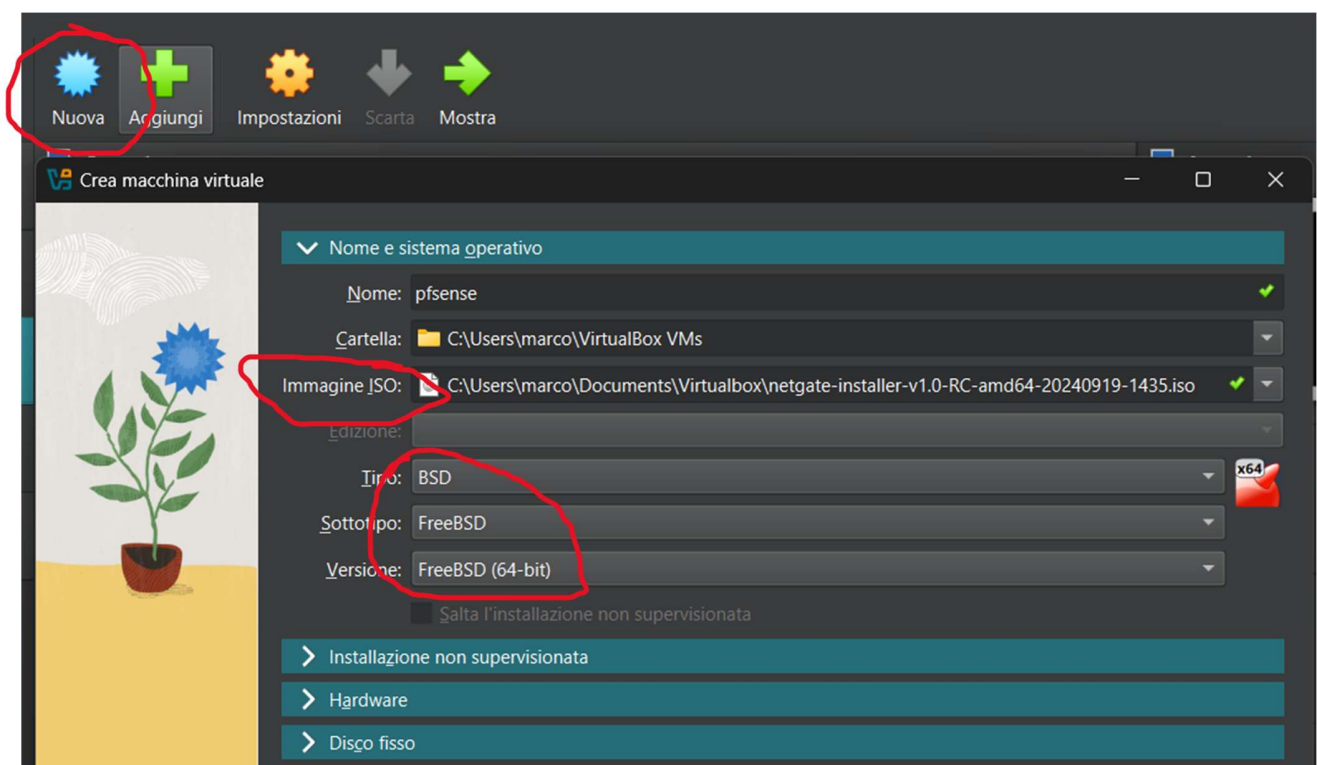


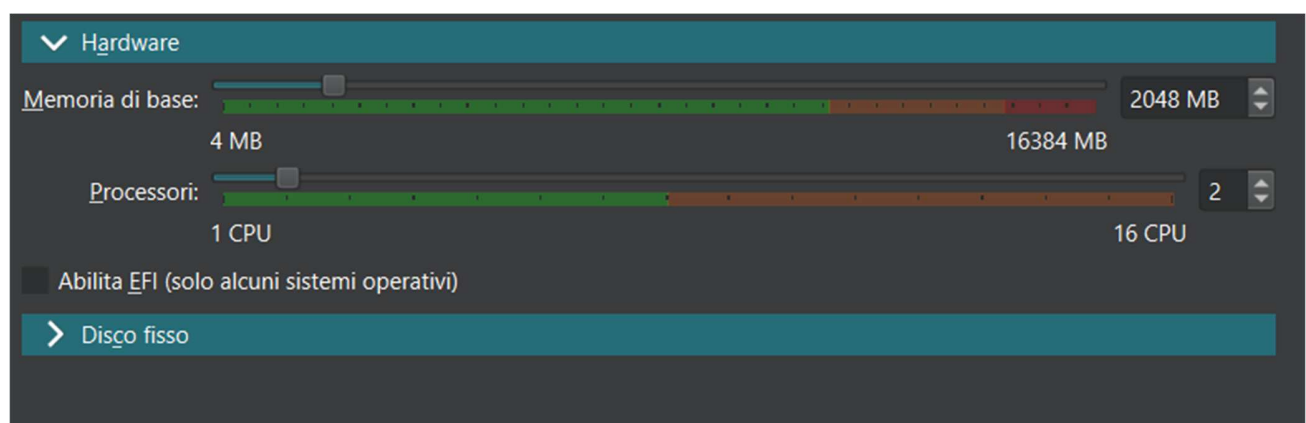
## S3/L5

Il Progetto di questa settimana prevede di installare PFsense come firewall per filtrare il traffico tra kali e DVWA (installato su metasploitable). Kali e metasploitable devono essere in due reti differenti

