

Report esercitazione con PfSense W9D4

In questo esercizio dovremo creare una regola per cui vengano bloccate le comunicazioni sulla porta 80 da Kali verso la DVWA di Metasploitable 2.

Prerequisiti:

- Installazione e configurazione dell'immagine di PfSense;
- Assicurarsi che Kali sia su rete interna;
- Configurazione di un IP statico sulla macchina Kali (nel nostro caso sarà 192.168.50.106);
- La vm di PfSense deve essere in esecuzione durante l'esercizio.

Step 1 Accediamo all'homepage di PfSense dal browser di Kali, spostiamoci su Interfaces/ Interfaces assignments e creiamo una nuova interfaccia, chiamiamola LAN2 ed assegnamo un IPv4 con una subnet diversa da quella di Kali (nel nostro caso sarà 192.168.51.1/24). È importante ricordare che dopo ogni modifica apportata a PfSense, bisognerà confermarla tramite un tasto su un banner che apparirà a schermo, altrimenti la modifica non verrà apportata.

Interfaces / LAN2 (em2)

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: xxxxxxxxxx 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.

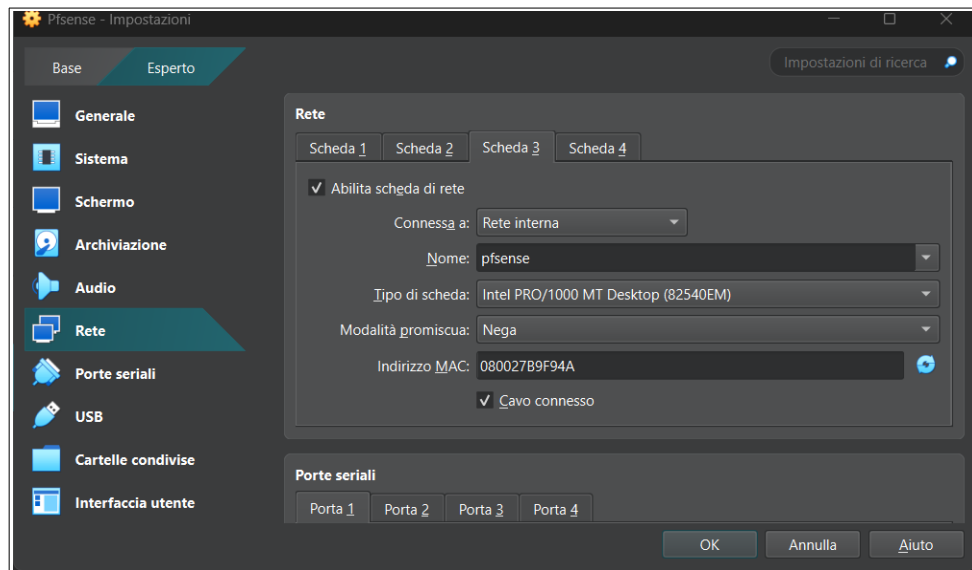
Speed and Duplex
Explicitly set speed and duplex mode for this interface.
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

Static IPv4 Configuration

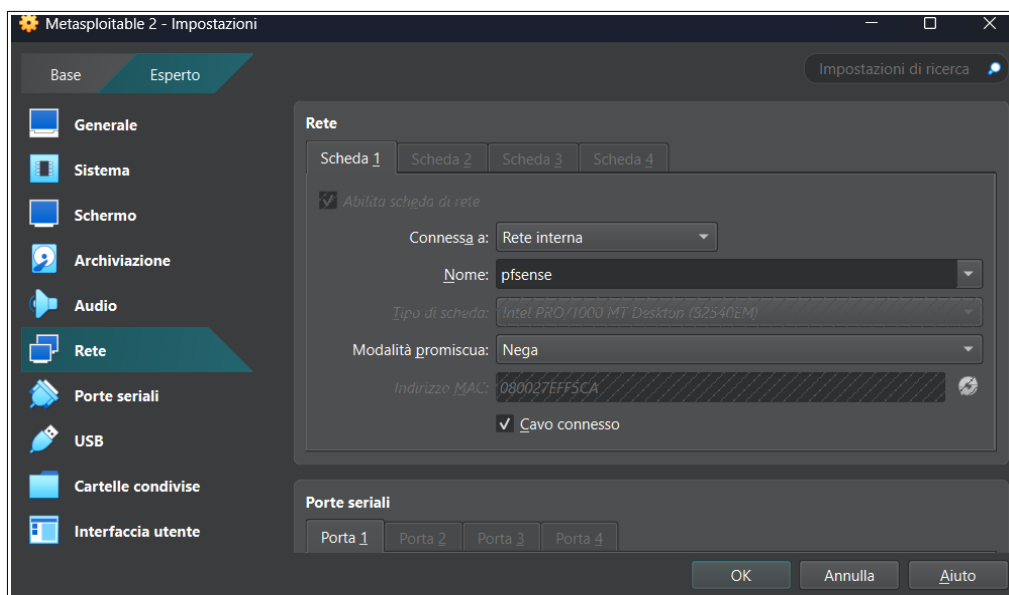
IPv4 Address /

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".

