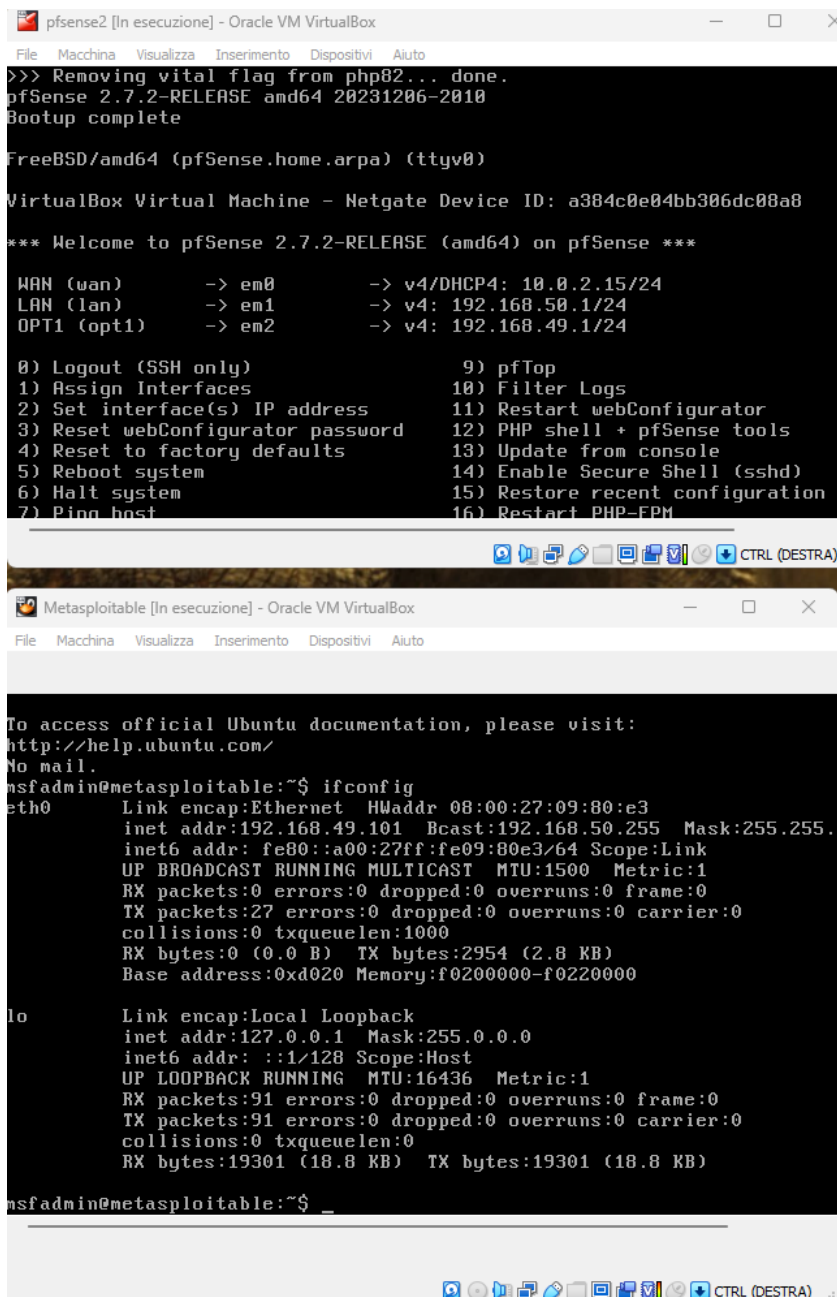


Sulla base di quanto visto, creare una regola firewall che **blocchi** l'accesso alla DVWA (su metasploitable) dalla macchina Kali Linux e ne impedisca di conseguenza lo scan. Un requisito fondamentale dell'esercizio è che le macchine Kali e Metasploitable siano su reti diverse, potete aggiungere una nuova interfaccia di rete a Pfsense in modo tale da gestire una ulteriore rete.

