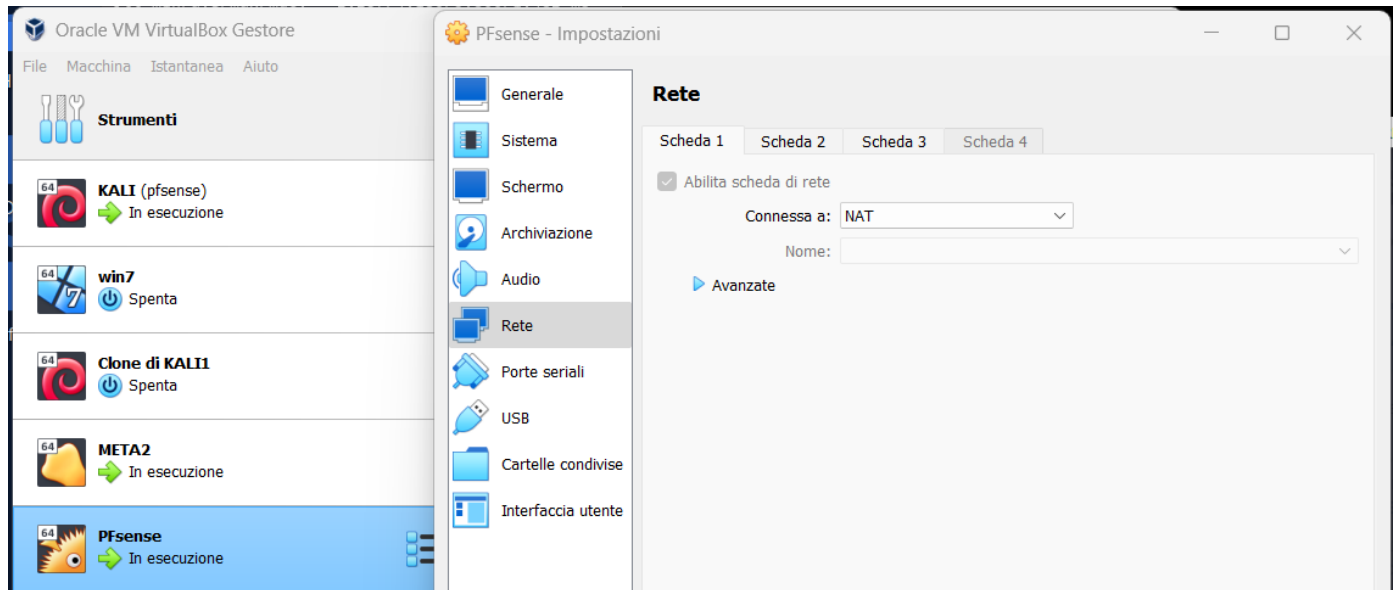
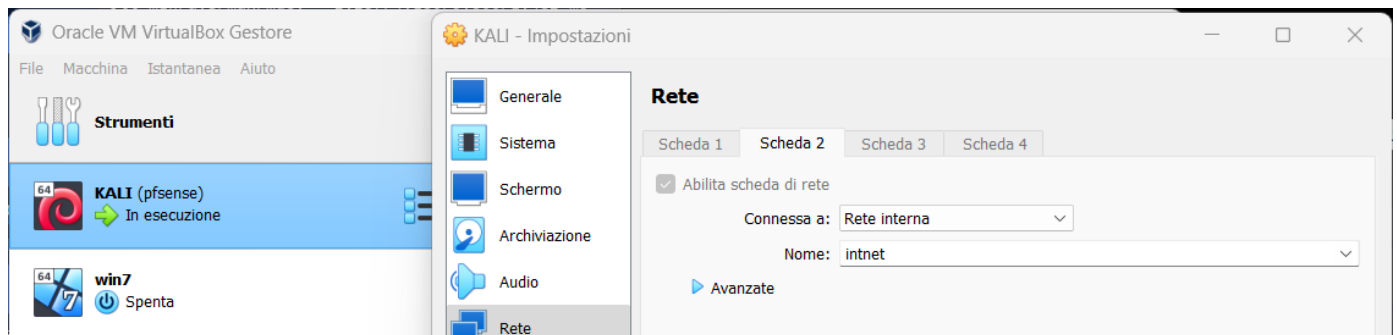
