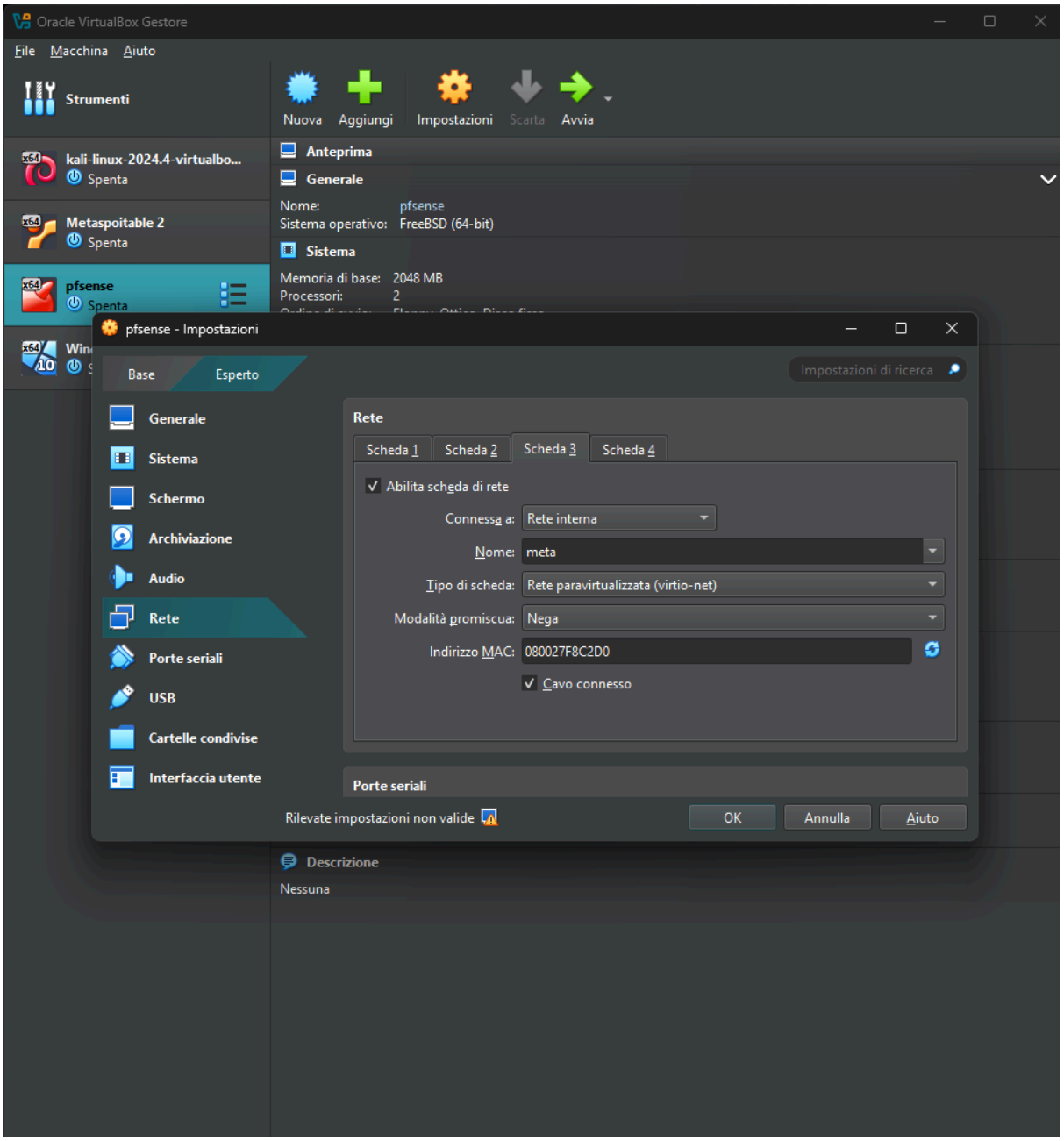
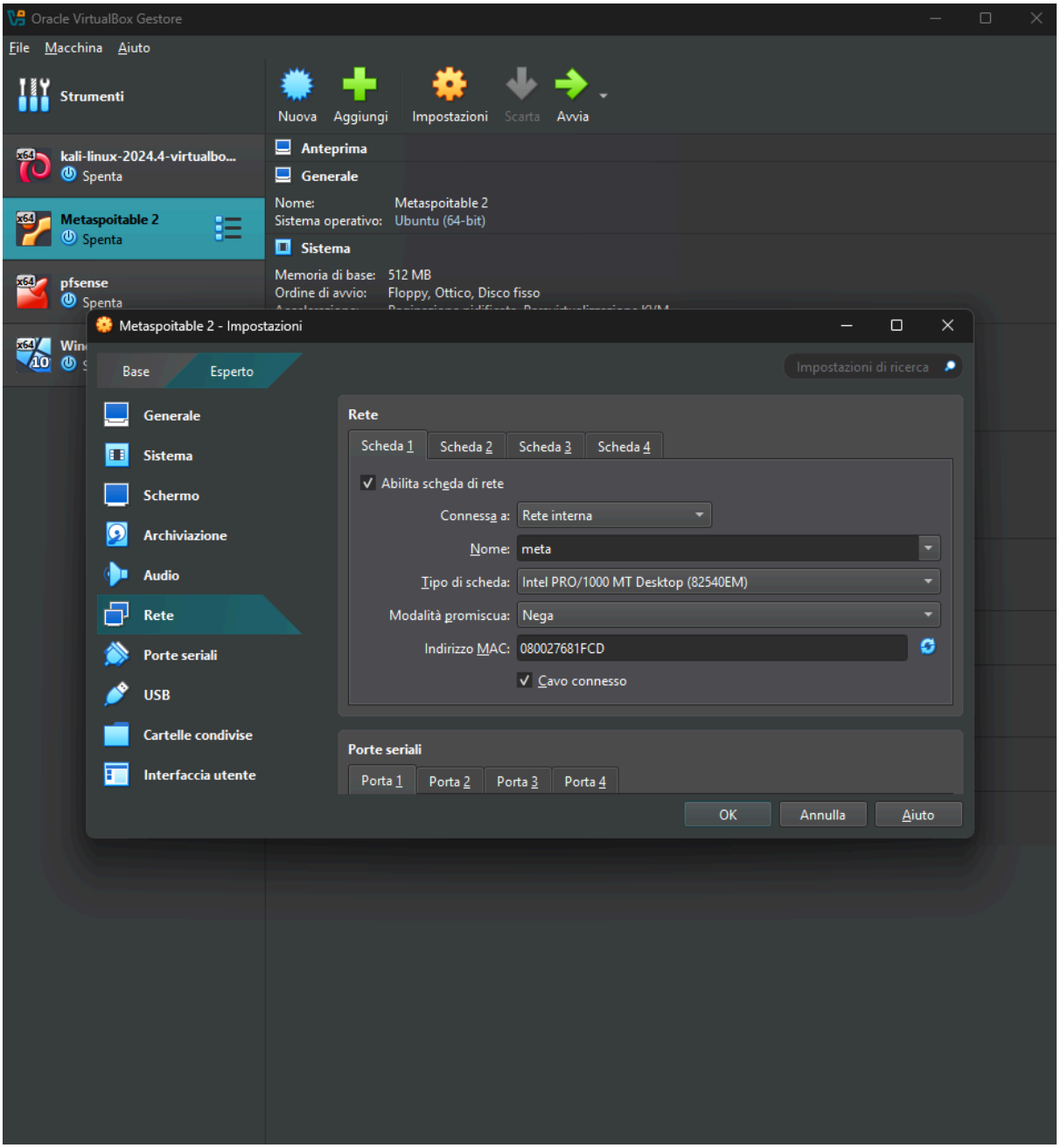
Creazione policy Pfsense

