

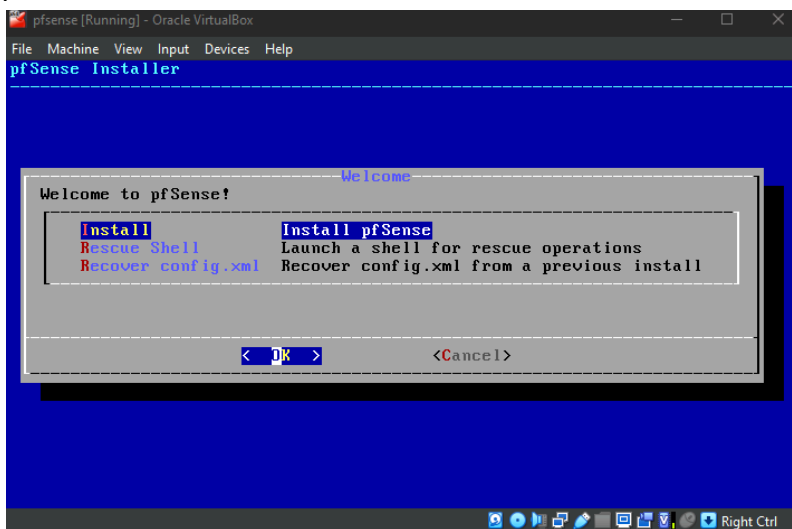
Progetto S3/L5

Il progetto di oggi prevede la configurazione di una regola firewall che impedisca l'accesso alla DVWA dalla macchina virtuale Kali Linux

Installazione Pfsense

1.

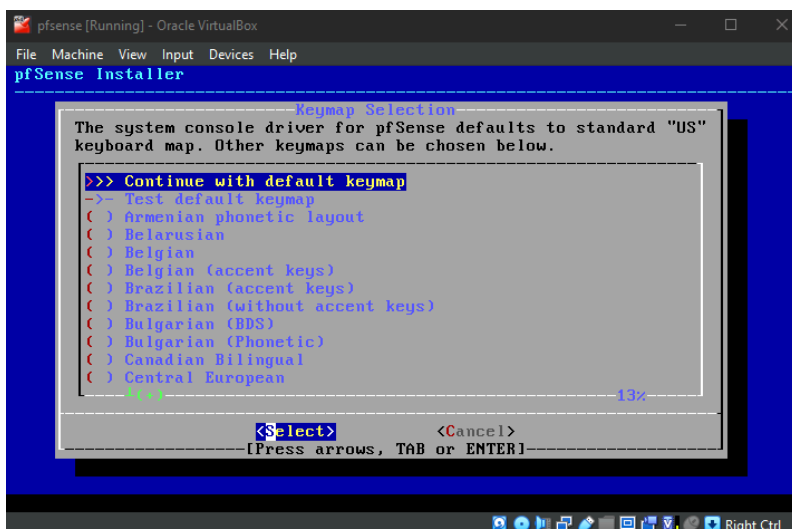
Avvia pfSense. Dopo averlo avviato, clicca su 'OK' e poi sulla freccia verde in alto per avviare la macchina virtuale. Clicca su 'Accept' per accettare le norme di copyright e poi seleziona 'Install pfSense'



2.

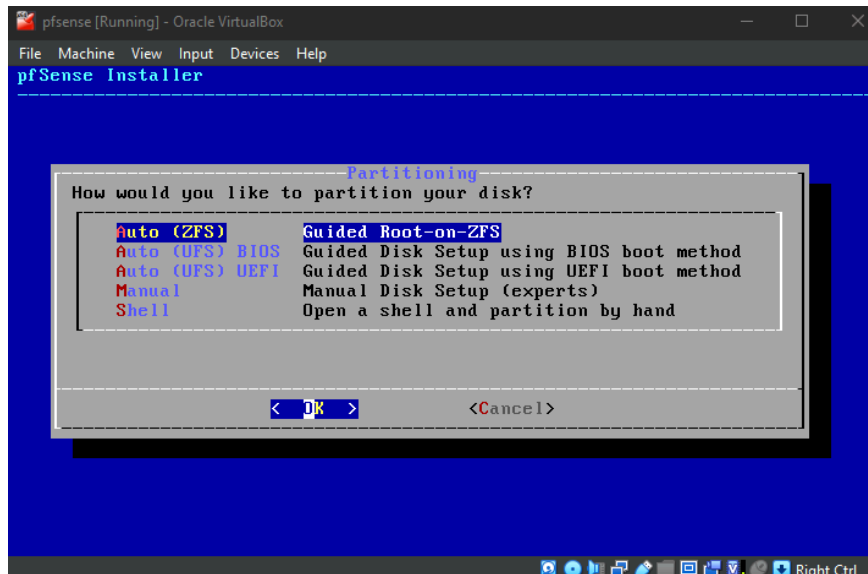
visto che io ho una tastiera con il layout americano selezionare Continue with the default

