	1/195 KiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
<input checked="" type="checkbox"/>	0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Add Add Delete Toggle Copy Save Separator

In questo caso ho solo modificato la voce Protocol in "Any".

Edit Firewall Rule

Action

Pass

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) whereas with block the packet is dropped silently. In either case, the original packet is not sent.

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

Any

Choose which IP protocol this rule should match.

Source

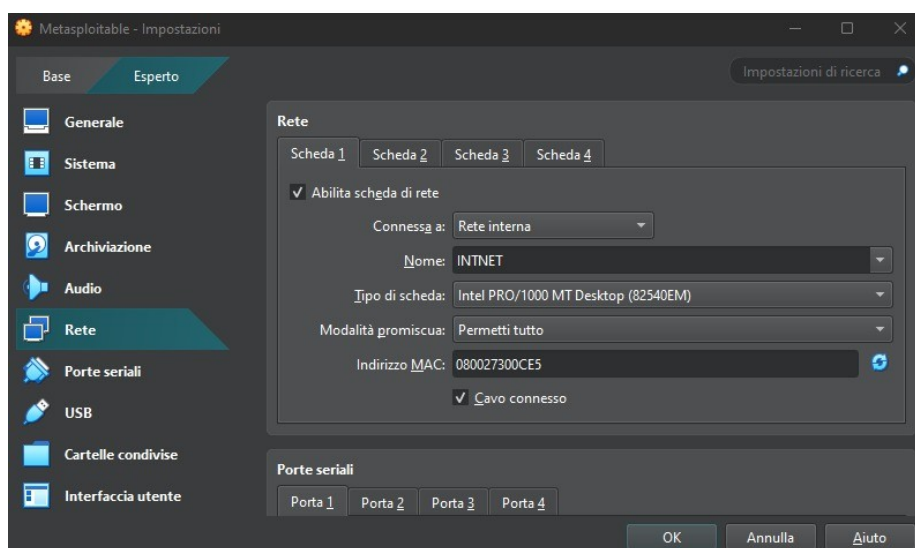
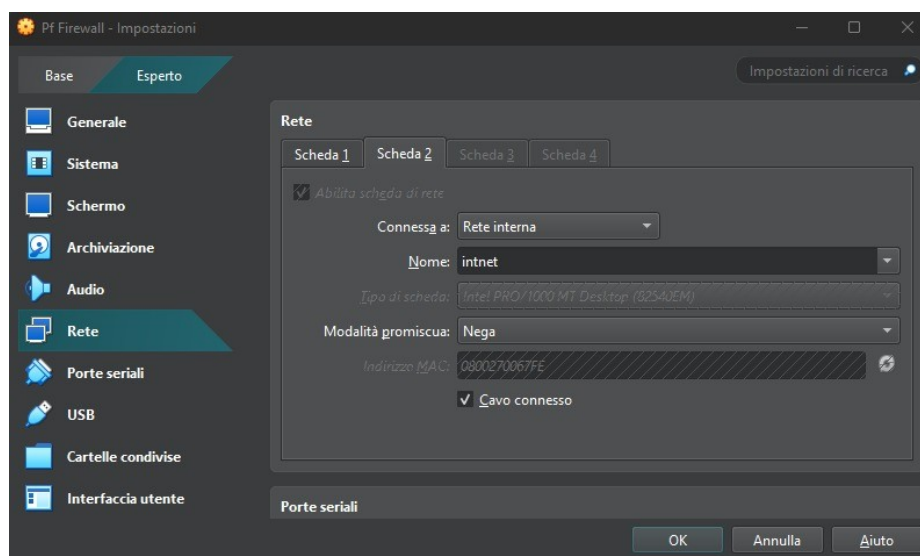
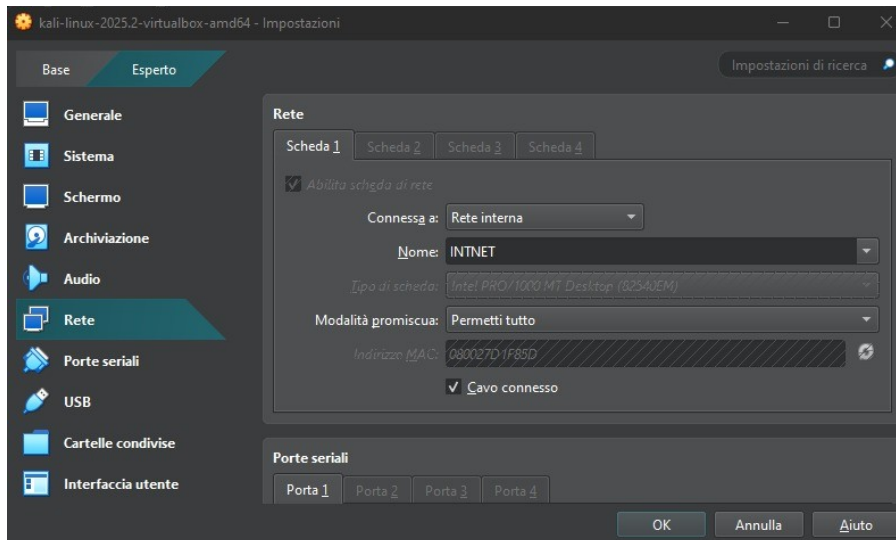
Source