Buongiorno oggi andremo a creare una regola firewall su Pfsense.



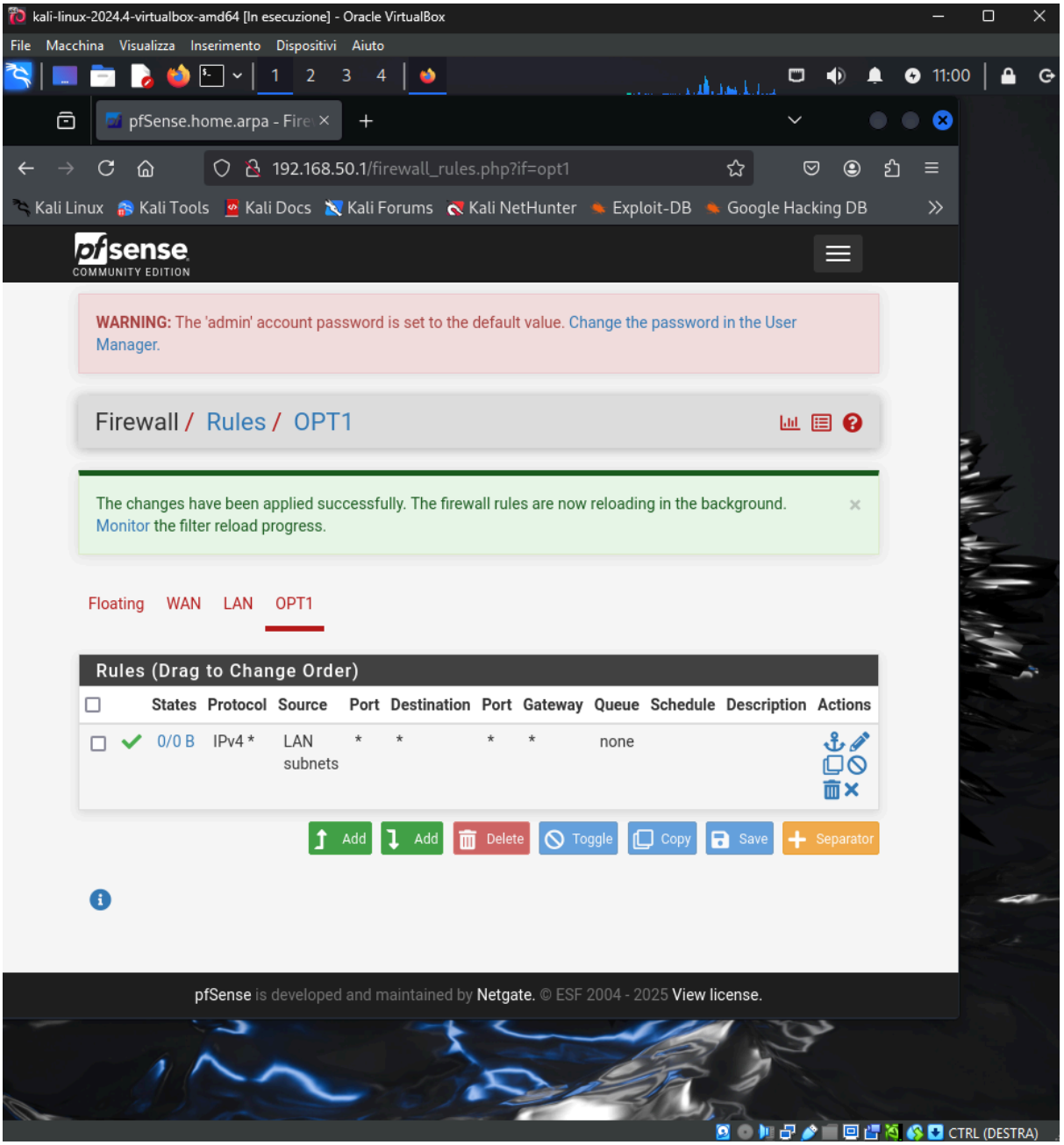
Per prima cosa andiamo a creare una terza scheda di rete sulla nostra macchina virtuale pfsense dove metteremo connessione alla rete interna e daremo un nuovo nome, in questo caso:”meta”.