keymap



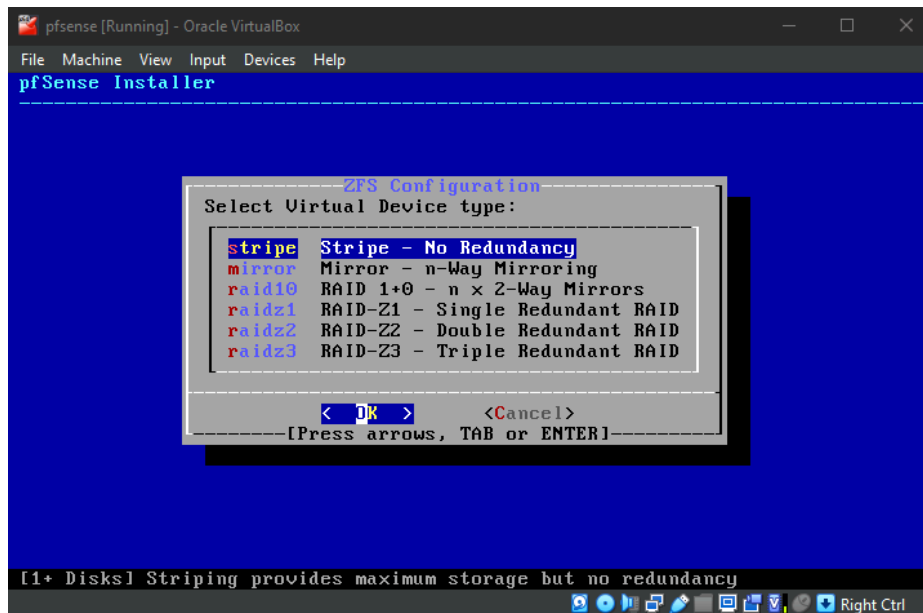
3.

Selezionare **Auto (ZFS)** e poi premere invio



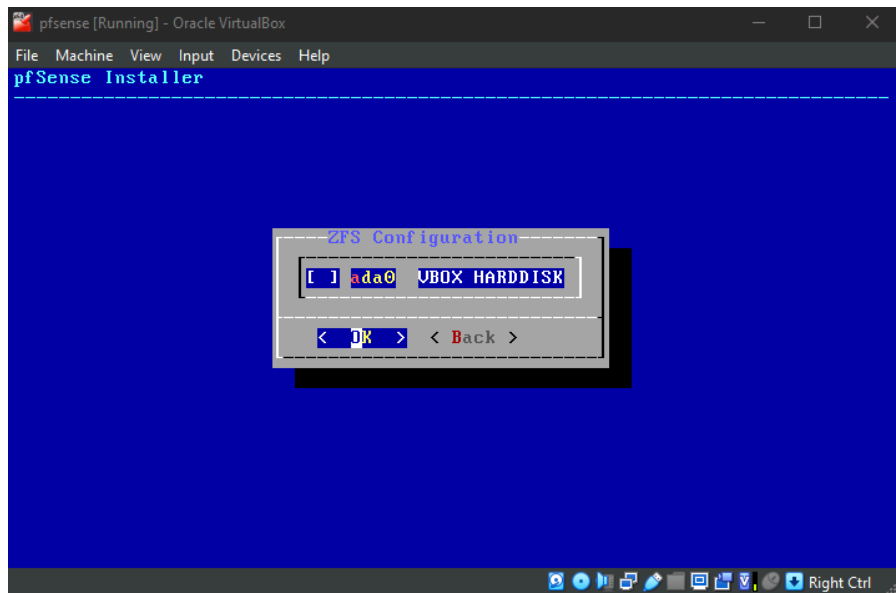
4.