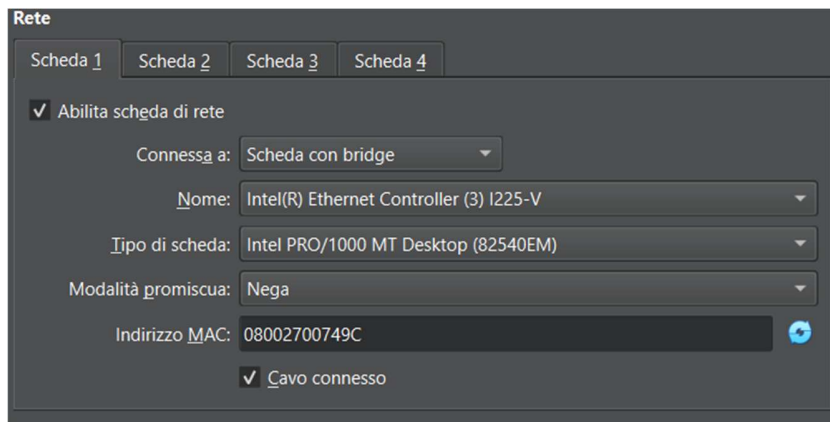
Avendo Kali e Metasploitable già installati, non rimane che installare PFSense. Creo una nuova macchina virtuale e aggiungo l'iso (non ho trovato il file OVA da importare). Selezione BSD, FreeBSD e FreeBSD 64 bit che corrispondono al tipo della distribuzione.