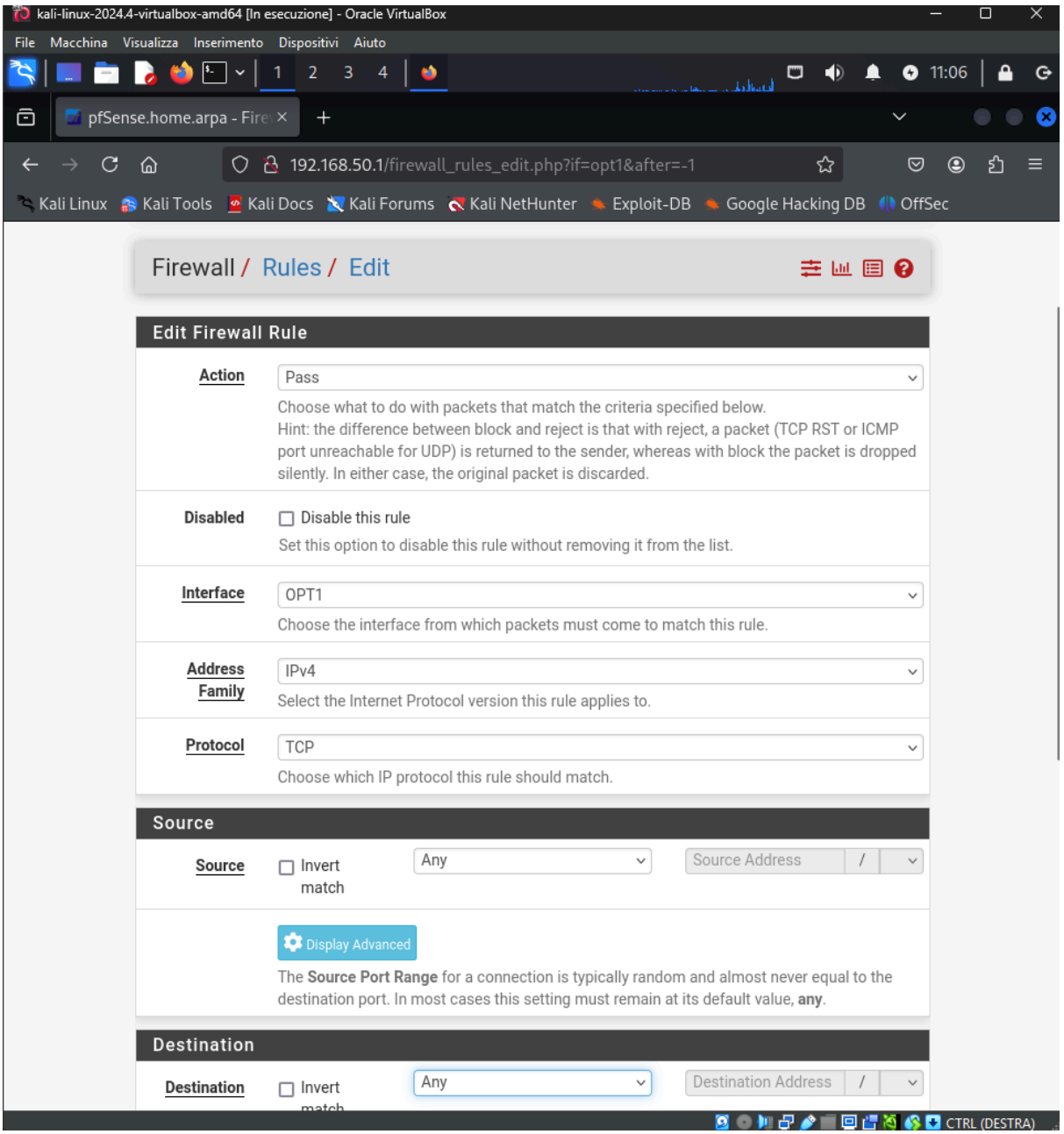
Ora invece andiamo a impostare sulla nostra macchina virtuale Metaspoitable2 la prima rete su connessione alla rete interna e metteremo il nome “meta” come fatto precedentemente sulla pfsense.
Una volta fatto questo avviamo le nostre macchine.