Step 2 Spostiamoci momentaneamente sulle impostazioni di Virtual box ed assegnamo alla VM di PfSense una nuova scheda di rete, impostiamola su internal e diamo il nome alla rete in modo che sia facilmente riconoscibile.



Step 3 Dalle impostazioni di Virtual Box di Metasploitable 2 impostiamo anche in questo caso la rete interna (nominandola come fatto in precedenza).



Step 4 Dalla GUI di PfSense, spostiamoci su Services/ DHCP Server/ LAN2 ed abilitiamo il servizio DHCP su un range di IP che comprenderà anche l'IP assegnato a Metasploitable 2.

The screenshot shows the pfSense web interface for the DHCP Server configuration on the LAN2 interface. At the top, there is a breadcrumb trail: Services / DHCP Server / LAN2. Below this, a yellow warning box states: "ISC DHCP has reached end-of-life and will be removed in a future version of pfSense. Visit System > Advanced > Networking to switch DHCP backend." The interface has two tabs: LAN and LAN2, with LAN2 selected. The configuration is divided into two main sections: General Settings and Primary Address Pool.

General Settings

- DHCP Backend:** ISC DHCP
- Enable:** ☒ Enable DHCP server on LAN2 interface
- BOOTP:** ☐ Ignore BOOTP queries
- Deny Unknown Clients:** ☐ Deny unknown clients. The dropdown menu is set to "Allow all clients".
When set to **Allow all clients**, any DHCP client will get an IP address within this scope/range on this interface. If set to **Allow known clients from any 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 **Allow known clients from only this interface**, only MAC addresses listed in static mappings on this interface will get an IP address within this scope/range.
- Ignore Denied Clients:** ☐ Ignore denied clients rather than reject
This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.
- Ignore Client Identifiers:** ☐ Do not record a unique identifier (UID) in client lease data if present in the client DHCP request
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.

Primary Address Pool

- Subnet:** 192.168.51.0/24
- Subnet Range:** 192.168.51.1 - 192.168.51.254
- Address Pool Range:** From 192.168.51.100 To 192.168.51.200
The specified range for this pool must not be within the range configured on any other address pool for this interface.
- Additional Pools:** + Add Address Pool

Step 5 Avviamo la VM di Metasploitable 2 e tramite il comando `sudo nano /etc/network/interfaces`, assegnamo il DHCP, e commentiamo tutte le righe sottostanti.

```
GNU nano 2.0.7      File: /etc/network/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 dhcp
#address 192.168.51.101
#netmask 255.255.255.0
#network 192.168.51.0
#broadcast 192.168.51.255
#gateway 192.168.51.1

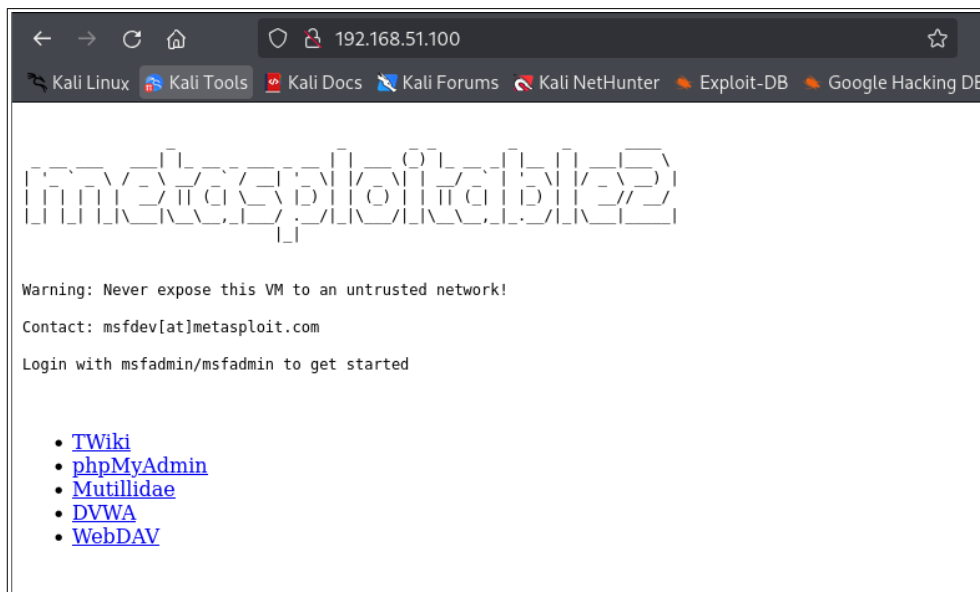
^G Get Help  ^O WriteOut  ^R Read File  ^Y Prev Page  ^K Cut Text   ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page  ^U UnCut Text ^T To Spell
```

Step 6 Diamo il comando ifconfig da Metasploitable 2 per controllare l'IP.