qui cliccare su Stripe visto che abbiamo solo un disco virtuale



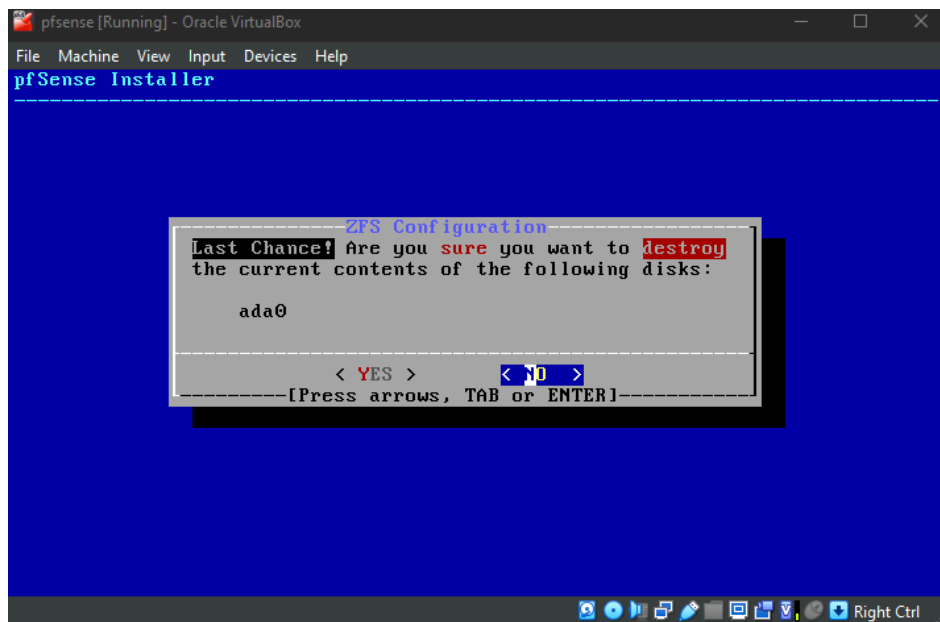
5.

Qua ci richiede di selezionare il nostro disco virtuale. per selezionarlo usare la barra spaziatrice e cliccare nvio sulla tastiera per procedere



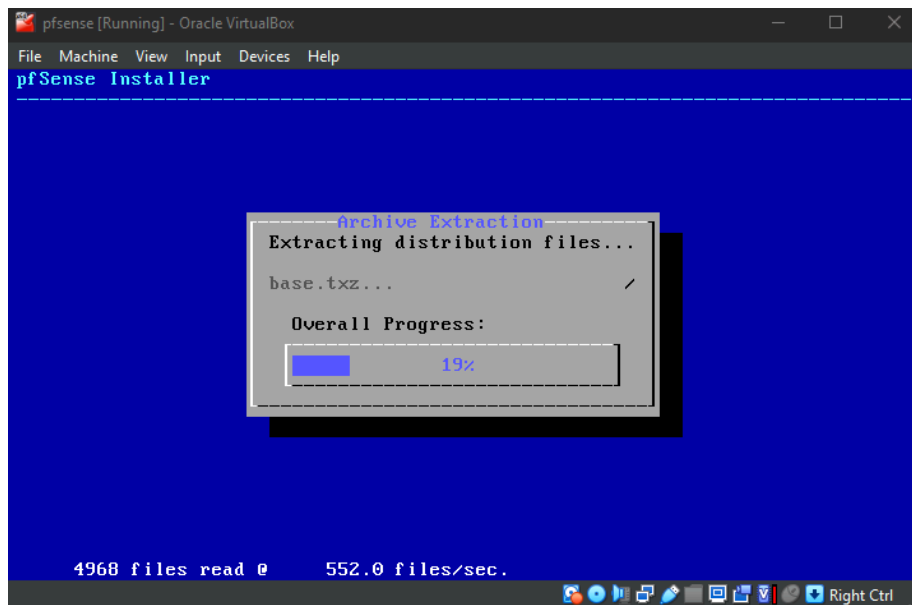
6.

dopo aver cliccato invio ci chiederà se siamo certi se vogliamo formattare l'hard drive che abbiamo selezionato. visto che e una memoria virtuale selezioniamo Yes