Sulla macchina Metaspoitable2 andiamo a configurare l'indirizzo ip,la netmask e il gateway tramite il comando $sudo nano /etc/network/interfaces come rappresentato nell'immagine sopra.

Una volta configurati andiamo a testarli con il comando $sudo /etc/init.d/networking restart e lanciando il comando successivo $ping 192.168.40.1 (il nostro gateway in questo caso). Dopo fatto questo andiamo sulla nostra macchina virtuale Kali Linux ,apriamo il browser, inseriamo il nostro indirizzo IP ed entriamo su pfSense.
Su pfSense creiamo oltre la WAN e la LAN(dove si trova l'IP di Kali) OPT1 dove andremo ad inserire l'Indirizzo IP di Metaspoitable2.

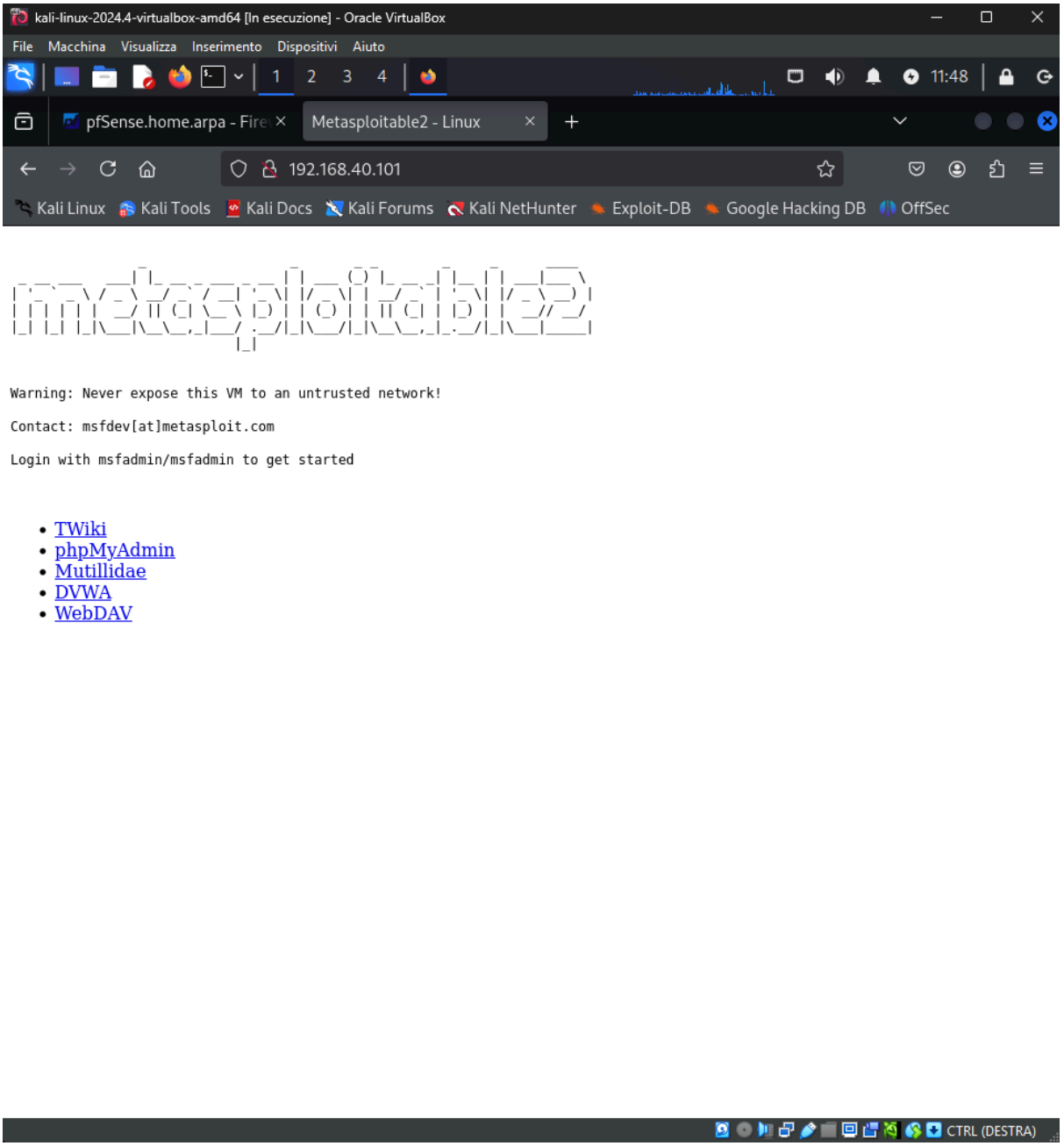


Una volta fatto ciò andiamo a inserire una regola firewall. Per crearla andiamo su Firewall-> Rules. Qui selezioniamo su quale interfaccia creare la regola, in questo caso scegliamo OPT1.