☐ Invert match

Any

5. ESERCIZIO PFSense: Da qui, l'obiettivo è stato creare una regola FireWall ai fini di bloccare l'accesso alla DVWA su Meta, addentrandomi nell'esercizio vero e proprio.

Innanzitutto ho impostato Kali Linux, Metasploitable e PFSense sulla stessa rete, a medesimo nome, come visibile negli screen.



6. Mi sono recato, tramite la pagina di configurazione, su “Interfaces” e “LAN”.

pfsense
COMMUNITY EDITION

System ▾

Interfaces ▾

Firewall ▾

Services ▾

VPN ▾

Status ▾

WARNING:
The password for this account is insecure. Password is currently set to the default value (pfsense).
[Change the password as soon as possible.](#)

Interfaces / LAN (em1)

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

Interfaces / OPT1 (em1.1)

General Configuration

Enable

☐ Enable interface

Description

OPT1

Enter a description (name) for the interface here.

IPv4 Configuration Type

None ▾

IPv6 Configuration Type

None ▾

MAC Address

XX:XX:XX:XX:XX:XX

The MAC address of a VLAN interface must be set on its parent interface

MTU

If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can va

MSS

If a value is entered in this field, then MSS clamping for TCP connections to the value entered abc

Ho poi configurato l'interfaccia, in modo da assicurare il collegamento a PFSense.

Enable	<input checked="" type="checkbox"/> Enable interface
Description	<input type="text" value="LAN"/> Enter a description (name) for the interface here.
IPv4 Configuration Type	<input type="text" value="Static IPv4"/>
IPv6 Configuration Type	<input type="text" value="None"/>
MAC Address	<input type="text" value="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	<input type="text"/> If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can
MSS	<input type="text"/> If a value is entered in this field, then MSS clamping for TCP connections to the value entered a minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.
Speed and Duplex	<input type="text" value="Default (no preference, typically autoselect)"/> Explicitly set speed and duplex mode for this interface.

E mi sono assicurato dell'IP, nuovamente.

The screenshot shows the PFSense web interface in a browser window. The address bar shows the URL `192.168.50.1/interfaces.php?if=opt1`. The browser's tab bar includes several tabs for Kali Linux, Kali Tools, OffSec, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, and Google Hacking DB. The main content area is divided into sections for MTU, MSS, Speed and Duplex, and Static IPv4 Configuration. The MTU, MSS, and Speed and Duplex sections are collapsed. The Static IPv4 Configuration section is expanded, showing the IPv4 Address set to `192.168.100.1` with a subnet mask of `/24`. The IPv4 Upstream gateway is set to `None`, and there is a green button labeled `+ Add a new gateway`. Below the gateway selection, there is explanatory text about selecting an upstream gateway for Internet connections versus local area networks, and a link to manage gateways.