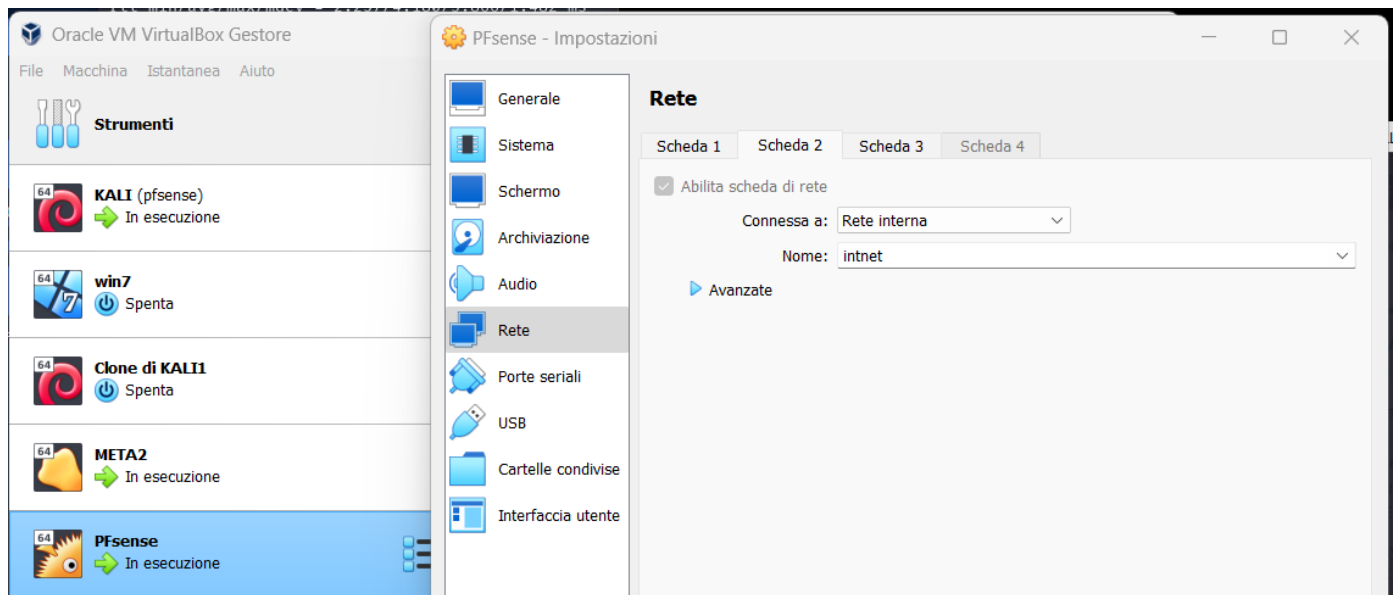