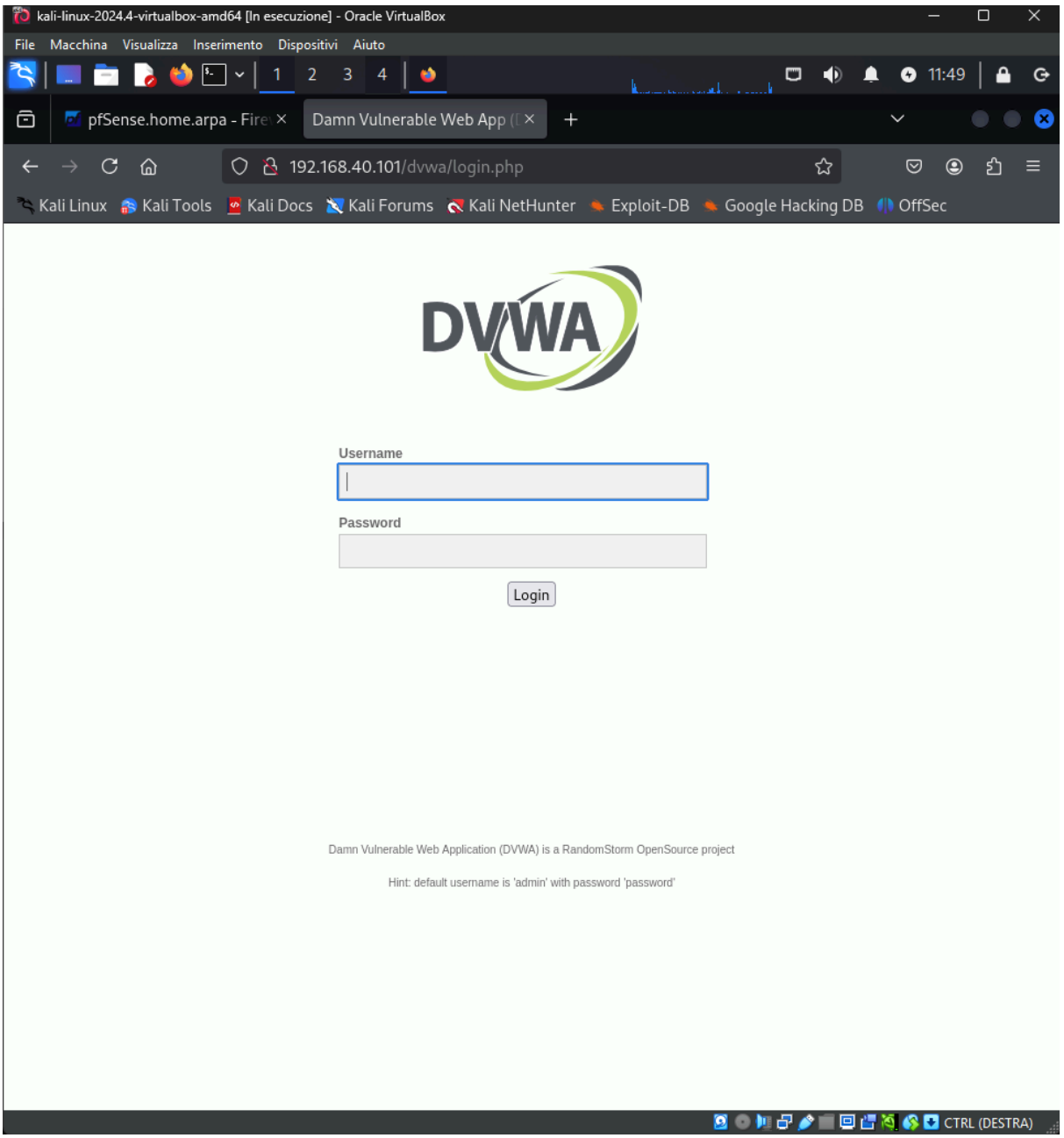


Qui possiamo inserire:
Action: che ci fa scegliere come gestire il traffico analizzato).
Interface : l'interfaccia da dove arrivano i pacchetti
Address family: a quale IP,IPv4 o IPv6 si vuole applicare la policy.
Protocol: quale protocollo vogliamo (es. tcp,udp,icmp)
Source: qui scegliamo che tipo di sorgente vogliamo inserire, come un singolo IP, oppure una rete intera.
Destination: in questa sezione scegliamo che tipo di sorgente inserire, come un singolo