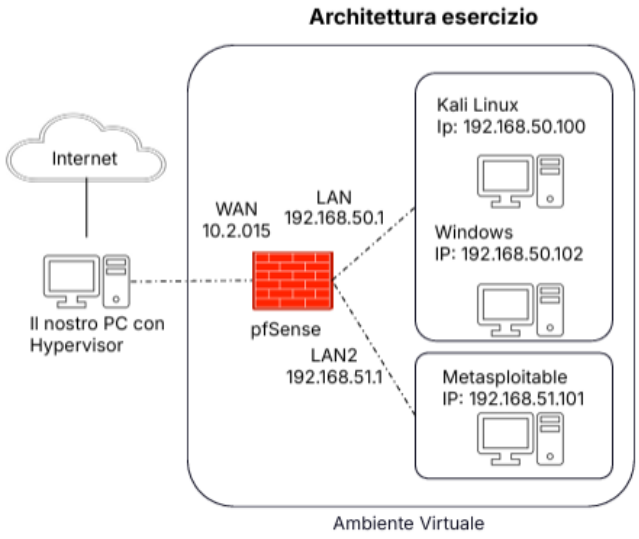
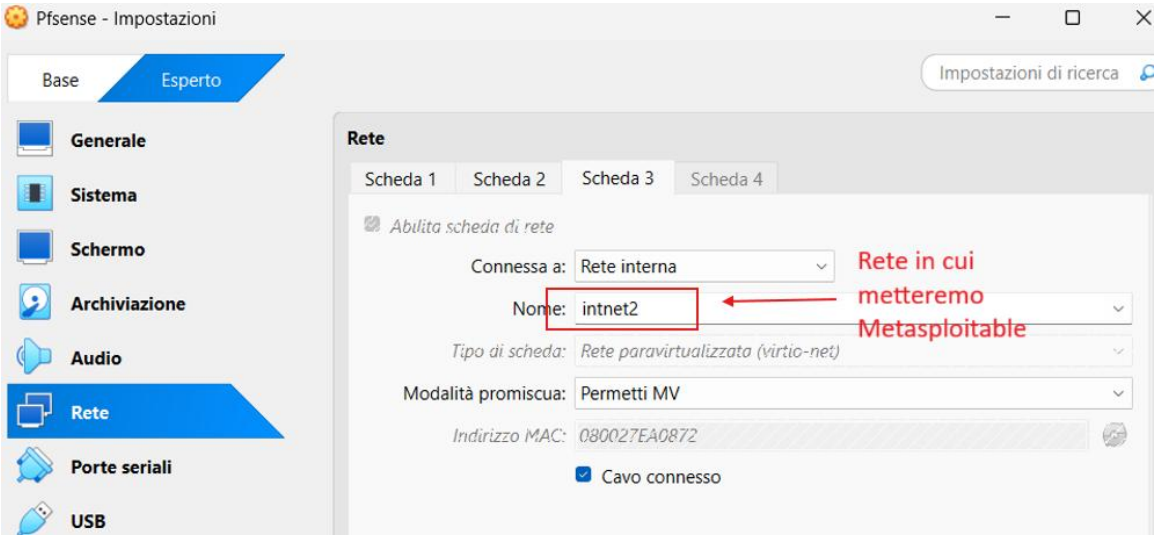
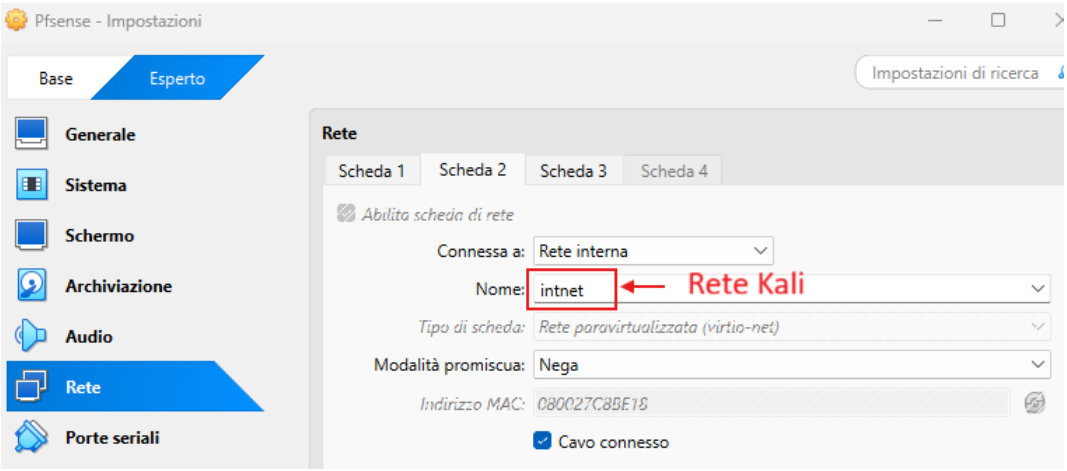


