

## CREAZIONE DI UNA POLICY FIREWALL IN PFSense

### Task:

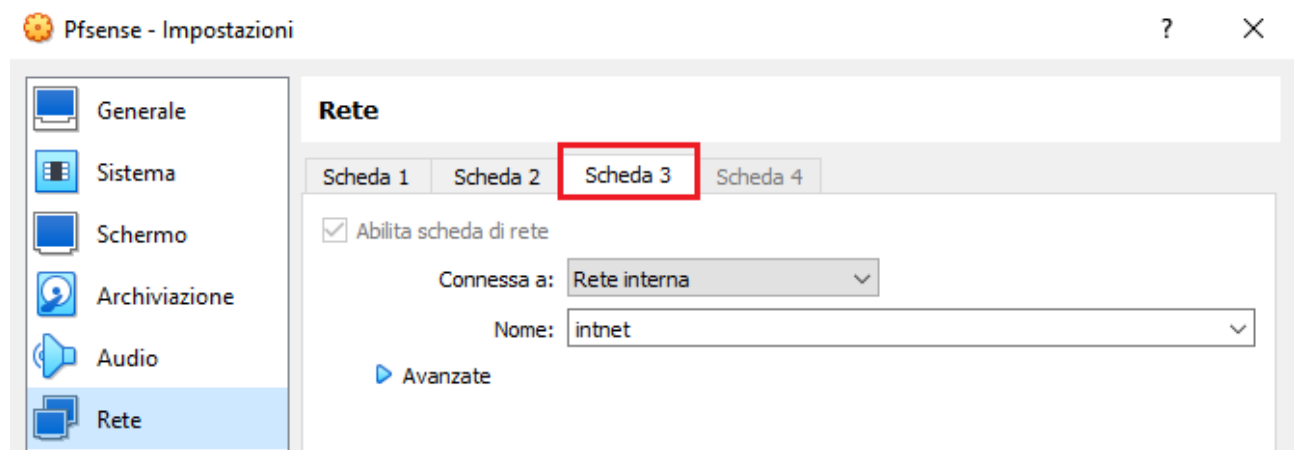
1. Creazione di una terza scheda di rete LAN in pfSense
2. Connessione tra le macchine Kali e Metasploitable tramite pfSense
3. Blocco del traffico da Kali verso i servizi web di Metasploitable tramite la creazione di una policy di blocco in pfSense

### 1. Creazione di una terza scheda di rete LAN in pfSense

pfSense è una distribuzione basata su FreeBSD, ottimizzata per essere utilizzata come Firewall.

Presenta di default una scheda di rete LAN ed una WAN. Ai fini dell'attività in oggetto, creiamo e configuriamo una terza scheda di rete locale.

Abilitiamo la terza scheda di rete da VM.



La situazione delle schede di rete locali è ora la seguente:

- Una scheda di rete **LAN** già presente, con indirizzo IPv4 **192.168.50.103** configurato in precedenza direttamente dalla macchina pfSense
- La nuova scheda di rete che chiameremo **LAN2**. Accediamo da Kali all'indirizzo 192.168.50.103 di pfSense e configuriamola nel modo seguente:

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](#)

Terminata la configurazione di LAN2 ecco il riepilogo aggiornato sulla macchina pfSense:

```
*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 10.0.2.15/24
LAN (lan)      -> em1      -> v4: 192.168.50.103/24
LAN2 (opt1)    -> em2      -> v4: 192.168.90.103/24
```

## 2. Connessione tra le macchine Kali e Metasploitable tramite pfSense

Creiamo una sottorete tra Kali e pfSense, inserendo l'indirizzo della scheda LAN (192.168.50.103) come gateway nelle impostazioni della scheda di rete di Kali:

```
kali@kali: /
File Actions Edit View Help
GNU nano 6.4 /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 192.168.50.100/24
gateway 192.168.50.103
```

Ripetiamo il procedimento per creare una sottorete tra pfSense e Metasploitable, collegando quest'ultima alla scheda LAN2 di pfSense (appena creata), inserendo 192.168.90.103 come indirizzo di gateway e scegliendo **192.168.90.101** come nuovo indirizzo IPv4 di Metasploitable:

```
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 static
address 192.168.90.101
netmask 255.255.255.0
network 192.168.90.0
broadcast 192.168.90.255
gateway 192.168.90.103
```



Successivamente verifichiamo la connettività tra le 3 macchine effettuando dei ping tests, che risultano positivi e confermano quindi la funzionalità dei nuovi settings di rete. Vediamo infatti che

- 1) pfSense comunica efficacemente con Kali e Metasploitable
- 2) Kali raggiunge sia pfSense che Metasploitable