IP, oppure una rete intera come destinatario. Nel campo valorizzato con «source address» si andranno ad inserire eventualmente gli indirizzi IP o indirizzi rete in notazione CIDR.
Destination port range: qui specifichiamo le porte di destinazione. Si possono specificare: singole porte, intervalli, (es . Porta 80 :HTTP).

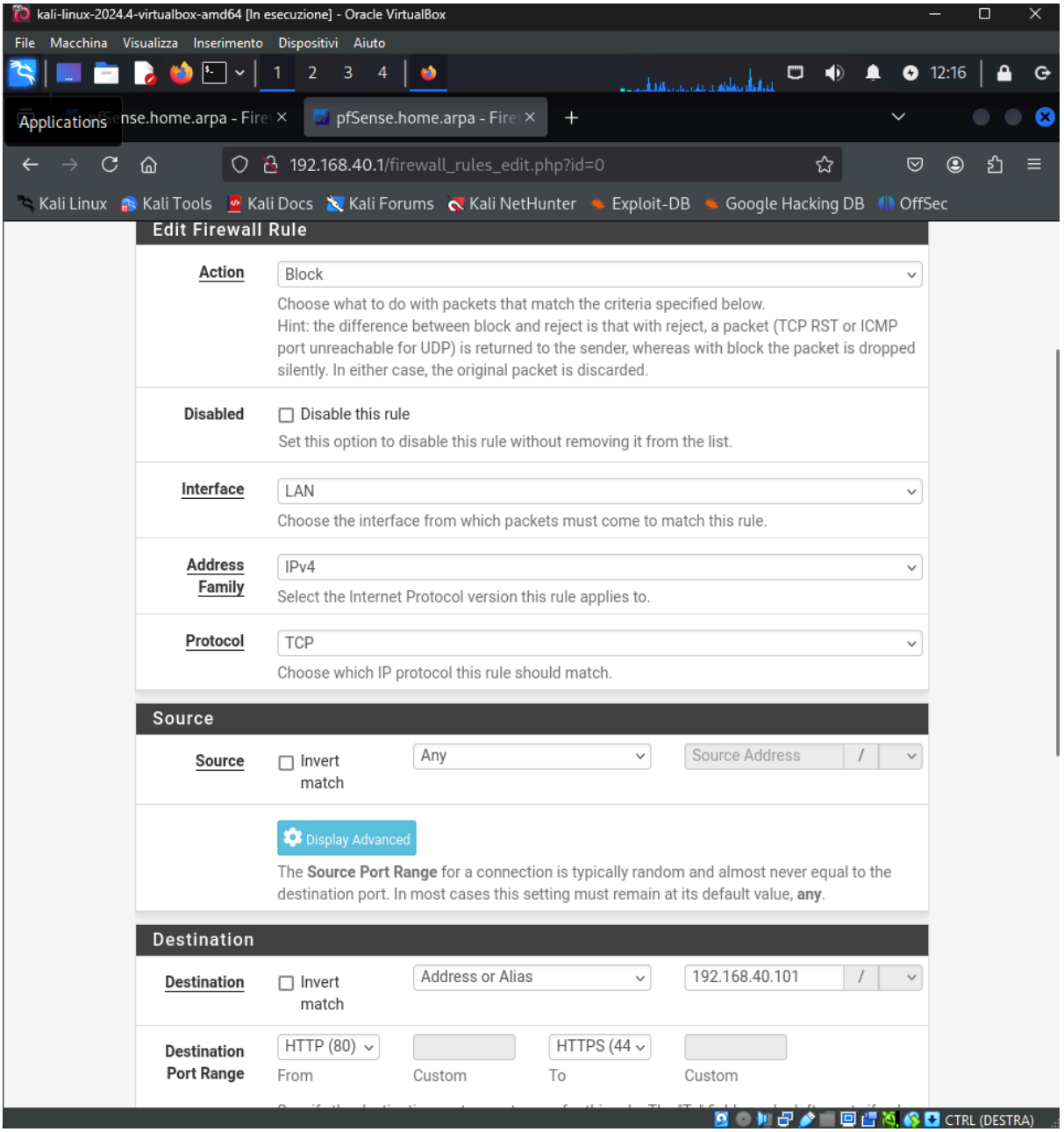
Ora creiamo una regola Firewall che blocca l’accesso alla DVWA(su Metasploitable) dalla macchina Kali Linux e ne impedisca di conseguenza lo scan.

