

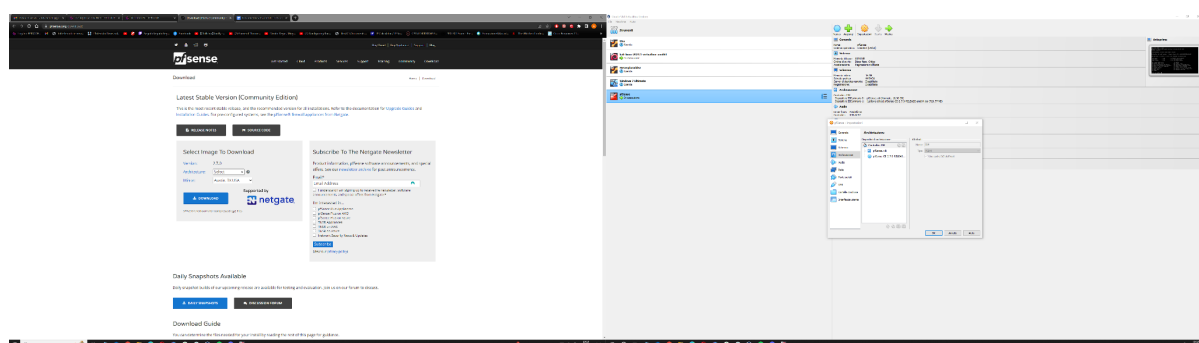
# Penetration Testing

Day 2 -> esercizio :

Creazione pratica di una regola sul firewall.

## ● Preparazione strumenti necessari

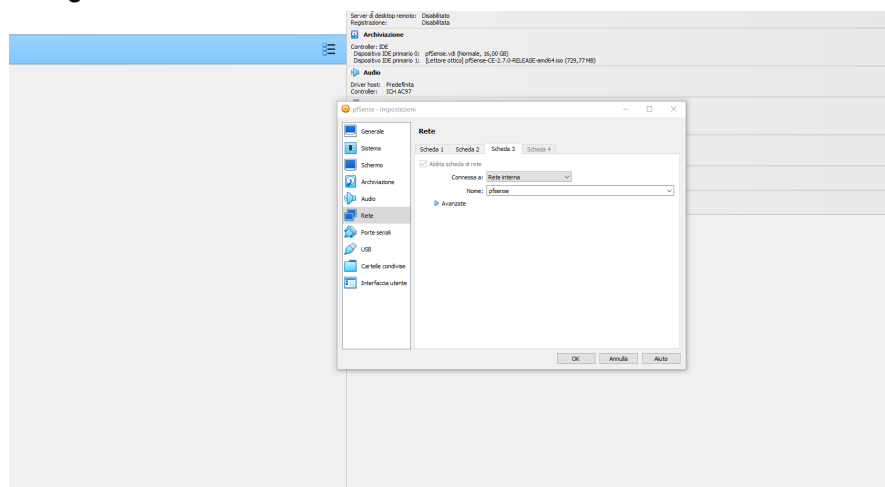
### 1. Download e configurazione pfSense



Una volta scaricato dal sito ufficiale e configurato nel nostro Virtual Box, ho provveduto a configurare il nostro firewall.