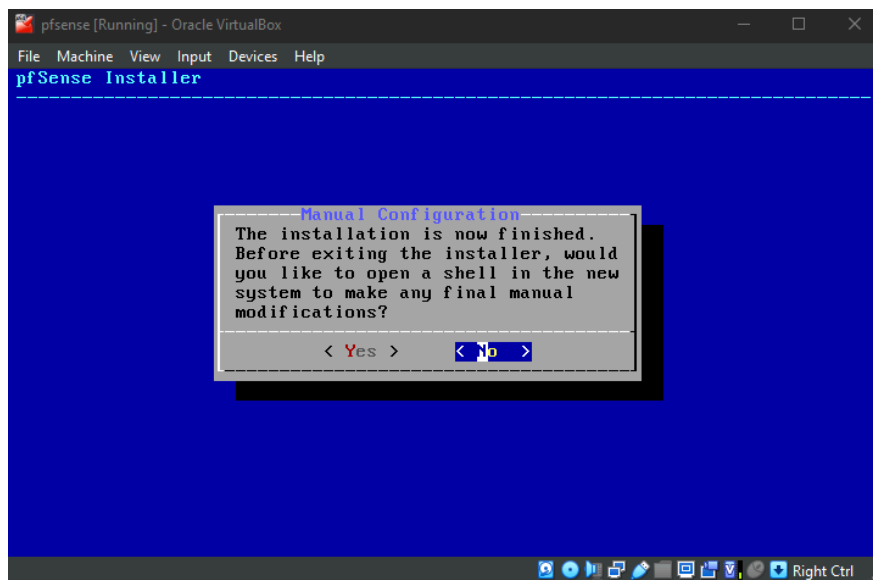
7.

Dopo aver cliccato yes procederà con l'installazione



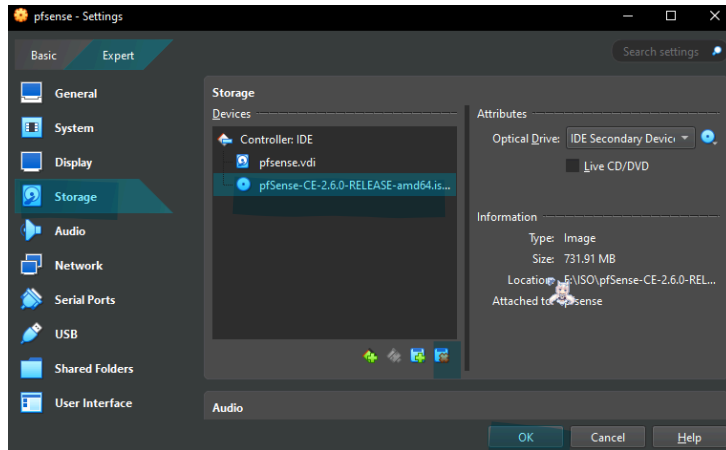
8.

Dopo che l'installazione è finita ci chiederà se vogliamo aprire una shell (Terminale) in questo caso non ci serve quindi selezioniamo No e poi Reboot per riavviare la macchina virtuale



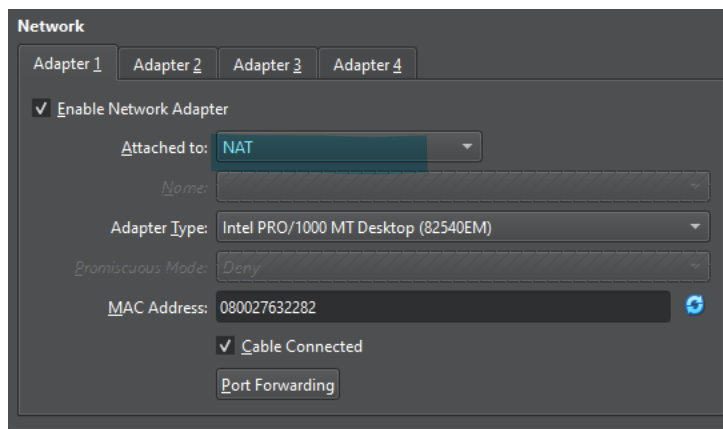
Rimozione ISO

Dopo che la macchina virtuale ha completato l'installazione, dobbiamo spegnerla per disconnettere la ISO. Per fare ciò, clicchiamo in alto su VirtualBox, selezioniamo impostazioni, quindi clicchiamo su Storage. A questo punto, facciamo clic sul disco e selezioniamo Rimuovi