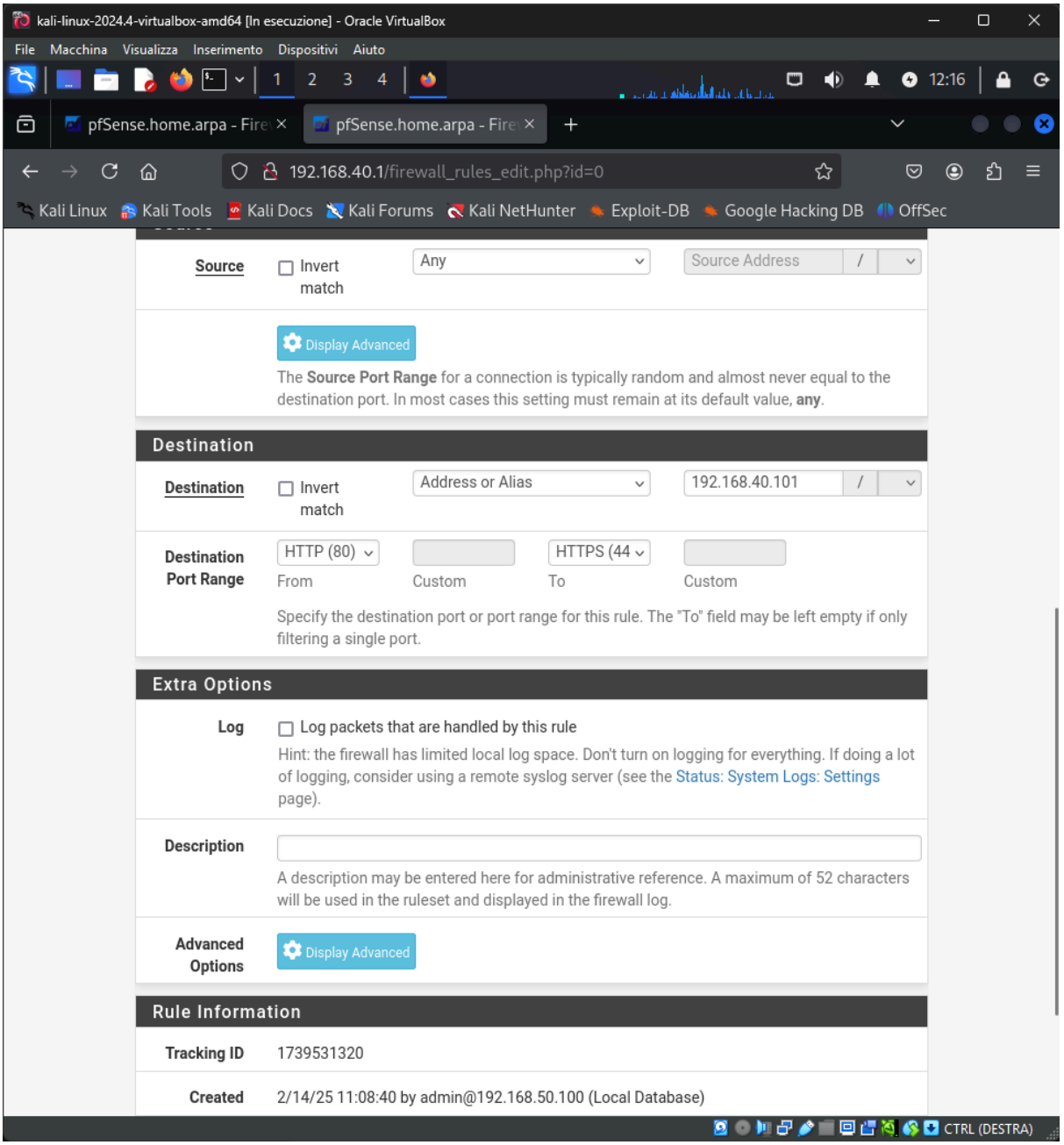


.

