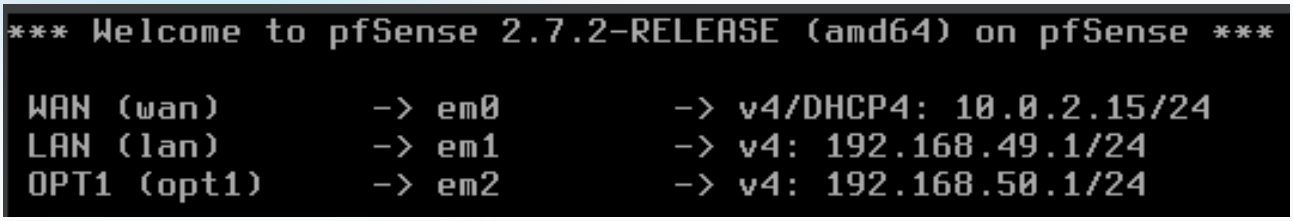
S5/L1

Creazione pratica di una regola Firewall.

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.

1. Settare le interfacce di rete su PfSense (WAN, LAN e OPT1)



2. Settiamo gli indirizzi IP di Kali Linux e di Metasploitable2

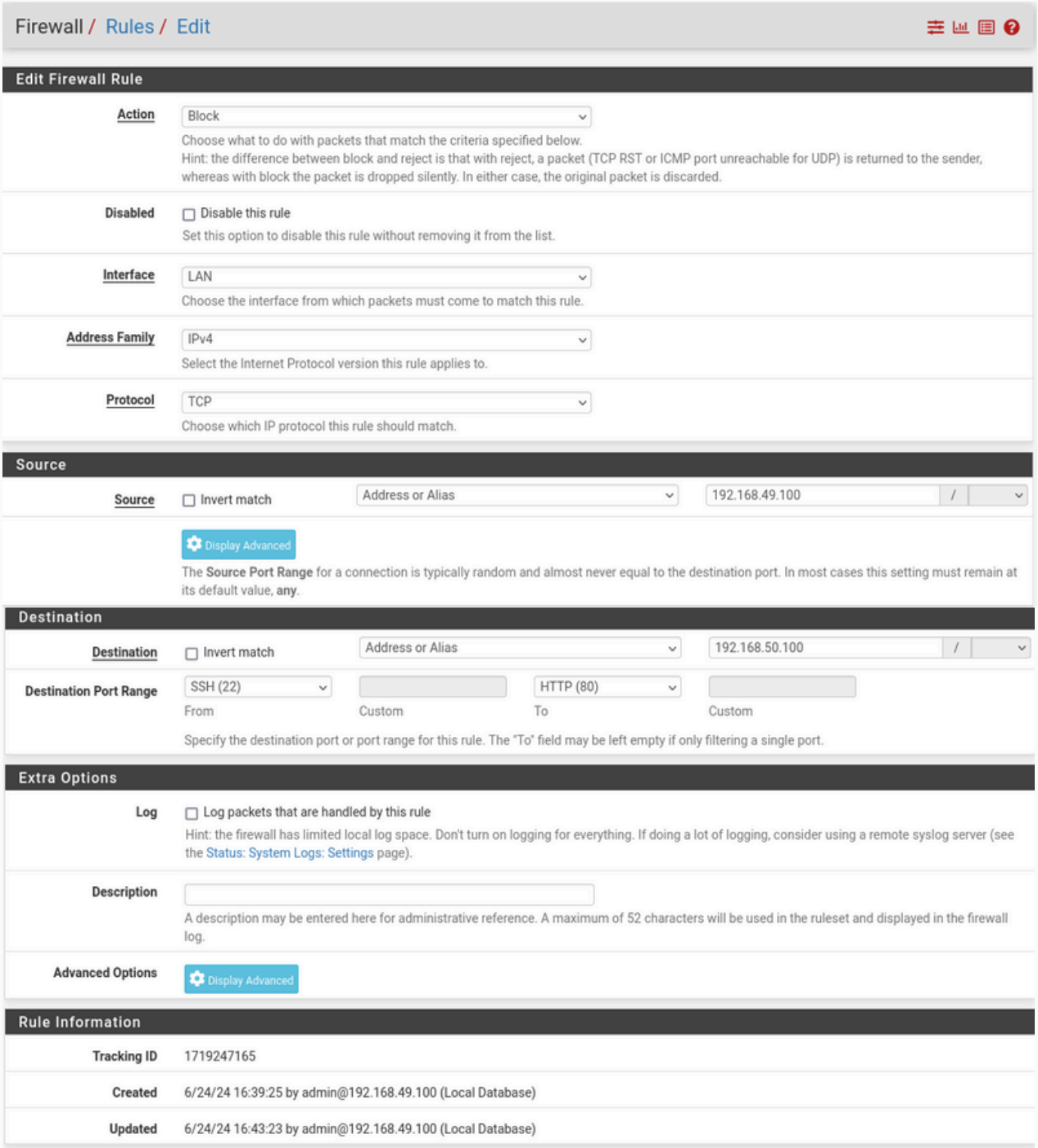
```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.49.100  netmask 255.255.255.0  broadcast 192.168.49.255
        inet6 fe80::a00:27ff:fe1e:364a  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:1e:36:4a  txqueuelen 1000  (Ethernet)
        RX packets 18  bytes 2014 (1.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 469  bytes 40150 (39.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Kali Linux - 192.168.49.100

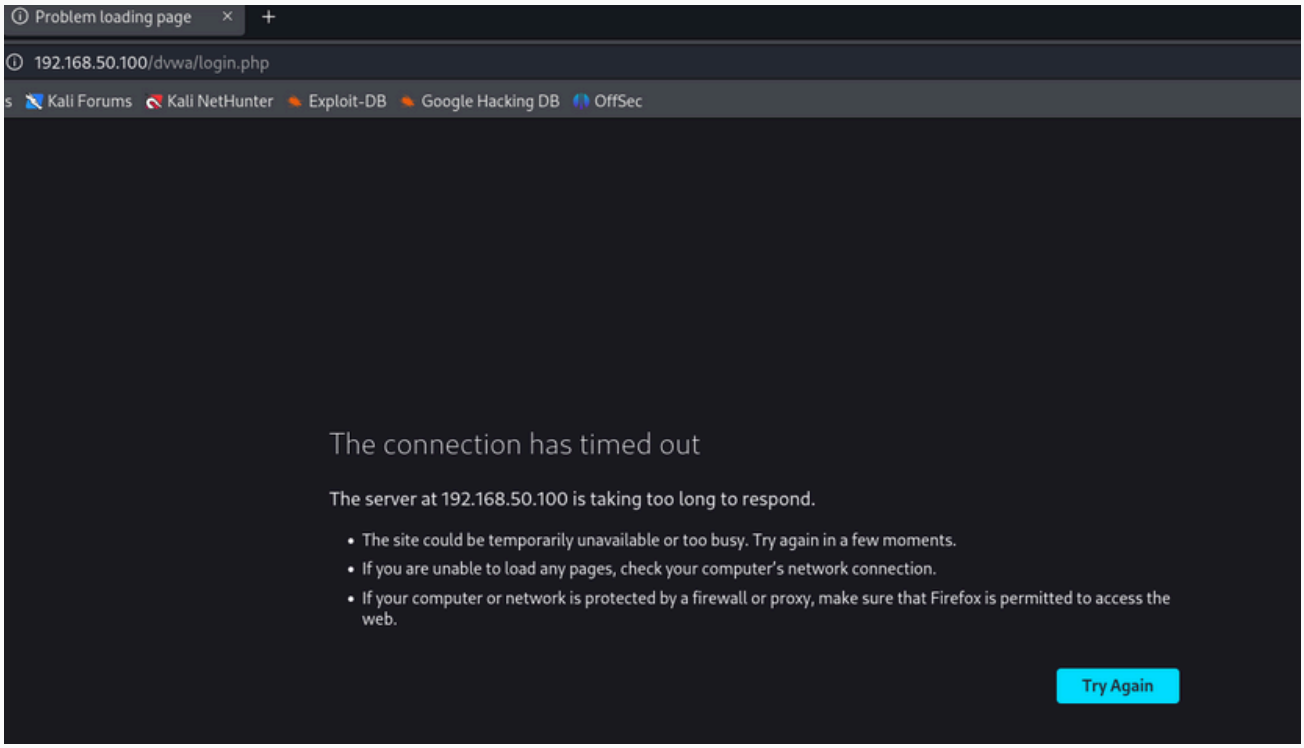
```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:6d:5f:cb
          inet addr:192.168.50.100  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe6d:5fcb/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:10 errors:0 dropped:0 overruns:0 frame:0
          TX packets:70 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:640 (640.0 B)  TX bytes:8449 (8.2 KB)
          Base address:0xd020 Memory:f0200000-f0220000
```

Metasploitable2 - 192.168.50.100

3. Una volta configurate le due reti, entriamo nella GUI Web di PfSense per impostare una nuova regola per bloccare lo scan delle porte e la connettività alla DVWA da parte di Kali Linux