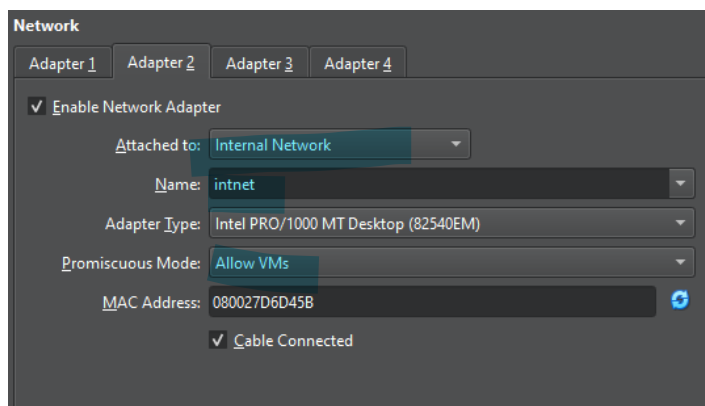


Configurazione adattatori rete

Adattatore 1: Impostare la rete Nat per il primo adattatore

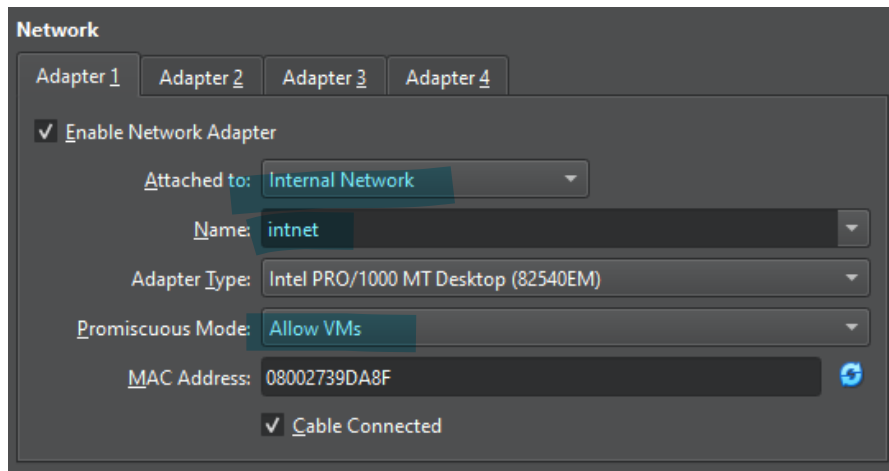


Adattatore 2: Internal Network



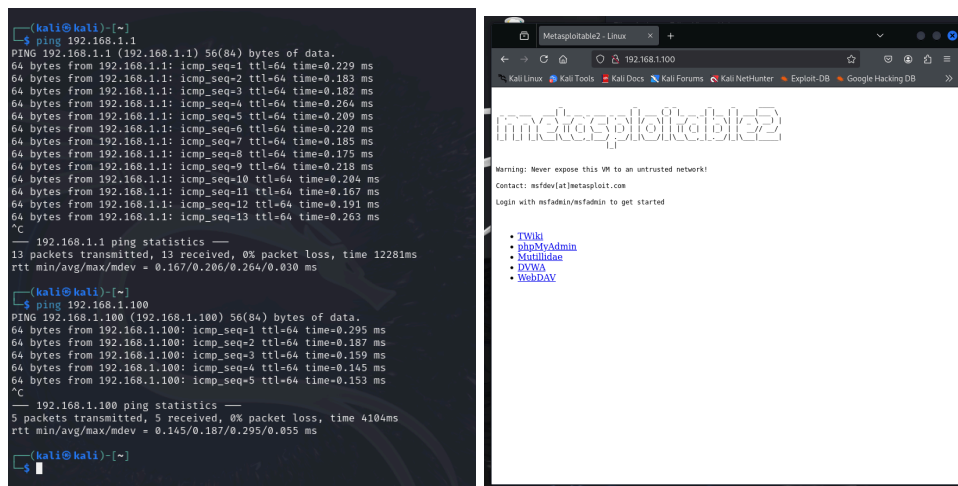
Kali Linux e Metasploitable

Per le altre due macchine virtuali dovremmo selezionare internal network. Ho fatto la stessa cosa per metasploitable e ho utilizzato lo stesso nome.