FIREWALL RULES PFSENSE W9D4

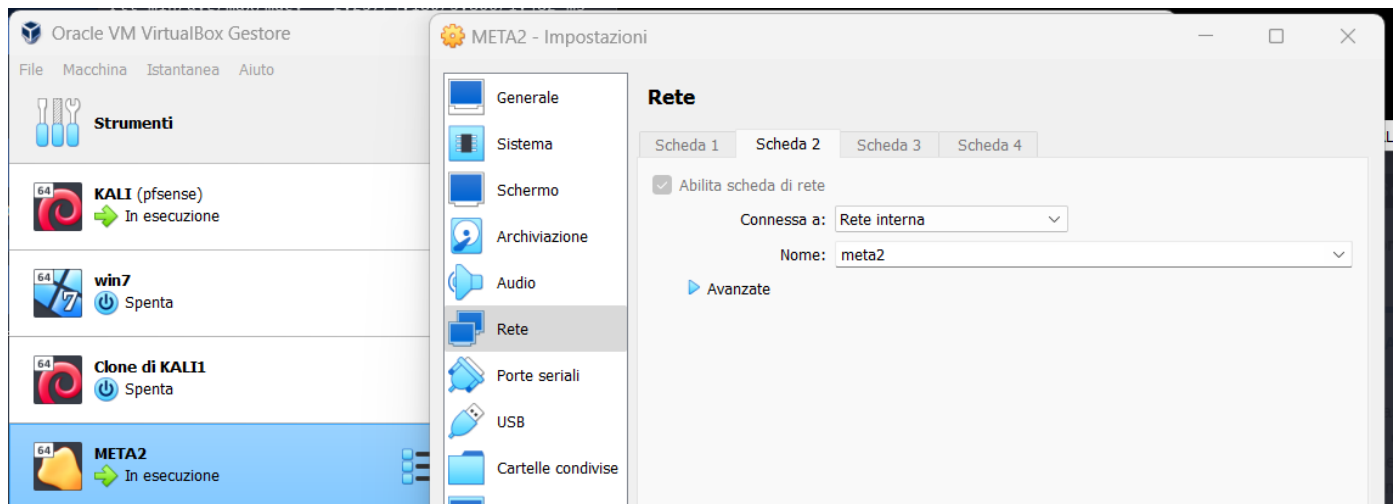
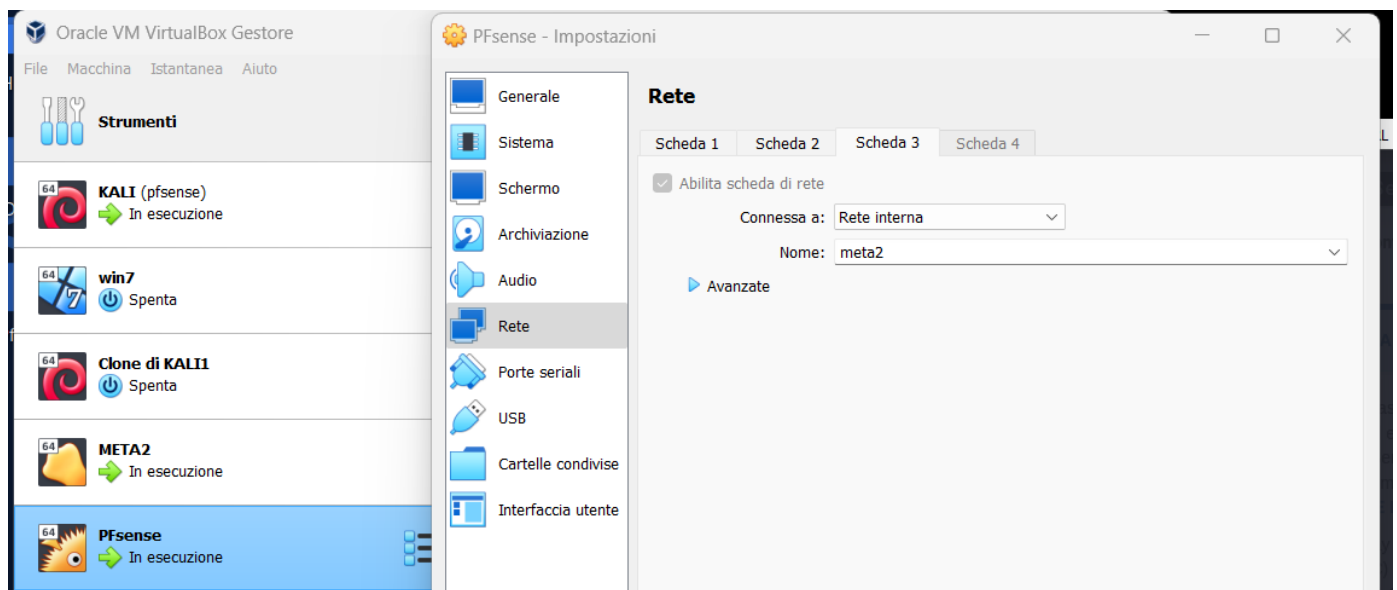
una volta scaricato pfsense e installato su VMBOX
impostiamo le reti dei 3 dispositivi come segue come segue
la prima sarà NAT