4. Impostando l' interfaccia LAN (che corrisponde alla subnet di Kali), il protocollo TCP, il source IP di Kali, il destination IP di Meta e poi il range delle porte da SSH(22) a HTTP(80), il collegamento tra le due sarà interrotto.
Provando a connettersi tramite Firefox a 192.168.50.1 la connessione non viene stabilita



5. Attraverso i log dei file di sistema del firewall, possiamo vedere come la nuova regola sia efficace.

✕	Jun 24 16:25:05	OPT1	Default deny rule IPv4 (1000000103)	192.168.50.100:52687	192.168.50.1:53	UDP
✕	Jun 24 16:25:05	OPT1	Default deny rule IPv4 (1000000103)	192.168.50.100:52687	192.168.50.1:53	UDP
✕	Jun 24 16:25:05	OPT1	Default deny rule IPv4 (1000000103)	192.168.50.100:52689	192.168.50.1:53	UDP
✕	Jun 24 16:25:05	OPT1	Default deny rule IPv4 (1000000103)	192.168.50.100:52689	192.168.50.1:53	UDP
✕	Jun 24 16:25:05	OPT1	Default deny rule IPv4 (1000000103)	192.168.50.100:37326	192.168.50.1:53	UDP
✕	Jun 24 16:25:05	OPT1	Default deny rule IPv4 (1000000103)	192.168.50.100:37326	192.168.50.1:53	UDP
✕	Jun 24 16:25:05	OPT1	Default deny rule IPv4 (1000000103)	192.168.50.100:33391	192.168.50.1:53	UDP
✕	Jun 24 16:25:05	OPT1	Default deny rule IPv4 (1000000103)	192.168.50.100:33391	192.168.50.1:53	UDP
✕	Jun 24 16:25:06	OPT1	Default deny rule IPv4 (1000000103)	192.168.50.100:46904	192.168.50.1:53	UDP
✕	Jun 24 16:25:06	OPT1	Default deny rule IPv4 (1000000103)	192.168.50.100:46904	192.168.50.1:53	UDP