Il che crea l'ambiente di test ottimale per lo step successivo di questa attività.

```
Enter a host name or IP address: 192.168.50.100

PING 192.168.50.100 (192.168.50.100): 56 data bytes
64 bytes from 192.168.50.100: icmp_seq=0 ttl=64 time=0.546 ms
64 bytes from 192.168.50.100: icmp_seq=1 ttl=64 time=1.052 ms
64 bytes from 192.168.50.100: icmp_seq=2 ttl=64 time=1.401 ms

--- 192.168.50.100 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.546/1.000/1.401/0.351 ms
```

```
Enter a host name or IP address: 192.168.90.101

PING 192.168.90.101 (192.168.90.101): 56 data bytes
64 bytes from 192.168.90.101: icmp_seq=0 ttl=64 time=7.726 ms
64 bytes from 192.168.90.101: icmp_seq=1 ttl=64 time=1.298 ms
64 bytes from 192.168.90.101: icmp_seq=2 ttl=64 time=1.565 ms

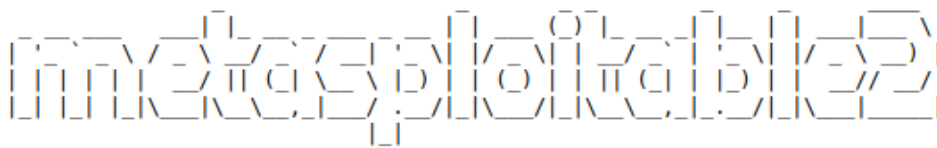
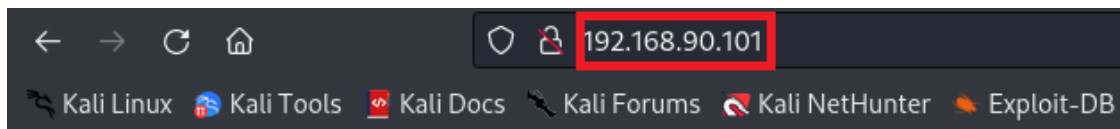
--- 192.168.90.101 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 1.298/3.530/7.726/2.969 ms
```

```
(kali㉿kali)-[/]
$ ping 192.168.50.103 LAN pfSense
PING 192.168.50.103 (192.168.50.103) 56(84) bytes of data.
64 bytes from 192.168.50.103: icmp_seq=1 ttl=64 time=0.712 ms
64 bytes from 192.168.50.103: icmp_seq=2 ttl=64 time=0.816 ms
64 bytes from 192.168.50.103: icmp_seq=3 ttl=64 time=0.884 ms
^C
— 192.168.50.103 ping statistics —
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 0.712/0.804/0.884/0.070 ms

(kali㉿kali)-[/]
$ ping 192.168.90.103 LAN2 pfSense
PING 192.168.90.103 (192.168.90.103) 56(84) bytes of data.
64 bytes from 192.168.90.103: icmp_seq=1 ttl=64 time=0.559 ms
64 bytes from 192.168.90.103: icmp_seq=2 ttl=64 time=0.675 ms
64 bytes from 192.168.90.103: icmp_seq=3 ttl=64 time=0.591 ms
^C
— 192.168.90.103 ping statistics —
3 packets transmitted, 3 received, 0% packet loss, time 2027ms
rtt min/avg/max/mdev = 0.559/0.608/0.675/0.048 ms

(kali㉿kali)-[/]
$ ping 192.168.90.101 IP Metasploitable
PING 192.168.90.101 (192.168.90.101) 56(84) bytes of data.
64 bytes from 192.168.90.101: icmp_seq=1 ttl=63 time=1.32 ms
64 bytes from 192.168.90.101: icmp_seq=2 ttl=63 time=1.86 ms
64 bytes from 192.168.90.101: icmp_seq=3 ttl=63 time=1.95 ms
^C
— 192.168.90.101 ping statistics —
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 1.320/1.706/1.945/0.275 ms
```

Inoltre, Kali (IP 192.168.50.100) può raggiungere i servizi web di Metasploitable all'indirizzo 192.168.90.101:

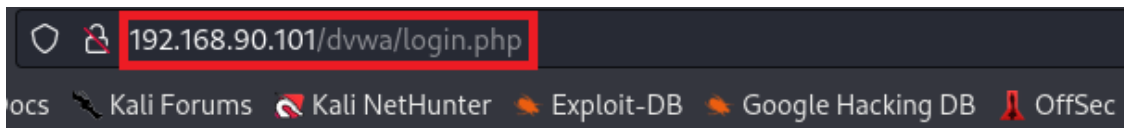


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

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



Username

Password

Login

### 3. Blocco del traffico da Kali verso i servizi web di Metasploitable tramite la creazione di una policy di blocco in pfSense

A questo punto, creiamo una policy di blocco del traffico proveniente da Kali verso l'applicazione web DVWA di Metasploitable. Per far ciò, rendiamo inaccessibili all'indirizzo 192.168.50.100 i servizi web di Metasploitable attivi sulla **porta 80 (http)** impostando una regola nel modo seguente:

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

Single host or alias

192.168.50.100

/

⚙️ 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

Single host or alias

192.168.90.101

/

Destination Port Range

HTTP (80)

From

Custom

HTTP (80)

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.