la seconda LAN nominata intnet associata a KALI



la terza sempre LAN rinominata meta2 associata a metaexplitable 2



impostiamo la rete di cali

```
(kali@kali)-[~]  
$ sudo nano /etc/network/interfaces  
[sudo] password for kali:
```

come segue

```
File Actions Edit View Help
GNU nano 7.2 /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
#iface eth0 inet static
iface eth0 inet dhcp
#address 192.168.50.102
#address 192.168.1.12/24
#address 192.168.1.102/24
gateway 192.168.1.1
#network 192.168.50.0
netmask 255.255.255.0
#broadcast 192.168.50.255
#gateway 192.168.50.1
network 192.168.1.0
```

apriamo una pagina di firefox e inseriamo l'indirizzo
192.168.1.1 per entrare nelle impostazioni di efsense

configuro una nuova interfaccia con come 192.162.50.1

abilitiamo la scheda di rete lan 2 riferita a metaexploitable2

The screenshot shows the pfSense web interface. The top navigation bar includes 'System', 'Interfaces', 'Firewall', 'Services', 'VPN', 'Status', 'Diagnostics', and 'Help'. The 'Interfaces' menu is open, showing options: 'Assignments', 'WAN', 'LAN', and 'LAN2'. Below the menu, the 'Interface Assignments' table is visible, listing three interfaces: WAN, LAN, and lan2, each with a corresponding network port.

Interface	Network port
WAN	em0 (08:00:27:bb:54:fe)
LAN	em1 (08:00:27:fd:14:e1)
lan2	em2 (08:00:27:7c:0f:b0)

abilito il dhcp server della linea 2

pf

sense

COMMUNITY EDITION

System

Interfaces

Firewall

Services

VPN

WARNING: The 'admin' account password is set to the default value

Status / Dashboard

Auto Config Backup

Captive Portal

DHCP Relay

DHCP Server

LAN

LAN2

General DHCP Options

DHCP Backend

ISC DHCP

Enable

☒ Enable DHCP server on LAN2 interface

BOOTP

☐ Ignore BOOTP queries

Deny Unknown Clients

Allow all clients

When set to **Allow all clients**, any DHCP client will get an IP address within this scope/range on this interface. If set to **Allow known clients from any interface**, any DHCP client with a MAC address listed in a static mapping on **any** scope(s)/interface(s) will get an IP address. If set to **Allow known clients from only this interface**, only MAC addresses listed in static mappings on this interface will get an IP address within this scope/range.

Ignore Denied Clients

☐ Ignore denied clients rather than reject
This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.

Ignore Client Identifiers

☐ Do not record a unique identifier (UID) in client lease data if present in the client DHCP request
This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.

Primary Address Pool

Subnet

192.168.50.0/24

Subnet Range

192.168.50.1 - 192.168.50.254

Address Pool Range

192.168.50.100







192.168.50.200

From

To

The specified range for this pool must not be within the range configured on any other address pool for this interface.