MTU	<input type="text"/> 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	<input type="text"/> 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	<input type="text" value="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	<input type="text" value="192.168.100.1"/> / <input type="text" value="24"/>
IPv4 Upstream gateway	<input type="text" value="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 .

Ho poi abilitato il DHCP sulla LAN, Il DHCP di pfSense assegna automaticamente un IP valido nella subnet LAN. In questo modo Kali può comunicare con pfSense e tentare l'accesso alla DMZ, permettendo di testare le regole firewall create.

Services / DHCP Server / LAN

ISC DHCP has reached end-of-life and will be removed in a future version of pfSense. Visit [System > Advanced > Networking](#) to switch DHCP back to ISC DHCP.

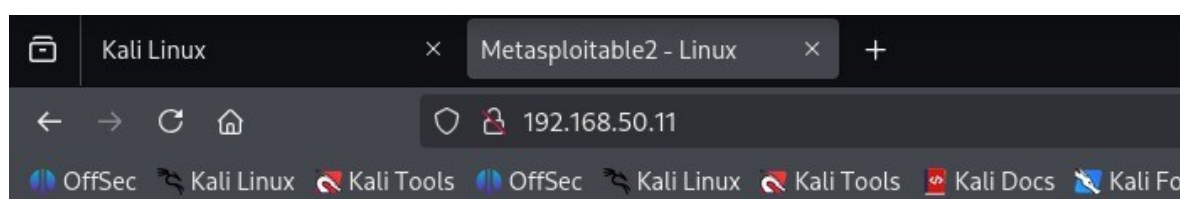
LAN DMZ

General Settings

DHCP Backend	ISC DHCP
Enable	<input checked="" type="checkbox"/> Enable DHCP server on LAN interface
BOOTP	<input type="checkbox"/> Ignore BOOTP queries
Deny Unknown Clients	<div>Allow all clients</div> <div>When set to Allow all clients, any DHCP client will get an IP address within this scope/range on this interface. If set to Interface, any DHCP client with a MAC address listed in a static mapping on any scope(s)/interface(s) will get an IP address. If set to Interface, only MAC addresses listed in static mappings on this interface will get an IP address.</div>

7. Ho successivamente verificato la corrispondenza tra Kali Linux e Metasploitable.
Ho pingato sul terminale l'IP di Metasploitable, ed ho confermato anche attraverso la DVWA

```
kali@kali
Session Actions Edit View Help
(kali@kali)-[~]
$ ping 192.168.50.11
PING 192.168.50.11 (192.168.50.11) 56(84) bytes of data.
64 bytes from 192.168.50.11: icmp_seq=1 ttl=64 time=0.629 ms
64 bytes from 192.168.50.11: icmp_seq=2 ttl=64 time=0.372 ms
64 bytes from 192.168.50.11: icmp_seq=3 ttl=64 time=0.333 ms
64 bytes from 192.168.50.11: icmp_seq=4 ttl=64 time=0.307 ms
64 bytes from 192.168.50.11: icmp_seq=5 ttl=64 time=0.328 ms
64 bytes from 192.168.50.11: icmp_seq=6 ttl=64 time=0.410 ms
64 bytes from 192.168.50.11: icmp_seq=7 ttl=64 time=0.285 ms
64 bytes from 192.168.50.11: icmp_seq=8 ttl=64 time=0.292 ms
64 bytes from 192.168.50.11: icmp_seq=9 ttl=64 time=0.342 ms
64 bytes from 192.168.50.11: icmp_seq=10 ttl=64 time=0.349 ms
64 bytes from 192.168.50.11: icmp_seq=11 ttl=64 time=0.265 ms
```