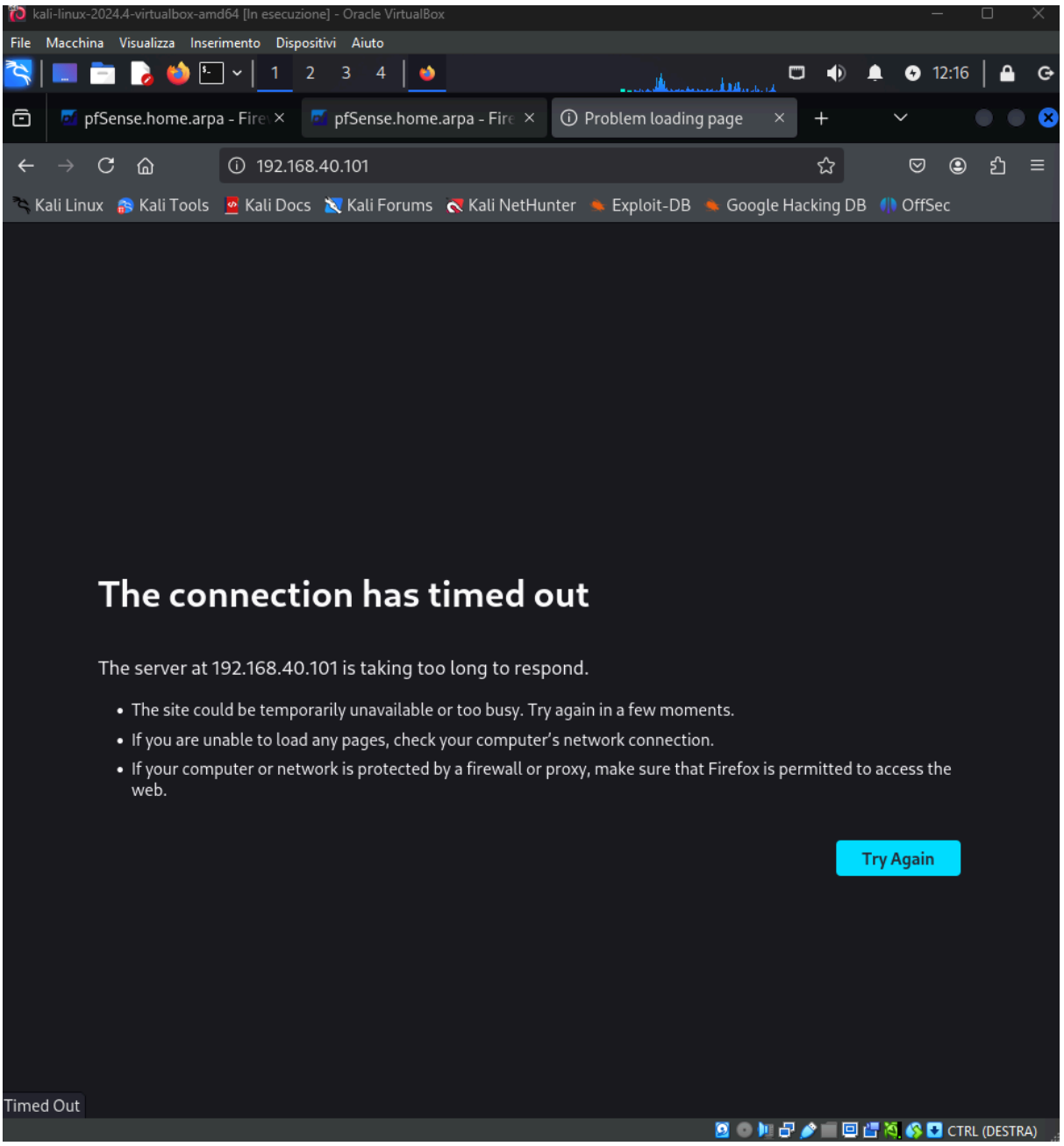


Come possiamo vedere da Kali se nel nostro Browser inseriamo l'indirizzo IP di Metasploitable2 ci permette di visionare l'accesso alla DVWA.
Ora creiamo una regola Firewall come abbiamo visto prima per bloccarne l'accesso.


kali-linux-2024.4-virtualbox-amd64 [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Applications
pfSense.home.arpa - Fire
192.168.40.1/firewall_rules_edit.php?id=0
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
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
Choose which IP protocol this rule should match.
Source
Source
Invert match
Any
Source Address
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
Address or Alias
192.168.40.101
Destination Port Range
HTTP (80)
From
Custom
HTTPS (44
To
Custom
CTRL (DESTRA)



Come si può notare dalle immagini sopra abbiamo creato una regola impostando:
Action: Block (per bloccare il traffico)
Interface: LAN (dove si trova Kali)
Protocol:TCP (perchè vogliamo bloccare il traffico internet http)
Source: tutti ma potevamo mettere anche solo l'IP di Kali
Destination: il nostro indirizzo ip con il range della porta 80 e 443 di default rispettivamente HTTP E HTTPS.



Come possiamo vedere una volta impostato il blocco non ci viene più data la possibilità di connessione.