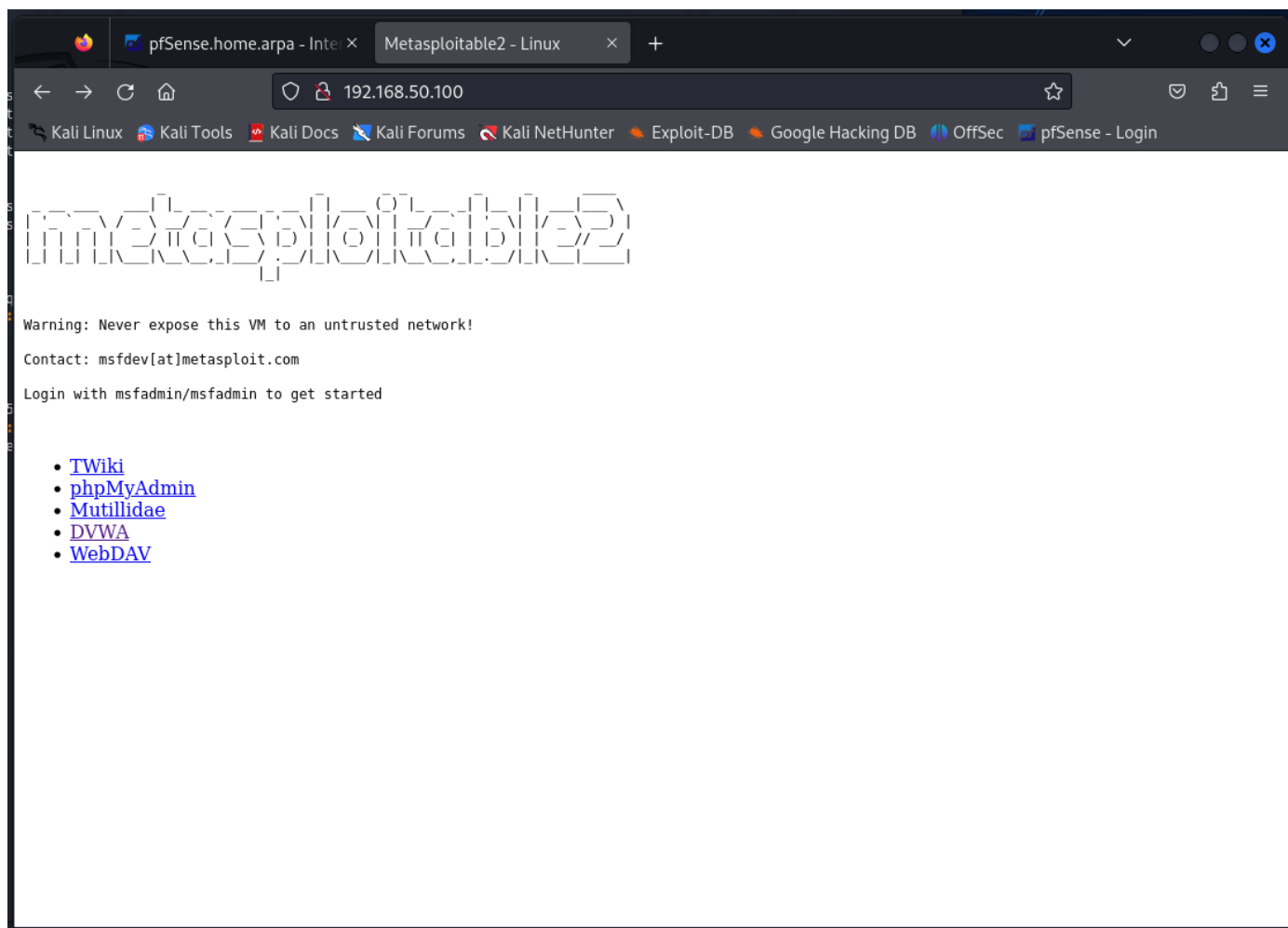
in modo da avere la rete come segue

Interfaces				
 WAN		1000baseT <full-duplex>	10.0.2.15	
 LAN		1000baseT <full-duplex>	192.168.1.1	
 LAN2		1000baseT <full-duplex>	192.168.50.1	

