

# W9D4 - Pfsense

Come possiamo vedere sotto si vede la configurazione di Pfsense (già prima configurata su VBOX con due schede di rete: rete interna e rete con bridge - attenzione selezionando come modalità promiscua "permetti tutto"), NOKALI è la seconda rete già configurata, in seguito farò vedere la configurazione con Metasploitable.

```
LAN (lan)      -> vtnet1      -> v4: 192.168.50.1/24
NOKALI (opt1)  -> vtnet2      -> v4: 192.168.51.1/24

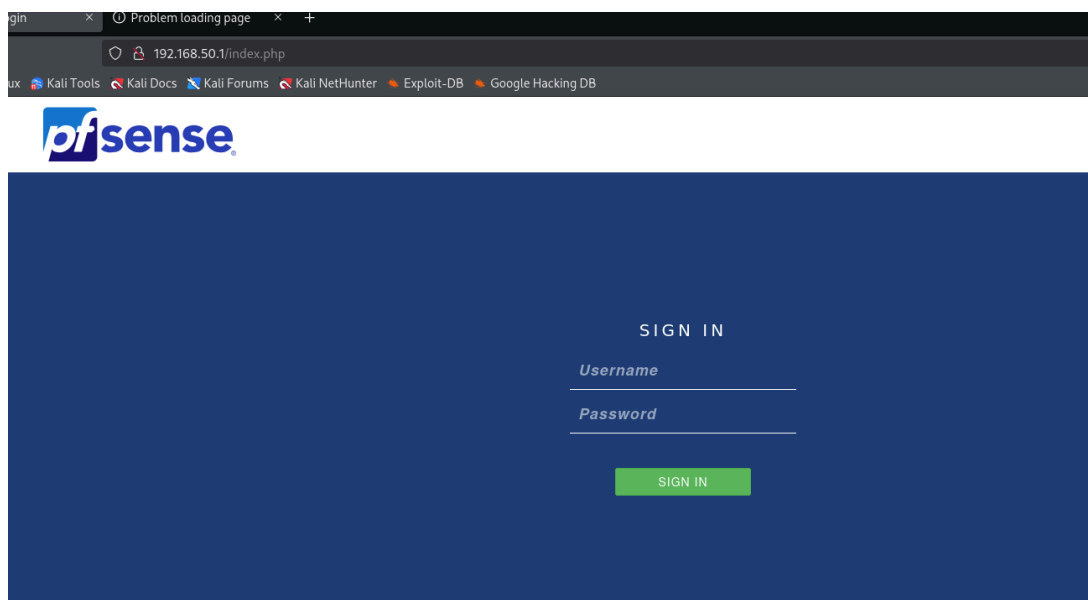
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: █
```

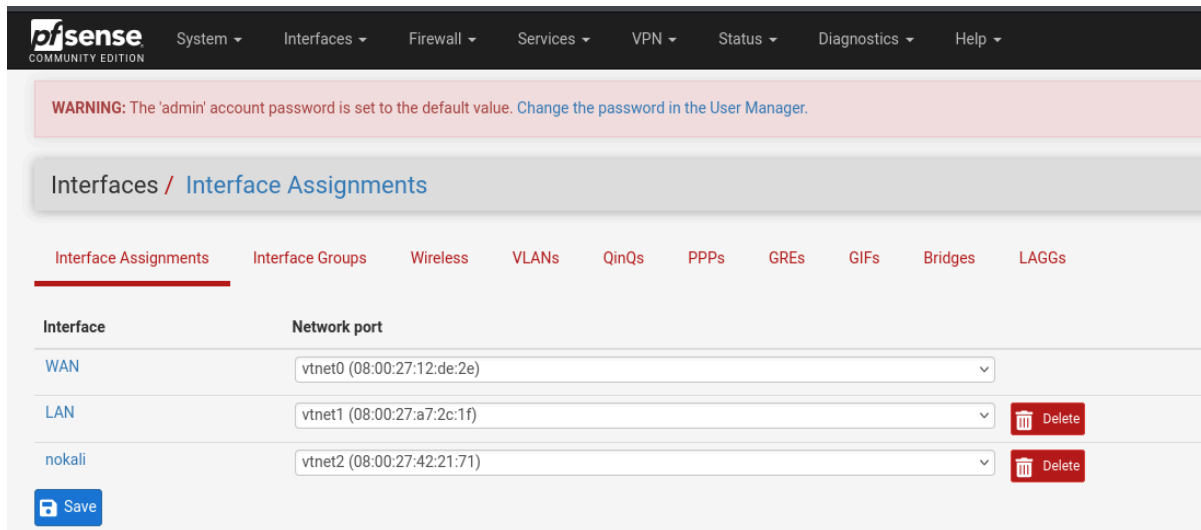
dalla Kali possiamo accedere a pfsense cercando con il suo IP, 192.168.50.1 e facciamo l'accesso con le credenziali:

username: admin

password: pfsense



andando su Interfaces e assignments si può vedere la seconda rete da aggiungere, nel nostro caso l'ho chiamata nokali



passiamo alla configurazione della metasploitable:

per non perdere l'altra configurazione, abilitiamo un'altra scheda di rete come rete interna chiamandola intnet2 e l'altra la disabilitiamo. Dopodiché lanciando il comando “sudo nano (/o vim) /etc/network/interfaces” modifichiamo il file assegnando l'indirizzo IP per la nuova rete, 192.168.51.101 e mettiamo come commento l'altra configurazione, come in figura:

```
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

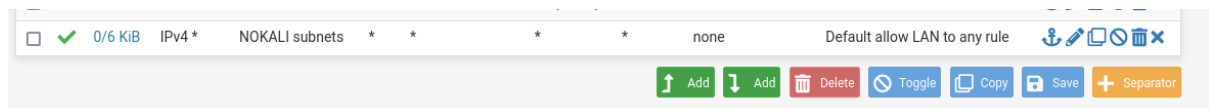
# The primary network interface
#auto eth0
#iface eth0 inet static
#address 192.168.50.101
#netmask 255.255.255.0
#gateway 192.168.50.1

auto eth0
iface eth0 inet static
address 192.168.51.101
netmask 255.255.255.0
gateway 192.168.51.1

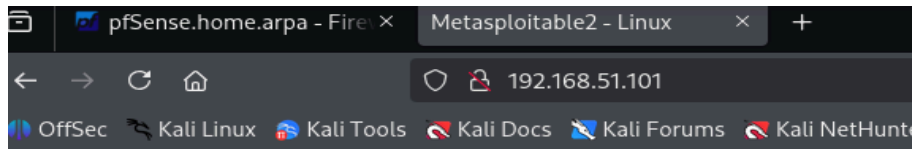
[ Read 19 lines ]
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cu
```

fatto ciò possiamo lanciare il comando “ sudo /etc/init.d/networking restart” per riavviare la rete

su Pfsense aggiungiamo la regola per la rete NOKALI cosi da far poter comunicare pfsense con metasploitable, andando su Firewall e rules



ecco ora se lo cerchiamo dalla Kali riusciamo ad accedere



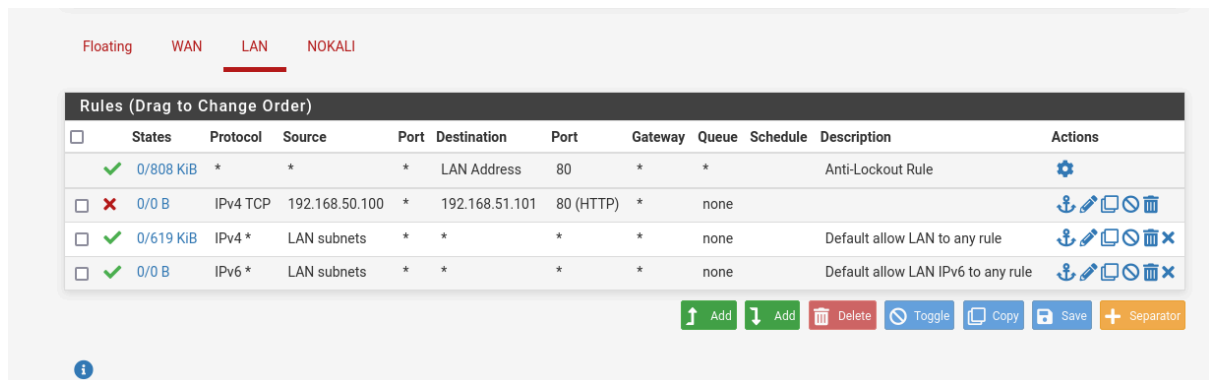
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

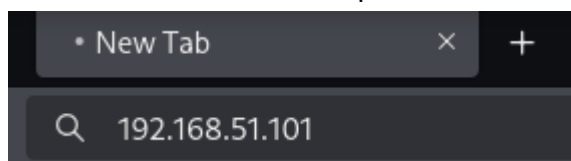
- [TWiki](#)
- [phpMyAdmin](#)
- [Mutillidae](#)
- [DVWA](#)
- [WebDAV](#)

creiamo una regola per bloccare l'accesso su Metasploitable dalla Kali su Pfsense, sempre su Rules, si aggiunge una regola di tipo blocco sulla rete LAN



come Source mettiamo l'IP address della Kali 192.168.50.100 e come Destination inseriamo l'IP address della Metasploitable 192.168.51.101, come porta, dato che ci interessa l'accesso alla DVWA, inseriamo la porta 80

fatto ciò la kali non riuscirà più ad accederci



**Facoltativo:**

per ispezionare i firewall log basta andare sul menu Status > System logs > firewall

Status / System Logs / Firewall / Normal View

System

Firewall

DHCP

Authentication

IPsec

PPP

PPPoE/L2TP Server

OpenVPN

NTP

Packages

Settings

Normal View

Dynamic View

Summary View

Last 500 Firewall Log Entries. (Maximum 500)						
Action	Time	Interface	Rule	Source	Destination	Protocol
✖	Sep 11 22:14:08	WAN	Block private networks from WAN block 192.168/16 (12004)	192.168.1.6:47248	192.168.1.255:15600	UDP
✖	Sep 11 22:14:14	WAN	Block private networks from WAN block 192.168/16 (12004)	192.168.1.4:47081	192.168.1.255:15600	UDP
✖	Sep 11 22:14:14	WAN	Block private networks from WAN block 192.168/16 (12004)	192.168.1.6:56133	192.168.1.255:15600	UDP
✖	Sep 11 22:14:20	WAN	Block private networks from WAN block 192.168/16 (12004)	192.168.1.4:52536	192.168.1.255:15600	UDP
✖	Sep 11 22:14:20	WAN	Block private networks from WAN block 192.168/16 (12004)	192.168.1.6:46944	192.168.1.255:15600	UDP
✖	Sep 11 22:14:24	WAN	Block private networks from WAN block 192.168/16 (12004)	192.168.1.136:57621	192.168.1.255:57621	UDP
✖	Sep 11 22:14:26	WAN	Block private networks from WAN block 192.168/16 (12004)	192.168.1.4:59591	192.168.1.255:15600	UDP

e potremmo ispezionare i log del Firewall