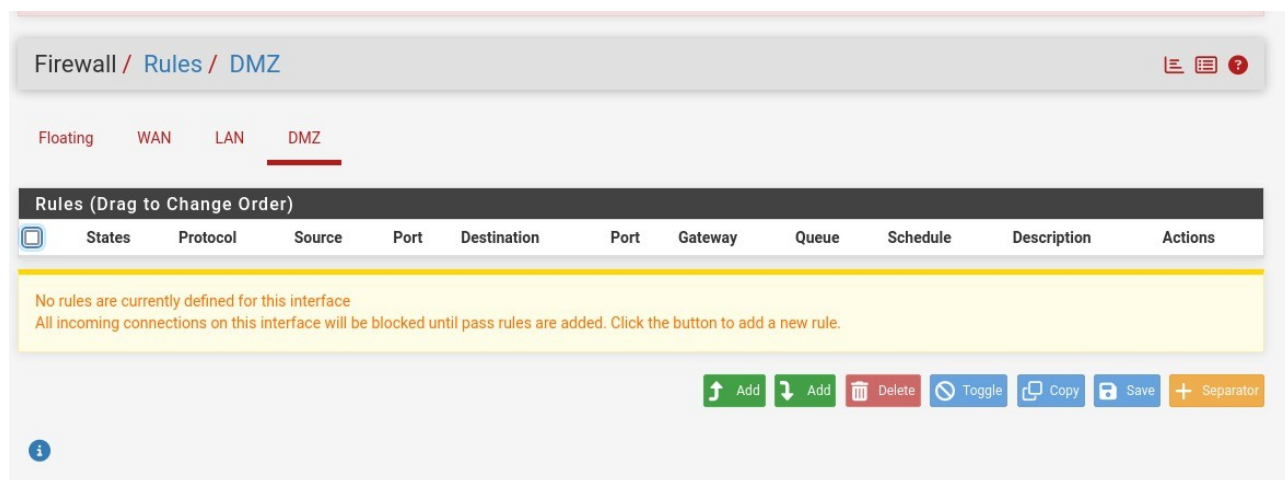
Warning: Never expose this VM to an untrusted network!

Contact: [msfdev\[at\]metasploit.com](mailto:msfdev[at]metasploit.com)

Login with msfadmin/msfadmin to get started

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

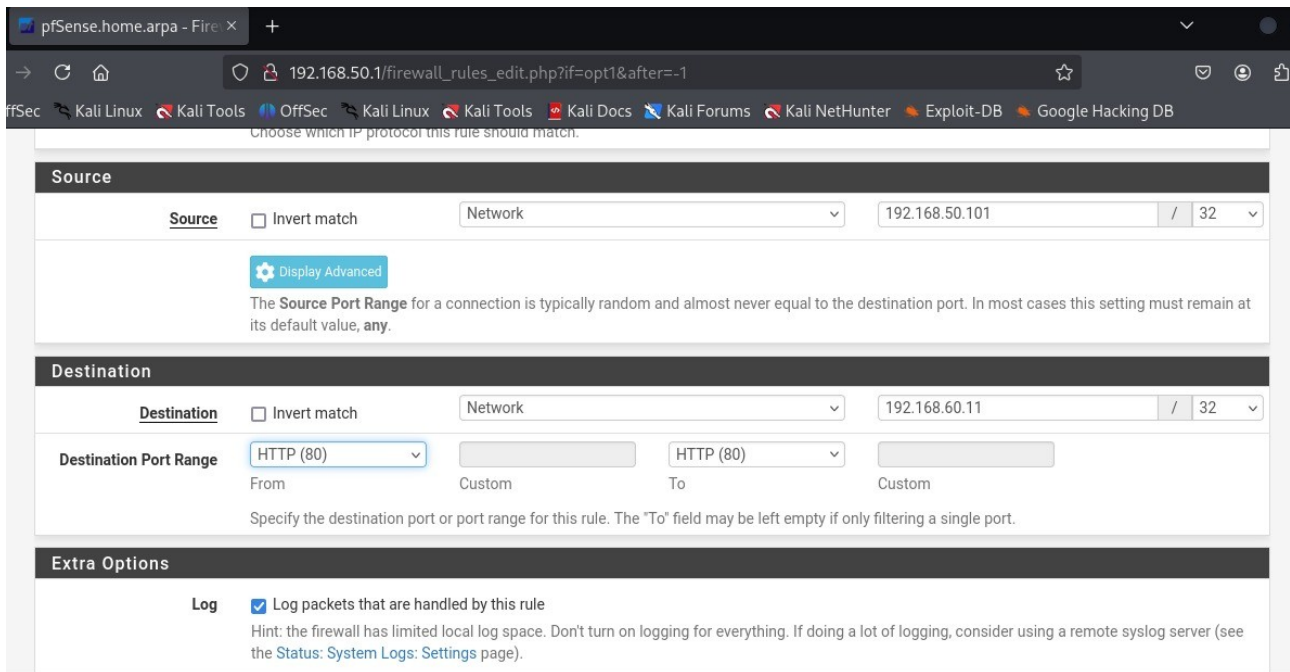
8. Mi sono poi recato nuovamente nella home di PFSense, sui setting delle regole dei Firewall. Da qui, semplicemente, ho selezionato “Add”, ed ho proceduto a creare una nuova regola.