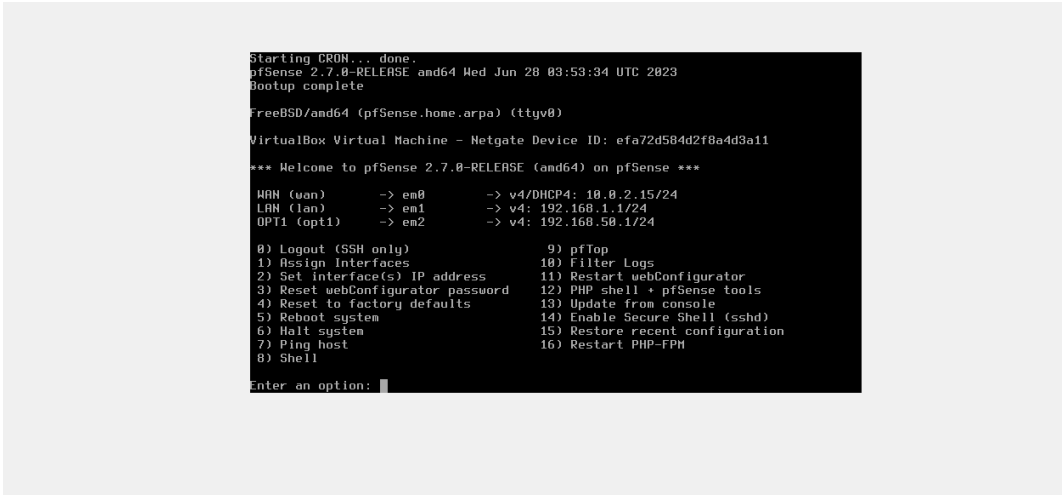
E' stato necessario cambiare il boot order da virtualbox, altrimenti il firewall non rileva l'hard disk e la ISO dalla quale abbiamo fatto partire l'installazione.

Una volta configurate tutte le caratteristiche di base, sono passato alla configurazione delle diverse schede di rete.

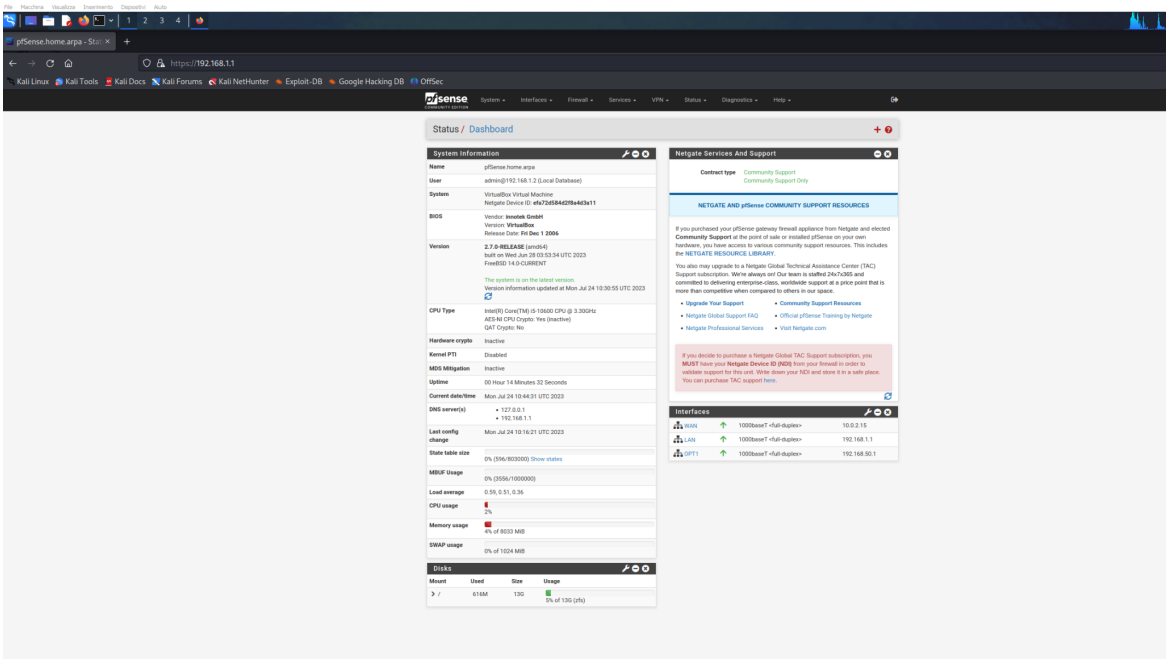


Come sappiamo il firewall ha 1 interfaccia rivolta verso la WAN, l'abbiamo configurata in modalità NAT affinché riceva l' IP direttamente dal nostro router