Una volta salvate le impostazioni, la nuova policy è attiva e si aggiunge alle altre in elenco.

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)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	✓	1 / 315 KiB	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
<input checked="" type="checkbox"/>	✗	0 / 0 B	IPv4 TCP	192.168.50.100	*	192.168.90.101	80 (HTTP)	*	none		
<input type="checkbox"/>	✓	5 / 216 KiB	IPv4 *	LAN net	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>	✓	0 / 0 B	IPv6 *	LAN net	*	*	*	none		Default allow LAN IPv6 to any rule	

↑ Add

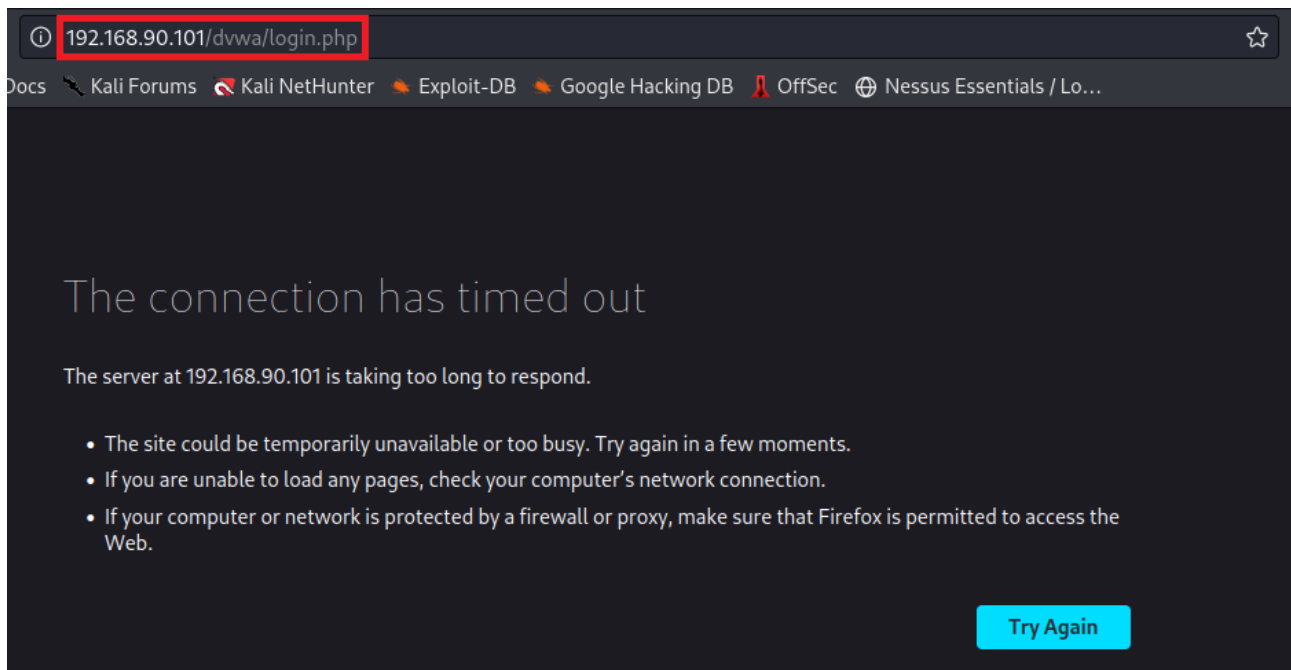
↓ Add

🗑 Delete

💾 Save

➕ Separator

A questo punto, tentiamo senza successo di raggiungere da Kali l'indirizzo web al quale si trova l'applicazione DVWA:



A ulteriore riprova dell'effettiva validità della nuova policy, effettuiamo con nmap una scansione di tipo TCP Connect indirizzata alla porta 80 di Metasploitable: essa viene rilevata come **filtered**, ossia come protetta da Firewall.

```
(kali@kali)-[~]
└─$ nmap -sT 192.168.90.101 -p 80
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-28 02:17 CET
Nmap scan report for 192.168.90.101
Host is up (0.00093s latency).

PORT      STATE      SERVICE
80/tcp    filtered  http

Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds
```