Ho scelto l’opzione “Block”, sulla tendina Action, lasciando il resto come l’ho trovato.

The screenshot shows the 'Edit Firewall Rule' form. It has several sections with labels and dropdown menus: 'Action' is set to 'Block' with a hint: '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 re... whereas with block the packet is dropped silently. In either case, the original packet is discarded.'; 'Disabled' has a checkbox 'Disable this rule' with the text 'Set this option to disable this rule without removing it from the list.'; 'Interface' is set to 'DMZ' with the text 'Choose the interface from which packets must come to match this rule.'; 'Address Family' is set to 'IPv4' with the text 'Select the Internet Protocol version this rule applies to.'; 'Protocol' is set to 'TCP' with the text 'Choose which IP protocol this rule should match.' Below these is a section titled 'Source' with a label 'Source', a checkbox 'Invert match', a dropdown menu set to 'Any', and a text input field containing 'Source Address'.

Ho poi impostato Source e Destination su “Network”, inserendo i relativi IP di Kali e Metasploitable, equivalendo “/32” ad Host singolo. Ho poi abilitato il Log, in modo da mostrare i pacchetti TCP verso Metasploitable/DVWA bloccati dalla regola.



pfSense.home.arpa - Fire X +

→ ↻ 🏠 192.168.50.1/firewall_rules_edit.php?if=opt1&after=-1 ☆ 🔒 📄

ffSec Kali Linux Kali Tools OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

Choose which IP protocol this rule should match.

Source

Source ☐ Invert match Network 192.168.50.101 / 32

[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 Network 192.168.60.11 / 32

Destination Port Range 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.