Verificare la comunicazione

Avviare le macchine virtuali e, per testare la connessione tra di loro, farò un ping da Kali a pfSense e da Kali a Metasploitable. Inoltre, proverò anche a connettermi a Metasploitable tramite il browser.



Configurazione Pfsense

Dopo aver verificato che tutto stia funzionando correttamente, dobbiamo accedere all'interfaccia di configurazione di pfsense su firefox. li potremmo configurare le regole di firewall.

Scrivere l'indirizzo ip di pfsense sulla barra di ricerca



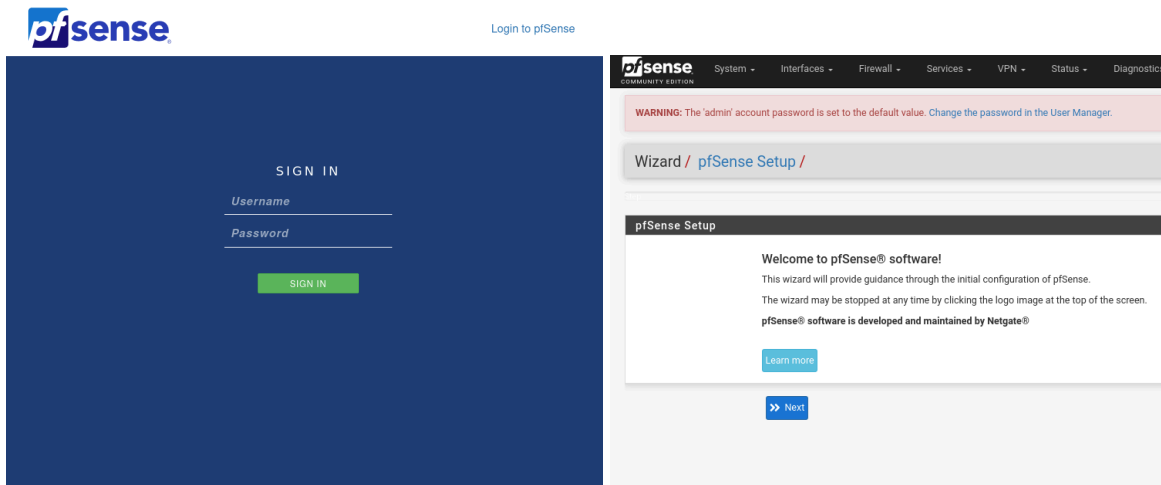
dopo aver premuto invio dovrebbe portarti in questa pagina. Qui dovrai fare l'accesso con le credenziali qui in basso

La password per accedere e:

username: admin

password: pfsense

Il setup iniziale possiamo anche saltarlo visto che non ci serve per questo esercizio.



Regola Firewall

dopo aver fatto l'accesso dobbiamo trovare l'indirizzo ip di metasploitable e di Kali.

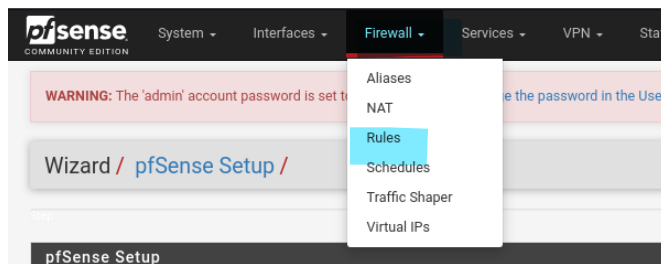
```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.109 netmask 255.255.255.0 broadcast 192.168.1.255
    ether 08:00:27:ad:25:87 txqueuelen 1000 (Ethernet)
    RX packets 5293 bytes 2719595 (2.5 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4937 bytes 585236 (571.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collision 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 222 bytes 20780 (20.2 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 222 bytes 20780 (20.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collision 0

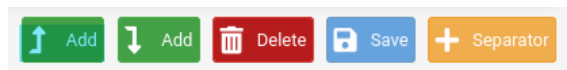
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.109 netmask 255.255.255.0 broadcast 192.168.1.255
    ether 08:00:27:ad:25:87 txqueuelen 1000 (Ethernet)
    RX packets 5293 bytes 2719595 (2.5 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4937 bytes 585236 (571.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collision 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 222 bytes 20780 (20.2 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 222 bytes 20780 (20.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collision 0
```

Navigare su firewall e cliccare su rules



clicca sulla freccia in alto per creare una regola in alto alla lista



Regola Firewall

Salva e applica la regola

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Firewall / Rules / Edit

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/UDP

Choose which IP protocol this rule should match.