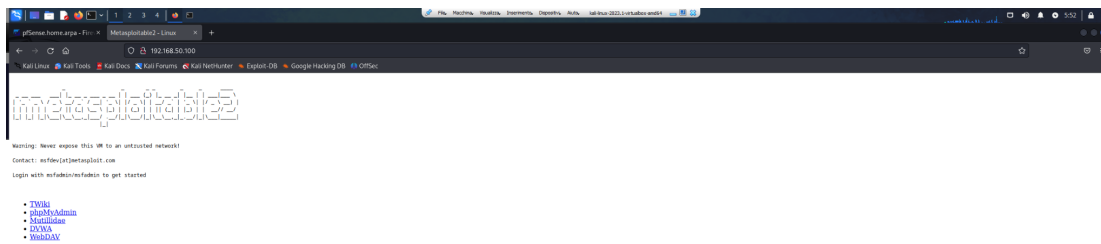
di casa. Le altre due interfacce invece sono state configurate in modalità interna, simulando due subnet differenti.



Una volta configurato il firewall ,l'ho avviato da interfaccia grafica sulla macchina Kali Linux. Per fare ciò, ho aperto firefox (un browser web qualunque va bene lo stesso), e inserendo l'indirizzo IP del gateway della macchina di Kali, sono entrato dopo essermi autenticato all'interno della GUI di pfSense.




Prima di creare la regola, mi sono connesso all'indirizzo della macchina di metasploitable 2 sempre da Firefox e ho testato la sua raggiungibilità.

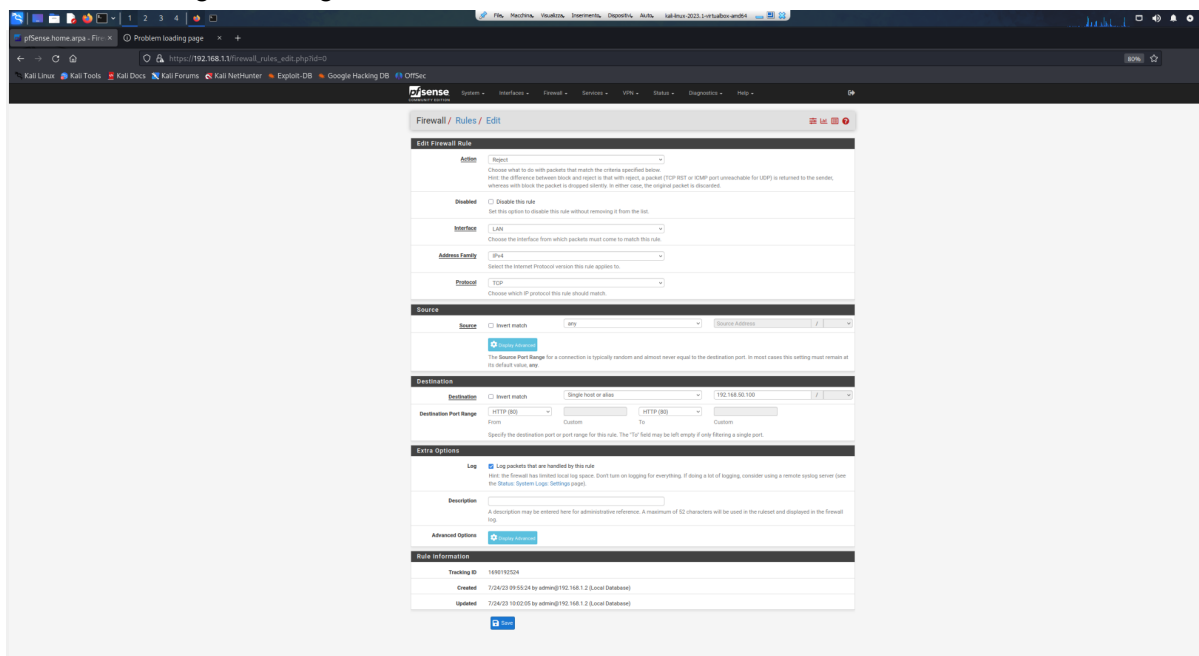


I

Una volta testata la raggiungibilità da kali,ho creato 1 regola che bloccasse ogni tipo di accesso verso quell'indirizzo IP. Per fare ciò sono andato nel menù a tendina : Firewall -> Rules.