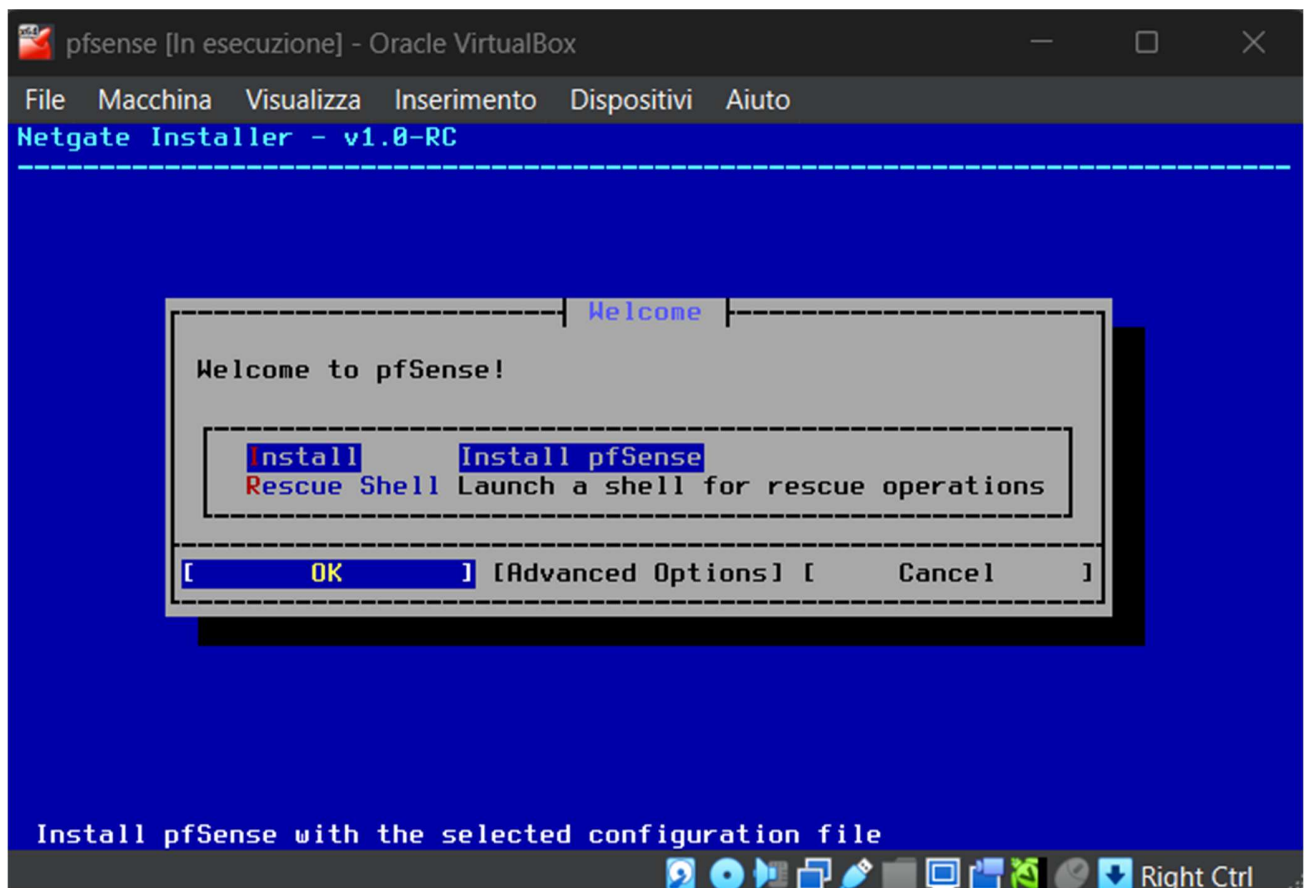
Alloco un paio di giga di ram e un paio di cpu



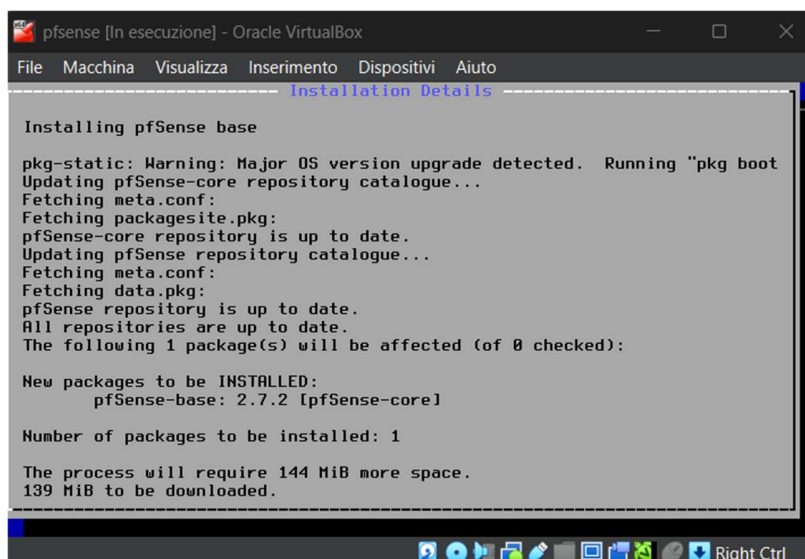
Metto il dispositivo in Bridge perché avrà bisogno di collegarsi a internet per degli aggiornamenti