Connettetevi poi in Web Gui per attivare la nuova interfaccia e configurarla.

Configuriamo le tre interfacce che ci serviranno. La WAN la possiamo lasciare in dhcp; l'interfaccia LAN 192.168.50.1 in cui troveremo KALI, e l'interfaccia OPT1 192.168.49.1 in cui troveremo METASPLOITABLE. Ovviamente ho cambiato l'indirizzo di meta per impostare l'interfaccia di rete su pfsense.



```
>>> Removing vital flag from php02... done.
pfSense 2.7.2-RELEASE amd64 20231206-2010
Bootup complete

FreeBSD/amd64 (pfSense.home.arp) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: a384c0e04bb306dc08a8

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

WAN (wan)      -> em0      -> v4/DHCP4: 10.0.2.15/24
LAN (lan)      -> em1      -> v4: 192.168.50.1/24
OPT1 (opt1)    -> em2      -> v4: 192.168.49.1/24

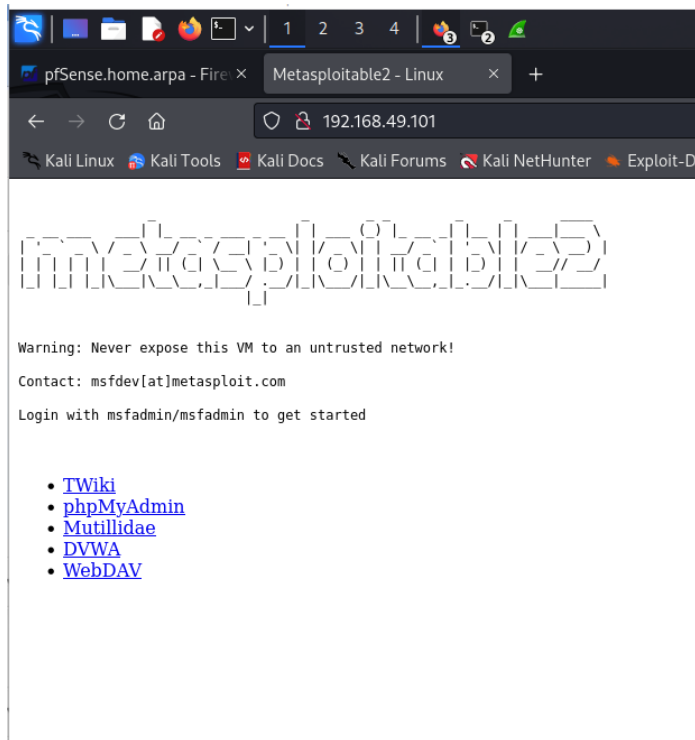
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:09:80:e3
          inet addr:192.168.49.101 Bcast:192.168.50.255 Mask:255.255.255
          inet6 addr: fe80::a00:27ff:fe09:80e3/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:27 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:2954 (2.8 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:91 errors:0 dropped:0 overruns:0 frame:0
          TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19301 (18.8 KB)  TX bytes:19301 (18.8 KB)

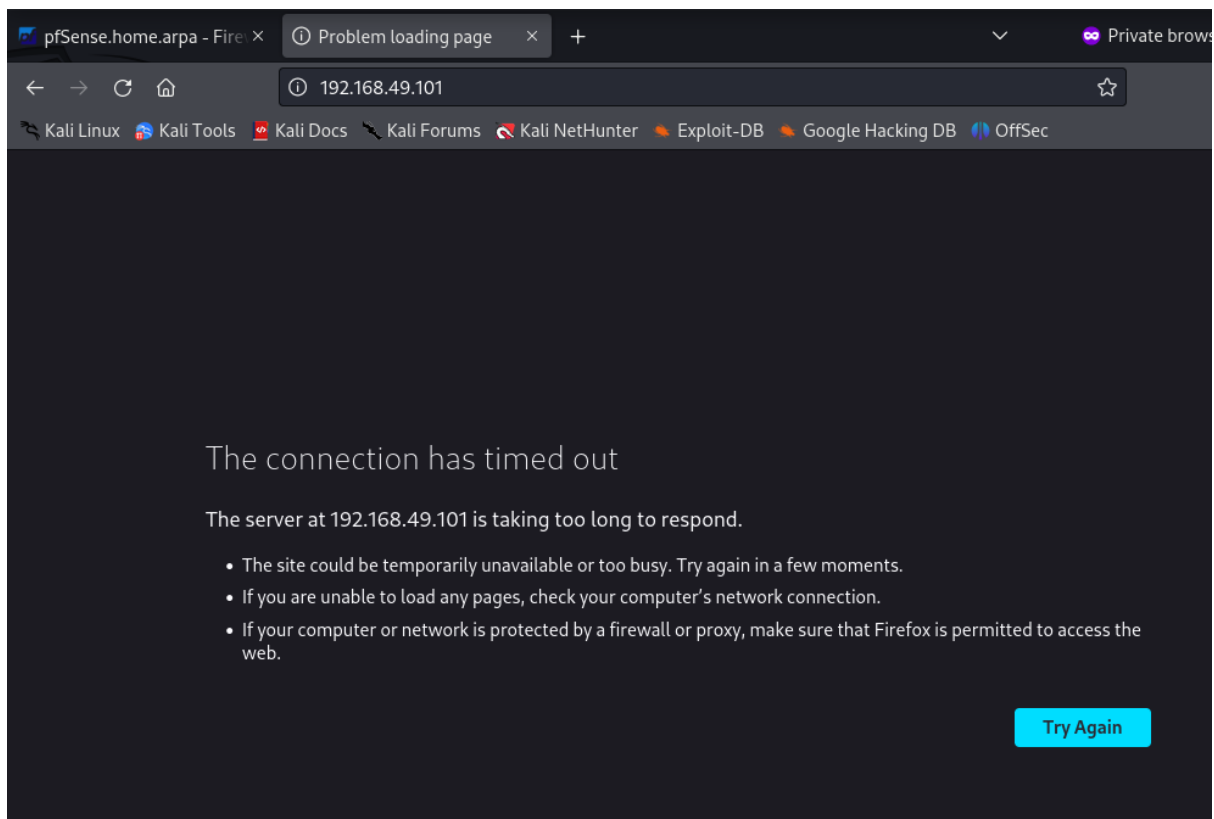
msfadmin@metasploitable:~$
```