Source

☐ Invert match 192.168.1.109 /

[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

☐ Invert match 192.168.1.110 /

Destination Port Range any From any 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).

Description

A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options [Display Advanced](#)

[Save](#)

Risultato finale

Kali Linux Clone (Running) - Oracle VM VirtualBox

File Machine View Input Devices Help

pfSense home.arpa - Firewall

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Firewall / Rules / Edit

The changes have been applied. Monitor the filter rules.

Floating WAN

Rules (Drag to Ruleset)

☐ States Prot 1/94 KIB

☐ IPv4 0/0 B TCP/UDP

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536

inet 127.0.0.1 netmask 255.0.0.0

inet6 ::1 prefixlen 128 scopeid 0<host>

loop txqueuelen 1000 (Local Loopback)

RX packets 222 bytes 20780 (20.2 KiB)

RX errors 0 dropped 0 overruns 0 frame 0

TX packets 222 bytes 20780 (20.2 KiB)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@kali) ~

```
ping 192.168.1.110
PING 192.168.1.110 (192.168.1.110) 56(84) bytes of data:
64 bytes from 192.168.1.109: icmp_seq=1 Destination Host Unreachable
64 bytes from 192.168.1.109: icmp_seq=2 Destination Host Unreachable
64 bytes from 192.168.1.109: icmp_seq=3 Destination Host Unreachable
64 bytes from 192.168.1.109: icmp_seq=4 Destination Host Unreachable
64 bytes from 192.168.1.109: icmp_seq=5 Destination Host Unreachable
64 bytes from 192.168.1.109: icmp_seq=6 Destination Host Unreachable
64 bytes from 192.168.1.109: icmp_seq=7 Destination Host Unreachable
64 bytes from 192.168.1.109: icmp_seq=8 Destination Host Unreachable
64 bytes from 192.168.1.109: icmp_seq=9 Destination Host Unreachable
64 bytes from 192.168.1.109: icmp_seq=10 Destination Host Unreachable
64 bytes from 192.168.1.109: icmp_seq=11 Destination Host Unreachable
64 bytes from 192.168.1.109: icmp_seq=12 Destination Host Unreachable
64 bytes from 192.168.1.109: icmp_seq=13 Destination Host Unreachable
64 bytes from 192.168.1.109: icmp_seq=14 Destination Host Unreachable
64 bytes from 192.168.1.109: icmp_seq=15 Destination Host Unreachable
64 bytes from 192.168.1.109: icmp_seq=16 Destination Host Unreachable
64 bytes from 192.168.1.109: icmp_seq=17 Destination Host Unreachable
64 bytes from 192.168.1.109: icmp_seq=18 Destination Host Unreachable
```

metasploitable Clone (Running) - Oracle VM VirtualBox

File Machine View Input Devices Help

TX packets:263 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:1000

RX bytes:23270 (22.7 KB) TX bytes:27457 (26.8 KB)

Base address:0xd020 Memory:f0200000-f0220000

Link encap:Local Loopback

inet addr:127.0.0.1 Bcast:255.0.0.0

inet6 addr: ::1/128 Scope:Host

UP LOOPBACK RUNNING MTU:16436 Metric:1

RX packets:499 errors:0 dropped:0 overruns:0 frame:0

TX packets:499 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:0

RX bytes:192297 (187.7 KB) TX bytes:192297 (187.7 KB)

msfadmin@metasploitable:~\$ ping 192.168.1.109

PING 192.168.1.109 (192.168.1.109) 56(84) bytes of data:

64 bytes from 192.168.1.109: icmp_seq=1 ttl=64 time=7.20 ms

64 bytes from 192.168.1.109: icmp_seq=2 ttl=64 time=0.441 ms

64 bytes from 192.168.1.109: icmp_seq=3 ttl=64 time=0.480 ms

64 bytes from 192.168.1.109: icmp_seq=4 ttl=64 time=0.496 ms

64 bytes from 192.168.1.109: icmp_seq=5 ttl=64 time=0.522 ms

64 bytes from 192.168.1.109: icmp_seq=6 ttl=64 time=0.663 ms

64 bytes from 192.168.1.109: icmp_seq=7 ttl=64 time=0.408 ms