Avvio PFSense e seguo le impostazioni di default



Uso tutte le opzioni di default e lascio l'accesso internet per poter scaricare gli aggiornamenti



The screenshot shows the pfSense installation window in Oracle VM VirtualBox. The title bar reads "pfsense [In esecuzione] - Oracle VirtualBox". The menu bar includes "File", "Macchina", "Visualizza", "Inserimento", "Dispositivi", and "Aiuto". The main window has a title "Installation Details" and displays the following text:

```
Installing pfSense base

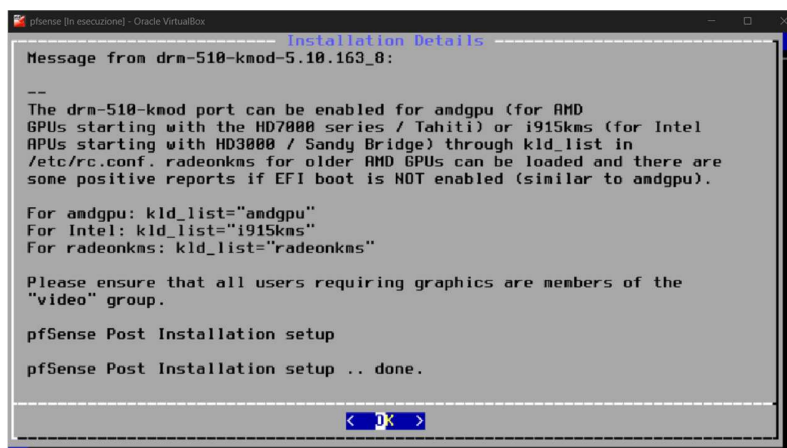
pkg-static: Warning: Major OS version upgrade detected. Running "pkg boot
Updating pfSense-core repository catalogue...
Fetching meta.conf:
Fetching packagesite.pkg:
pfSense-core repository is up to date.
Updating pfSense repository catalogue...
Fetching meta.conf:
Fetching data.pkg:
pfSense repository is up to date.
All repositories are up to date.
The following 1 package(s) will be affected (of 0 checked):

New packages to be INSTALLED:
  pfSense-base: 2.7.2 [pfSense-core]

Number of packages to be installed: 1

The process will require 144 MiB more space.
139 MiB to be downloaded.
```

The bottom of the window shows a taskbar with various icons and a "Right Ctrl" button.