Vediamo che da kali riusciamo a connetterci al dvwa di meta senza aver impostato la regola del firewall.



| Floating WAN LAN OPT1 | | | | | | | | | | | |
|---|-------------|----------|----------------|------|----------------|-----------|---------|-------|----------|------------------------------------|---------|
| Rules (Drag to Change Order) | | | | | | | | | | | |
| <input type="checkbox"/> | States | Protocol | Source | Port | Destination | Port | Gateway | Queue | Schedule | Description | Actions |
| <input checked="" type="checkbox"/> | ✓ 0/100 KIB | * | * | * | LAN Address | 443 80 | * | * | | Anti-Lockout Rule | |
| <input type="checkbox"/> | ✗ 0/0 B | IPv4 TCP | 192.168.50.100 | * | 192.168.49.101 | 80 (HTTP) | * | none | | | |
| <input type="checkbox"/> | ✓ 0/0 B | IPv4 * | LAN subnets | * | * | * | * | none | | Default allow LAN to any rule | |
| <input type="checkbox"/> | ✓ 0/0 B | IPv6 * | LAN subnets | * | * | * | * | none | | Default allow LAN IPv6 to any rule | |
| Add Add Delete Toggle Copy Save Separator | | | | | | | | | | | |

Andiamo a creare una regola nel firewall che impedisca all'indirizzo sorgente di connettersi al server dell'indirizzo di destinazione sulla porta 80.



Qui possiamo vedere che la regola inserita nel firewall funziona ed impedisce alla nostra macchina di entrare sul dvwa di meta.