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:ef:f5:ca
          inet addr:192.168.51.100  Bcast:192.168.51.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feef:f5ca/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:190 errors:0 dropped:0 overruns:0 frame:0
          TX packets:219 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:26930 (26.2 KB)  TX bytes:64277 (62.7 KB)
          Base address:0xd020 Memory:f0200000-f0220000
```

Step 7 Controllare la connettività da Kali verso Metasploitable 2 tramite test di ping e tramite browser da Kali.

```
(kali㉿kali)-[~]
$ ping 192.168.51.100
PING 192.168.51.100 (192.168.51.100) 56(84) bytes of data.
64 bytes from 192.168.51.100: icmp_seq=1 ttl=63 time=5.65 ms
64 bytes from 192.168.51.100: icmp_seq=2 ttl=63 time=3.17 ms
64 bytes from 192.168.51.100: icmp_seq=3 ttl=63 time=3.51 ms
64 bytes from 192.168.51.100: icmp_seq=4 ttl=63 time=8.70 ms
64 bytes from 192.168.51.100: icmp_seq=5 ttl=63 time=7.34 ms
^C
— 192.168.51.100 ping statistics —
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 3.165/5.671/8.696/2.140 ms
```



Step 8 Possiamo finalmente spostarci sulla GUI di PfSense e da Firewall/ Rules/ LAN, possiamo creare una nuova regola che blocchi il traffico sulla porta 80 da Kali a Metasploitable 2. Come source IP impostiamo quello di Kali e come destination quello di Metasploitable 2, abilitiamo i log che ci serviranno in seguito.

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.

Source
Source ☐ Invert match Address or Alias 192.168.50.106 /
[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 192.168.51.100 /
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).

Step 9 Le regole del firewall hanno un approccio top-down, sarà quindi nostra cura assegnare la giusta posizione alla regola perché possa entrare in funzione correttamente.