The screenshot shows the pfSense post-installation message window in Oracle VM VirtualBox. The title bar reads "pfsense [In esecuzione] - Oracle VirtualBox". The menu bar includes "File", "Macchina", "Visualizza", "Inserimento", "Dispositivi", and "Aiuto". The main window has a title "Installation Details" and displays the following text:

```
Message from drm-510-kmod-5.10.163_8:

--

The drm-510-kmod port can be enabled for amdgpu (for AMD
GPUs starting with the HD7000 series / Tahiti) or i915kms (for Intel
APUs starting with HD3000 / Sandy Bridge) through kld_list in
/etc/rc.conf. radeonkms for older AMD GPUs can be loaded and there are
some positive reports if EFI boot is NOT enabled (similar to amdgpu).

For amdgpu: kld_list="amdgpu"
For Intel: kld_list="i915kms"
For radeonkms: kld_list="radeonkms"

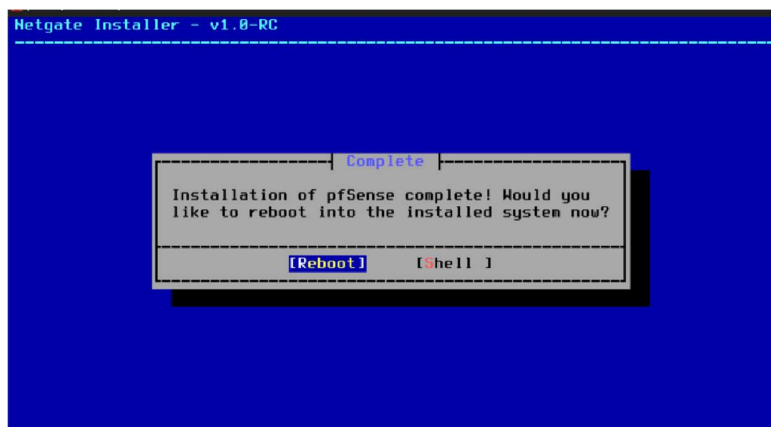
Please ensure that all users requiring graphics are members of the
"video" group.

pfSense Post Installation setup

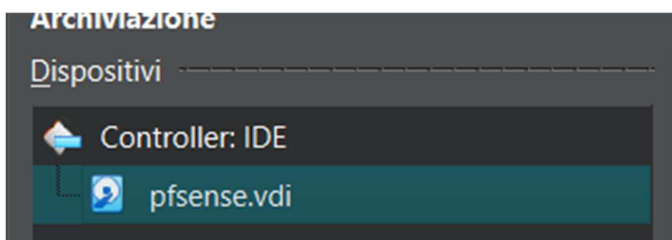
pfSense Post Installation setup .. done.
```

The bottom of the window shows a taskbar with various icons and a "Right Ctrl" button.

Ad aggiornamento terminato, riavvio:



E scelgo il file iso



Accedo a metasploitable, per fare il login uso default user:password che ho trovato [qui](#)

### Logging in to Metasploitable 2

The login for Metasploitable 2 is `msfadmin:msfadmin`.

```
pfSense [In esecuzione] - Oracle VirtualBox
Generating RRD graphs...done.
Starting syslog...done.
Starting CRON... done.
pfSense 2.7.2-RELEASE amd64 20240304-1953
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)
VirtualBox Virtual Machine - Netgate Device ID: a7948f8bb42cbe331b2a

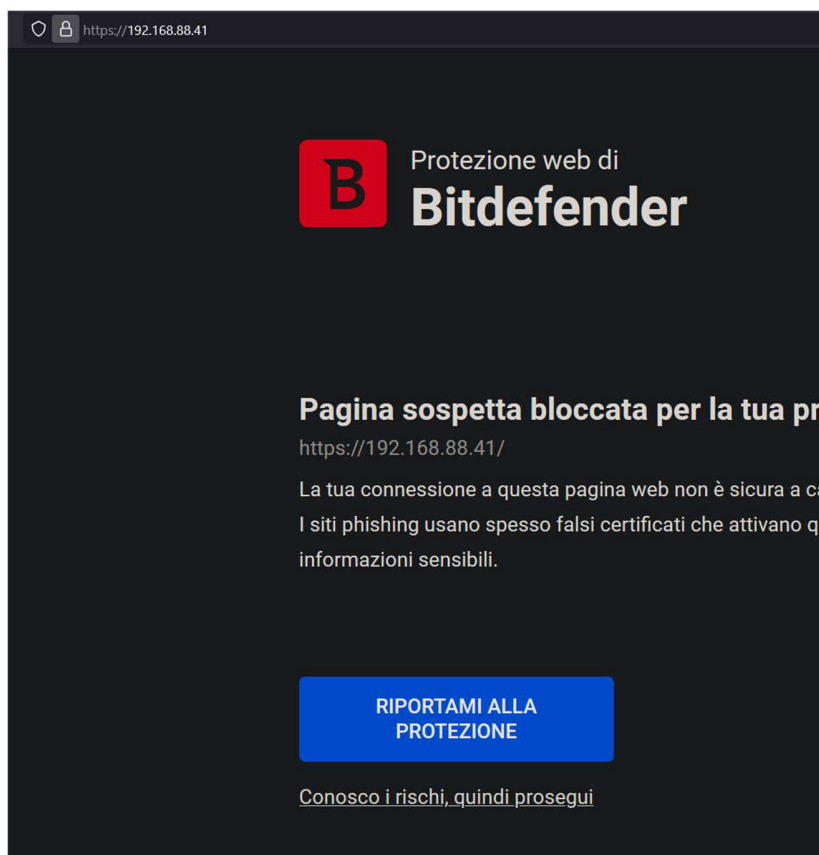
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.88.41/24

0) Logout (SSH only)          9) pflop
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: █
```