controlliamo su kali il nostro ip e il ping con metasploitable

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ ping 192.168.50.100  
PING 192.168.50.100 (192.168.50.100) 56(84) bytes of data.  
64 bytes from 192.168.50.100: icmp_seq=1 ttl=63 time=5.87 ms  
64 bytes from 192.168.50.100: icmp_seq=2 ttl=63 time=2.26 ms  
64 bytes from 192.168.50.100: icmp_seq=3 ttl=63 time=4.42 ms  
^C  
--- 192.168.50.100 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2038ms  
rtt min/avg/max/mdev = 2.257/4.180/5.866/1.482 ms  
(kali@kali)-[~]  
$ ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host noprefixroute  
        valid_lft forever preferred_lft forever  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000  
    link/ether 08:00:27:77:47:37 brd ff:ff:ff:ff:ff:ff  
    inet 192.168.1.100/24 brd 192.168.1.255 scope global dynamic eth0  
        valid_lft 7122sec preferred_lft 7122sec  
    inet6 fe80::a00:27ff:fe77:4737/64 scope link proto kernel_ll  
        valid_lft forever preferred_lft forever
```

accendiamo a metaexploitable digitando il suo indirizzo



e vediamo che è raggiungibile

torriamo sulla scheda di configurazione pfsense e impostiamo una regola da firewall
come segue

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.

Source