Extra Options

Log ☒ Log packets that are handled by this rule

Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

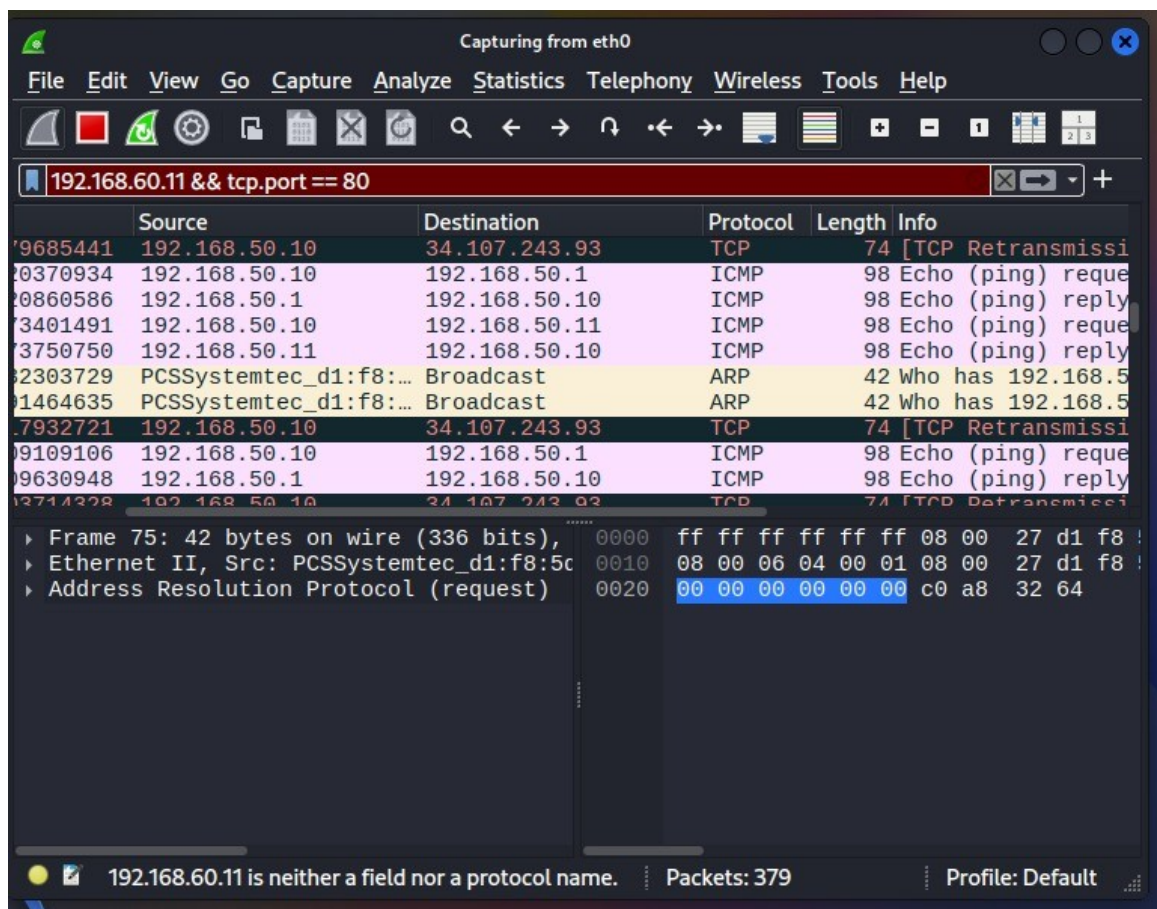
9: VERIFICA DEL BLOCCO D'ACCESSO.

Ho innanzitutto visionato i tentativi di connessione di Wireshark

Sono visibili i pacchetti TCP rossi. Sono i pacchetti inviati da Kali verso Metasploitable sulla porta 80. La dicitura "Retransmission" indica che Kali non riceve risposta e ritenta più volte.

Questo è esattamente ciò che ci aspettiamo quando il firewall blocca il traffico TCP sulla porta 80.

Poi vediamo anche i pacchetti ICMP, in rosa (Echo ping request/reply). Sono pacchetti di ping inviati da Kali e le eventuali risposte. Nulla di allarmante: confermano che la macchina Metasploitable è raggiungibile in rete, ma non sulla porta 80. Inoltre, possiamo anche notare una totale assenza di SYN/ACK.