A questo punto ho selezionato le regole che sarebbero state applicate alla mia interfaccia LAN, perché è l'interfaccia alla quale è collegata la mia macchina Kali ( la macchina per la quale voglio creare la regola).

Ho selezionato il pulsante  per aggiungere la regola in cima alle altre già esistenti, e ho creato la seguente regola :



Nella regola ho impostato l'azione che volevo che venisse effettuata (Reject)

Firewall / Rules / Edit

### Edit Firewall Rule

**Action** Reject

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 rejected whereas with block the packet is dropped silently. In either case, the original packet is discarded.

L'interfaccia ,il tipo di indirizzo IP e il protocollo che avrei respinto :

**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.

L'indirizzo IP di destinazione e il numero di porta.

Inoltre ho spuntato l'opzione extra log, che dovrebbe fornirci dei log in caso questa regola venga sollecitata.

**Destination**

**Destination** ☐ Invert match Single host or alias 192.168.50.100

**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.

**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.

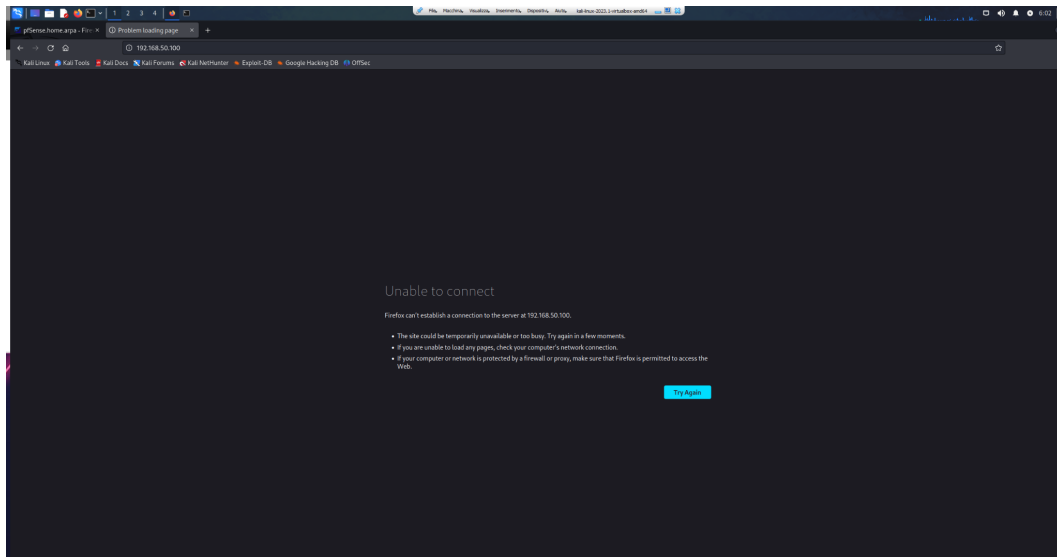
**Advanced Options** [Display Advanced](#)

**Rule Information**

Tracking ID	1690192524
Created	7/24/23 09:55:24 by admin@192.168.1.2 (Local Database)
Updated	7/24/23 10:02:05 by admin@192.168.1.2 (Local Database)

[Save](#)

Dopo aver salvato la configurazione ho provato a ricollegarmi sempre con il browser all'indirizzo IP 192.168.50.100 per controllare che effettivamente il firewall applicasse la regola e :



La regola funziona, il firewall sta applicando un blocco sulla porta TCP 80 ( protocollo HTTP) sull IP della macchina di Metasploitable che non è più così raggiungibile tramite browser web.