Vado nel browser e provo ad accedere:



L'antivirus si arrabbia, proseguo. Accedo con le credenziali di default che sono **admin:pfsense**

## General Information

On this screen the general pfSense parameters will be set.

**Hostname**

Name of the firewall host, without domain part.

Examples: pfsense, firewall, edgefw

**Domain**

Domain name for the firewall.

Examples: home.arpa, example.com

Do not end the domain name with '.local' as the final part (Top Level Rendezvous, Airprint, Airplay) and some Windows systems and network devices may not work. Alternatives such as 'home.arpa', 'local.lan', or 'mylocal' are safe.

The default behavior of the DNS Resolver will ignore manually configured DNS servers below for client queries, visit [DNS Resolver Settings](#) for more information.

**Primary DNS Server**

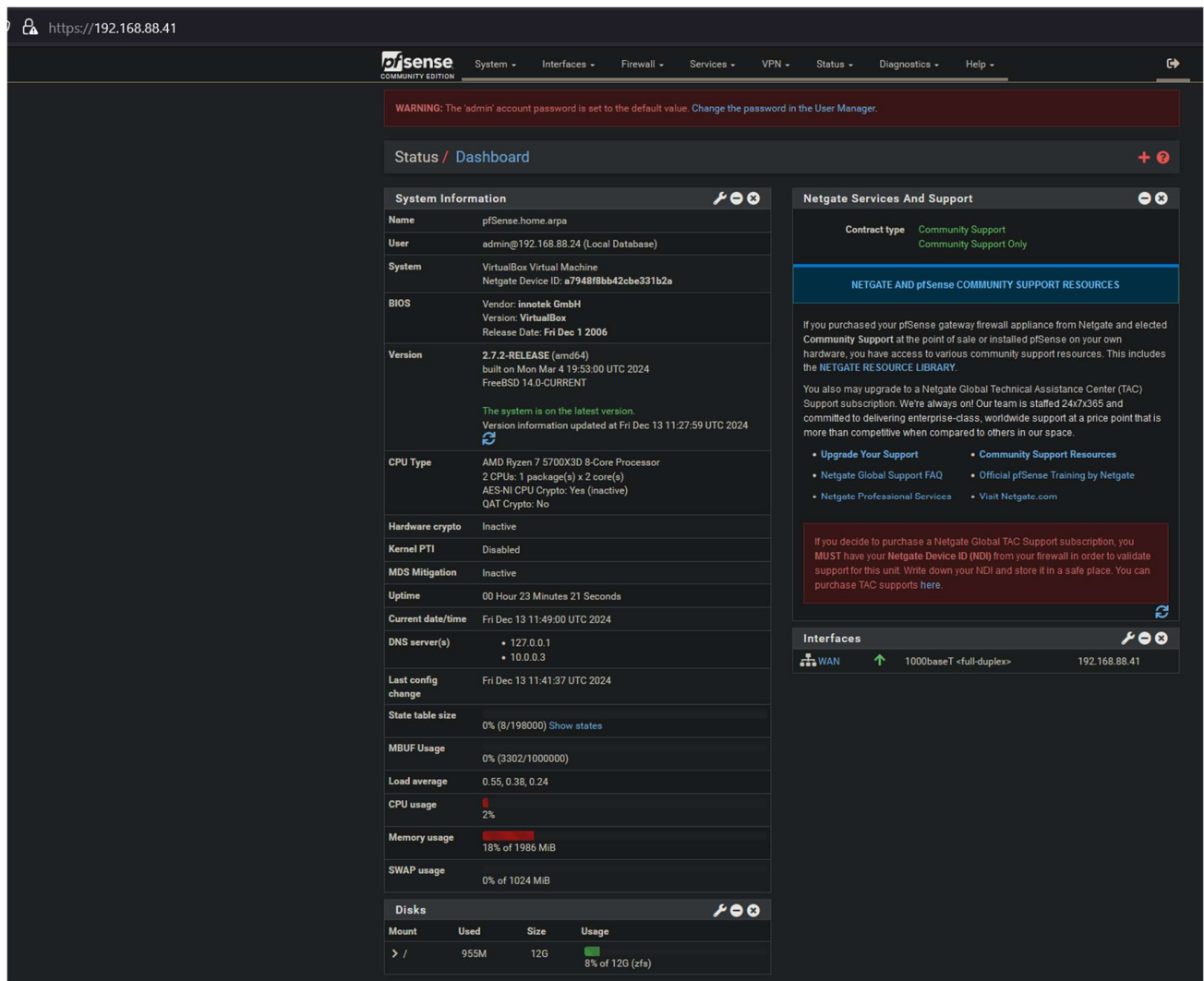
**Secondary DNS Server**

**Override DNS**



Allow DNS servers to be overridden by DHCP/PPP on WAN

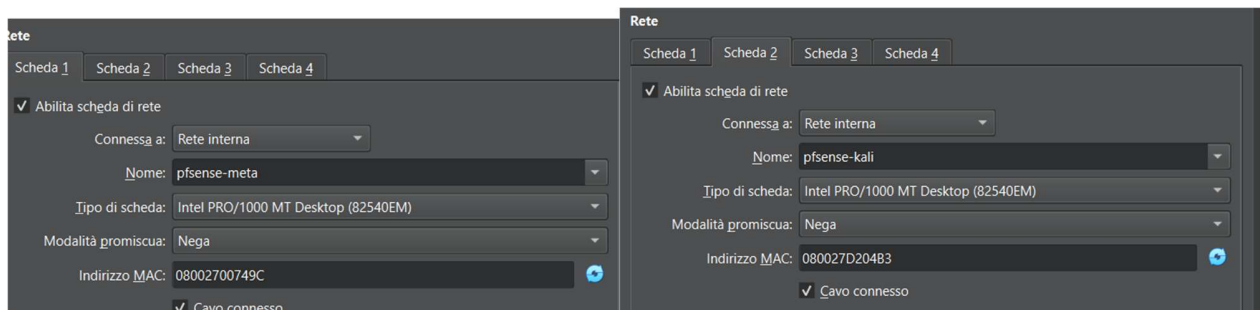
La configurazione è terminata. Verranno aggiunte in seguito regole firewall



Apro metasploitable e controllo l'ip locale con ifconfig

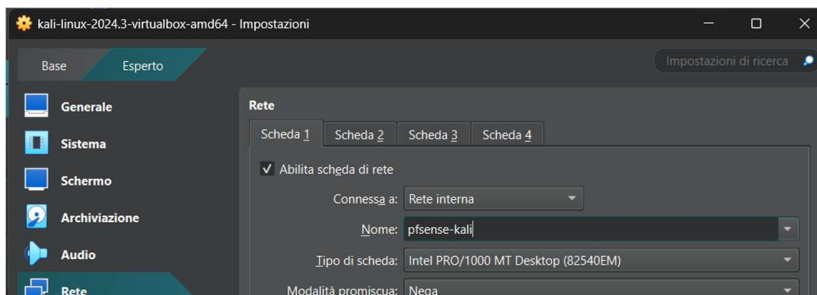
Ora passo alla configurazione delle reti di pfsense.