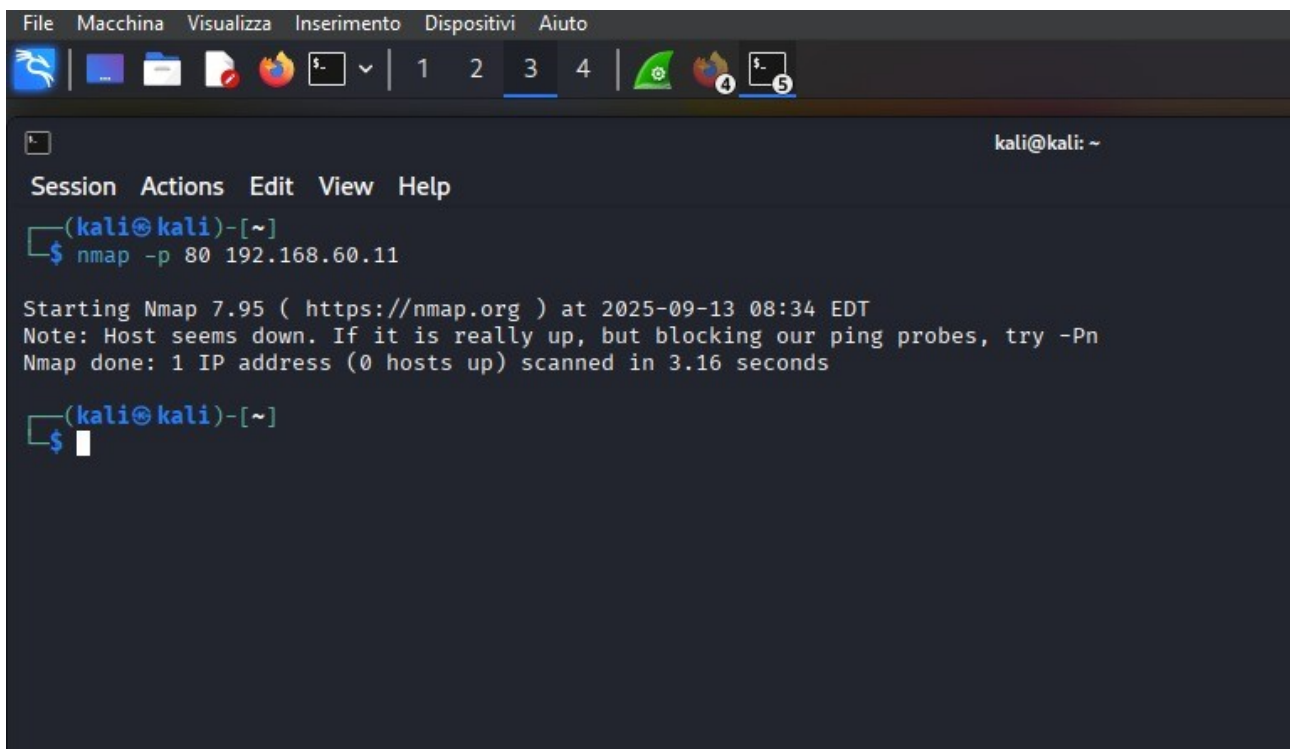


9. Verifica tramite Nmap. Per questa verifica ho fatto un test sia a regola assente che a regola attiva, per vedere la differenza.

PRIMA DELLA REGOLA

```
(kali㉿kali)-[~]  
$ nmap -Pn -p 80 192.168.60.11  
  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-13 08:39 EDT  
Nmap scan report for 192.168.60.11  
Host is up.  
  
PORT      STATE      SERVICE  
80/tcp    filtered  http  
  
Nmap done: 1 IP address (1 host up) scanned in 2.20 seconds
```

DOPO LA REGOLA



```
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto  
[Icons]  
  
kali@kali: ~  
Session  Actions  Edit  View  Help  
  
(kali㉿kali)-[~]  
$ nmap -p 80 192.168.60.11  
  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-13 08:34 EDT  
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn  
Nmap done: 1 IP address (0 hosts up) scanned in 3.16 seconds  
  
(kali㉿kali)-[~]  
$
```

Come visibile dal PORT STATE SERVICE, un'altra conferma della riuscita del blocco.