Source ☐ Invert match Address or Alias 192.168.1.100 /

[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 192.168.50.100 /

Destination Port Range

From HTTP (80) Custom To HTTP (80) Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

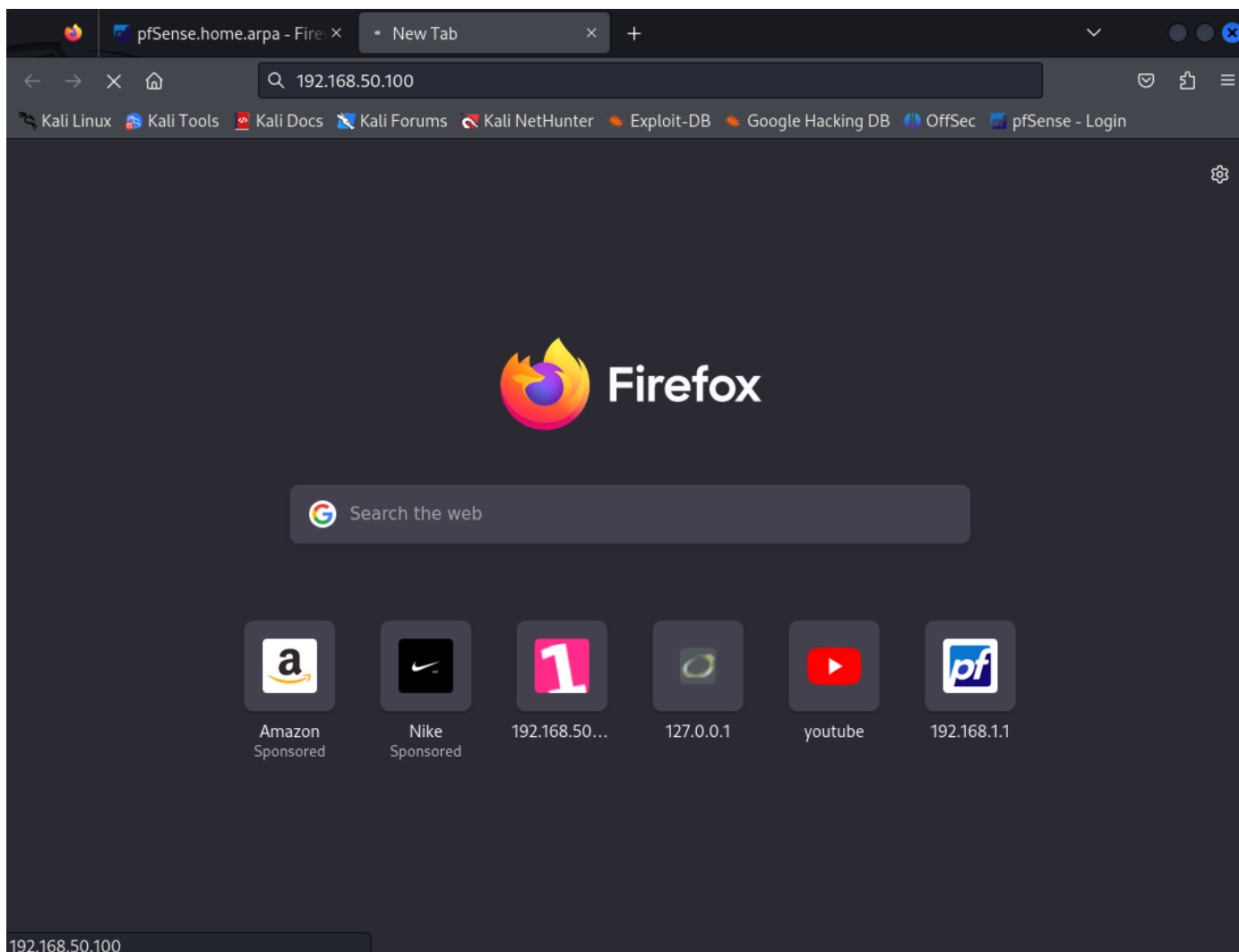
in modo da impedire al nostro kali di raggiungere metaexploitable2

salvate le impostazioni

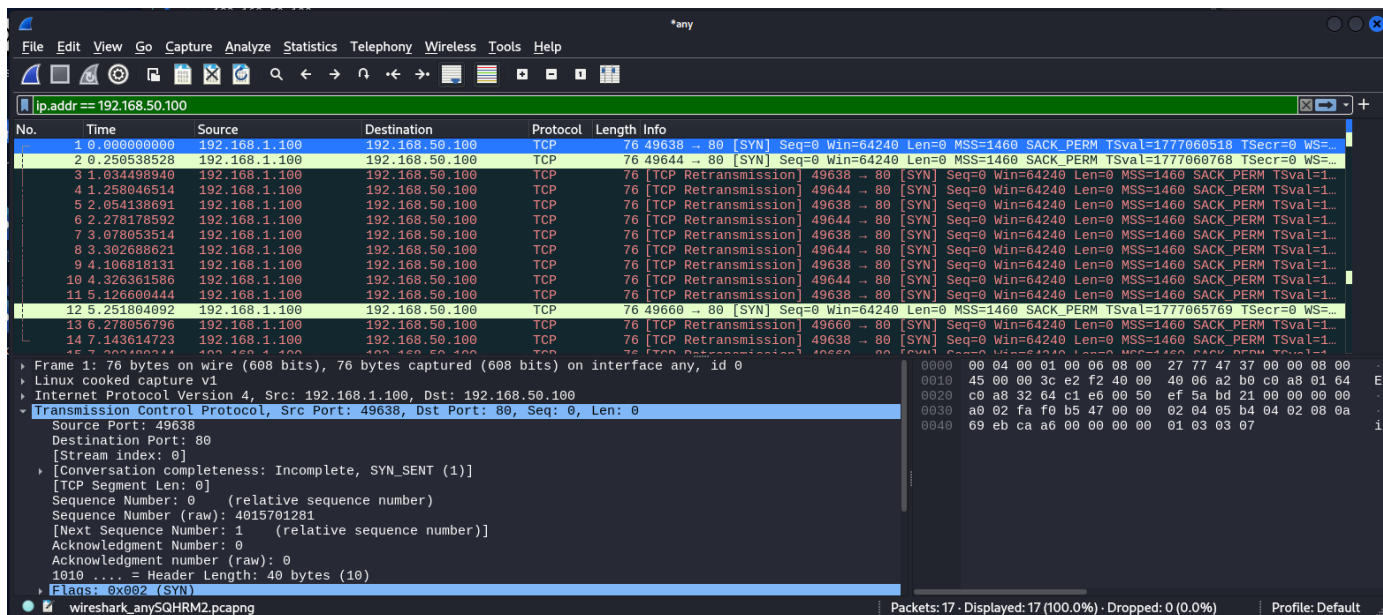
proviamo a fare il ping

```
(kali@kali)-[~]
$ ping 192.168.50.100
PING 192.168.50.100 (192.168.50.100) 56(84) bytes of data:
64 bytes from 192.168.50.100: icmp_seq=1 ttl=63 time=1.85 ms
64 bytes from 192.168.50.100: icmp_seq=2 ttl=63 time=2.56 ms
64 bytes from 192.168.50.100: icmp_seq=3 ttl=63 time=1.81 ms
64 bytes from 192.168.50.100: icmp_seq=4 ttl=63 time=0.826 ms
64 bytes from 192.168.50.100: icmp_seq=5 ttl=63 time=1.98 ms
^C
— 192.168.50.100 ping statistics —
5 packets transmitted, 5 received, 0% packet loss, time 4003ms
rtt min/avg/max/mdev = 0.826/1.804/2.556/0.557 ms
```

e funziona in quanto abbiamo inserito la regola per la porta 80 e protocollo HTTP
se aggiorniamo la pagina firefox non ci darà nessun risultato



e come vediamo dalla seguente immagine da wireshark non c'è risposta dal metaexploitable



ci saranno solo richieste SYN da parte del nostro ip