Firewall / Rules / LAN

The changes have been applied successfully. The firewall rules are now reloading in the background.
[Monitor the filter reload progress.](#)

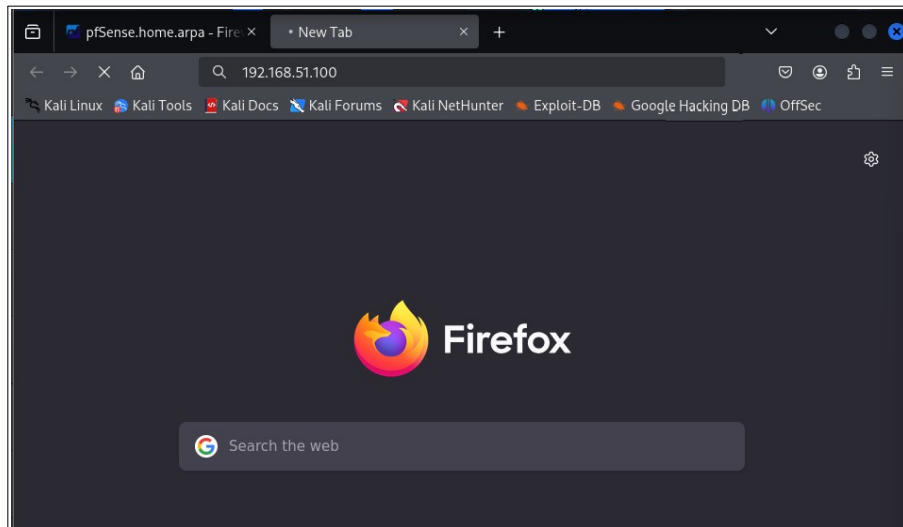
Floating WAN LAN LAN2

Rules (Drag to Change Order)

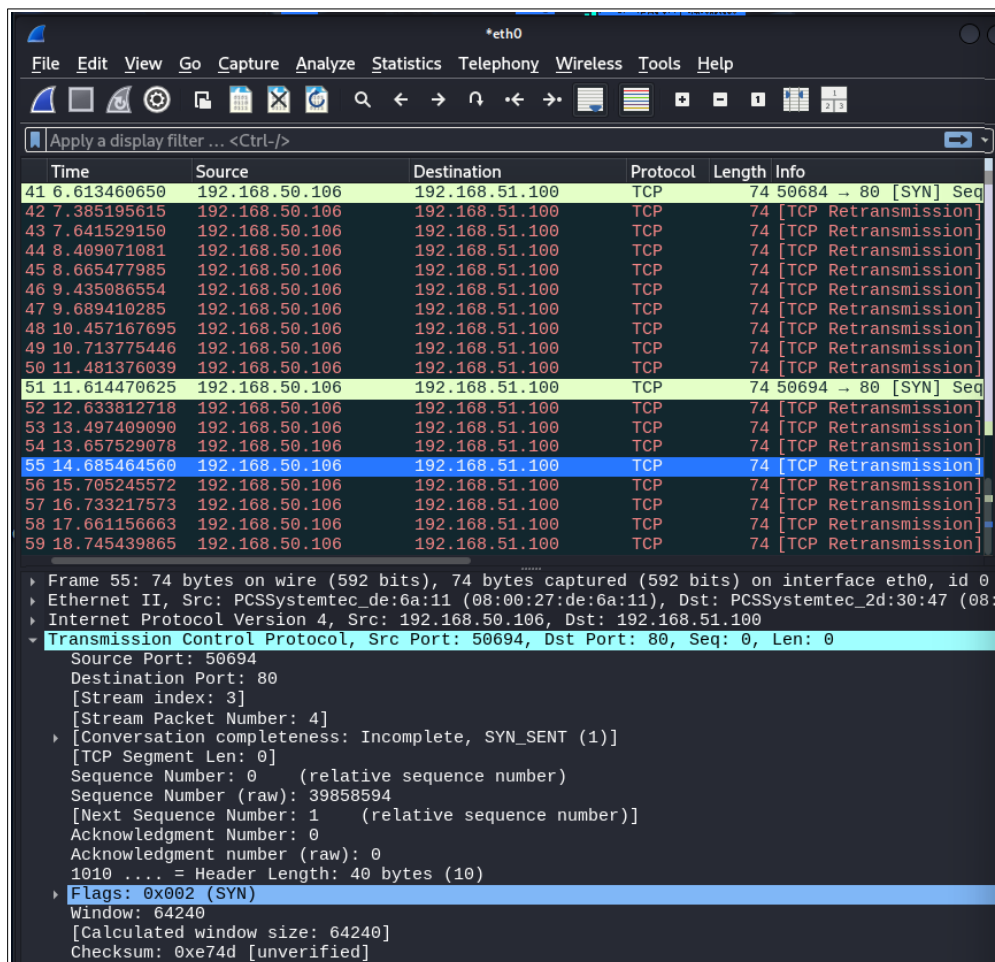
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	✓ 0/685 KiB	*	*	*	LAN Address	443 80	*	*	*	Anti-Lockout Rule	
<input type="checkbox"/>	✗ 0/0 B	IPv4 TCP	192.168.50.106	*	192.168.51.100	80 (HTTP)	*	none		block DVWA from Kali	
<input checked="" type="checkbox"/>	✓ 0/2.57 MiB	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

Step 10 Una volta impostata la regola possiamo controllare il suo funzionamento provando nuovamente a caricare la pagina web della DVWA di Metasploitable 2, notando che non riuscirà a caricare la pagina perché è appunto bloccata dal firewall.























Step 11 Facciamo un ultimo controllo, questa volta tramite Wireshark e, come possiamo notare dall'immagine sottostante, il traffico sulla porta 80 da 192.168.50.106 a 192.168.51.100 è bloccato e riceviamo un messaggio di errore (il protocollo TCP non completa la three-way-handshake).



Facoltativo

Ispezionare i log del Firewall.

✖	Apr 30 13:00:15	LAN	 block DVWA from Kali (1746017088)	  192.168.50.106:42832	  192.168.51.100:80	TCP:S
✖	Apr 30 13:00:16	LAN	 block DVWA from Kali (1746017088)	  192.168.50.106:42822	  192.168.51.100:80	TCP:S
✖	Apr 30 13:00:16	LAN	 block DVWA from Kali (1746017088)	  192.168.50.106:42832	  192.168.51.100:80	TCP:S
✖	Apr 30 13:00:17	LAN	 block DVWA from Kali (1746017088)	  192.168.50.106:42822	  192.168.51.100:80	TCP:S

Action	Time	Interface	Rule description	Rule ID	Source	Destination	Protocol
Block	30	LAN	Block DVWA from Kali	1746017088	192.168.50.106	192.168.51.100	TCP