Pfsense ha bisogno di due interfacce di rete, poiché kali e metasploitable devono appartenere a due reti diverse

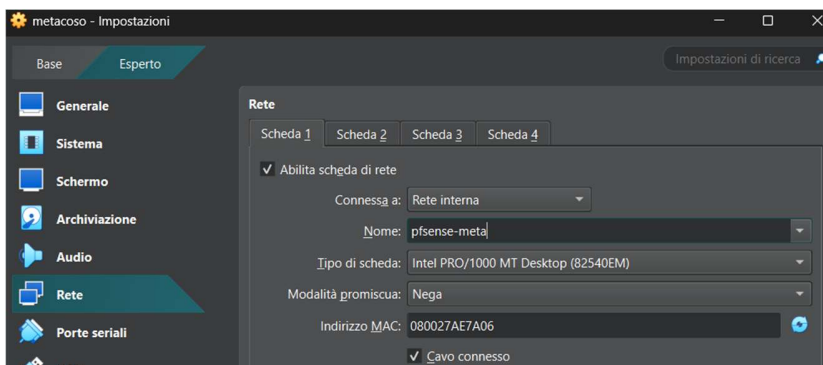


Ora assegno gli ip alle interfacce di pfsense, che fungeranno da gateway per kali e per metasploitable

Metto Kali sull'interfaccia pfsense-kali



E metasploitable sull'interfaccia pfsense-metasploitable



Ora accendo le macchine e configuro a mano indirizzo ipv4 statico, subnet mask e gateway, partendo da pfsense

Scelgo 1:

```

pfsense [In esecuzione] - Oracle VirtualBox
Generating RRD graphs...done.
Starting syslog...done.
Starting CRON... done.
pfSense 2.7.2-RELEASE amd64 20240304
Bootup complete

FreeBSD/amd64 (pfSense.home.arp) (t
VirtualBox Virtual Machine - Netgate

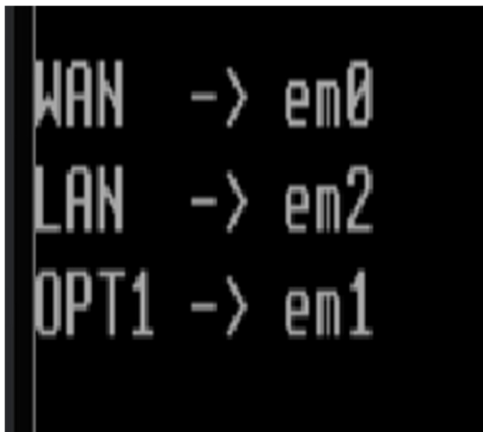
*** Welcome to pfSense 2.7.2-RELEASE

WAN (wan)      -> em0      ->

0) Logout (SSH only)
1) Assign Interfaces
2) Set interface(s) IP address
3) Reset webConfigurator password
4) Reset to factory defaults
5) Reboot system
6) Halt system
7) Ping host
8) Shell

```





```
WAN -> em0
LAN -> em2
OPT1 -> em1
```

Dopo questo passaggio le macchine non mi funzionano più. Ecco come avrei fatto:

Accedo all'indirizzo LAN corrispondente all'interfaccia di pfsense-kali usando l'indirizzo lan indicato

Ragguingo la web gui di pfsense

Seleziono la lan da cui voglio bloccare l'accesso

Aggiungo una regola per il firewall:

action block, interface l'interfaccia di kali, source l'indirizzo locale di kali, destination l'indirizzo lan di metasploitable (nella rete locale di metasploitable), destination port range 80

Questa regola non è molto sicura perché cambiando indirizzo ip locale o rete si può comunque raggiungere dvwa