Configurazione reti in VirtualBox

pfSense

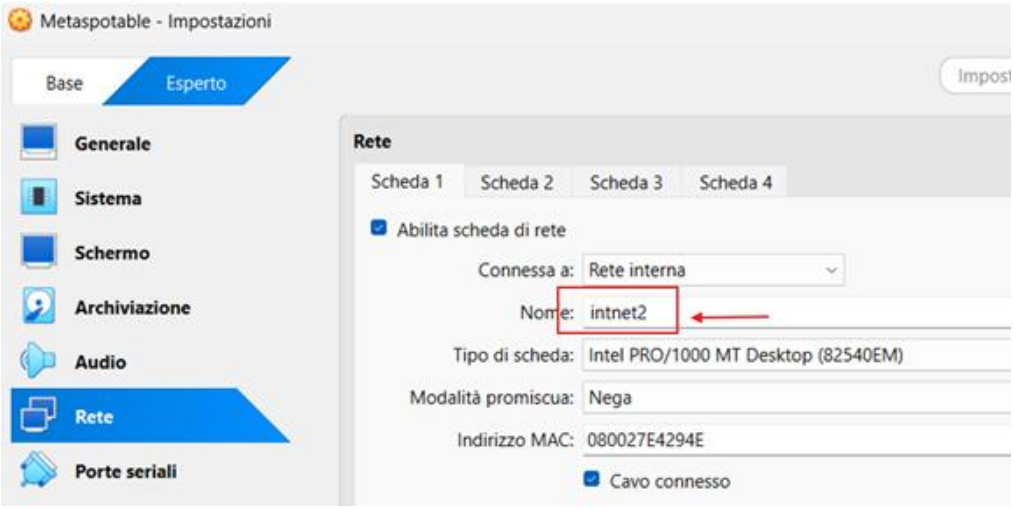
In pfSense configureremo due reti distinte, una per Kali e una per Metasploitable





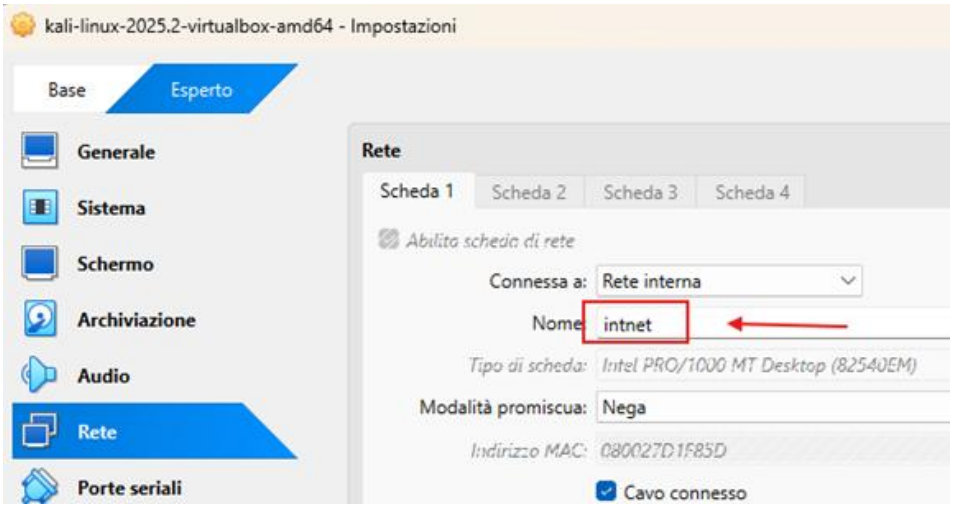
Metasploitable

Metasploitable si troverà dentro una delle 2 reti di pfSense **intenet2**



Kali

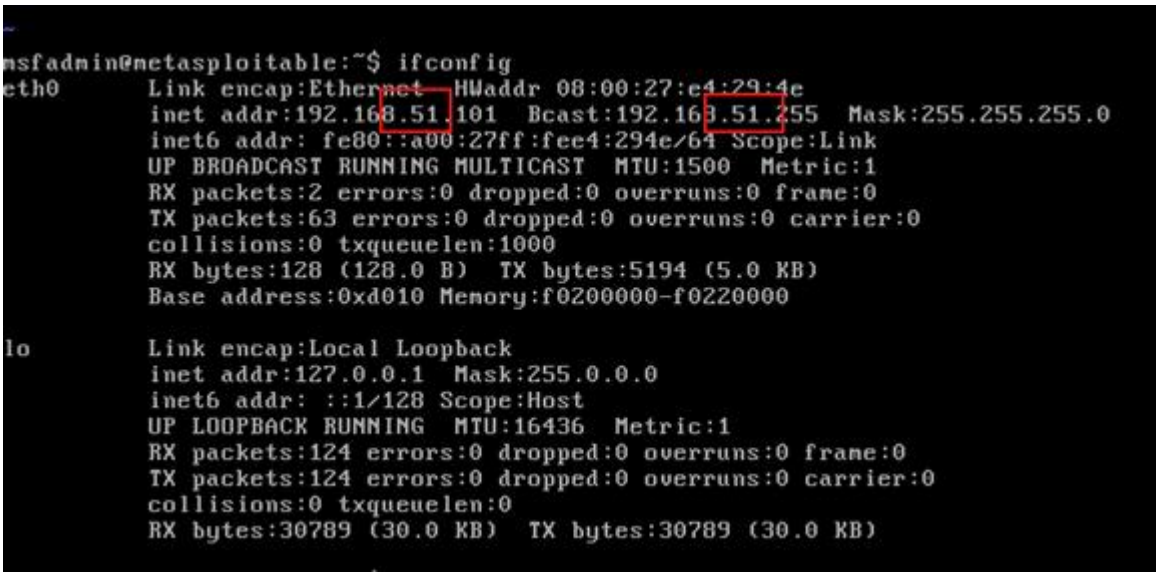
Kali si troverà dentro l'altra delle due reti interne di pfSense **intnet**



Configurazione interne delle VM

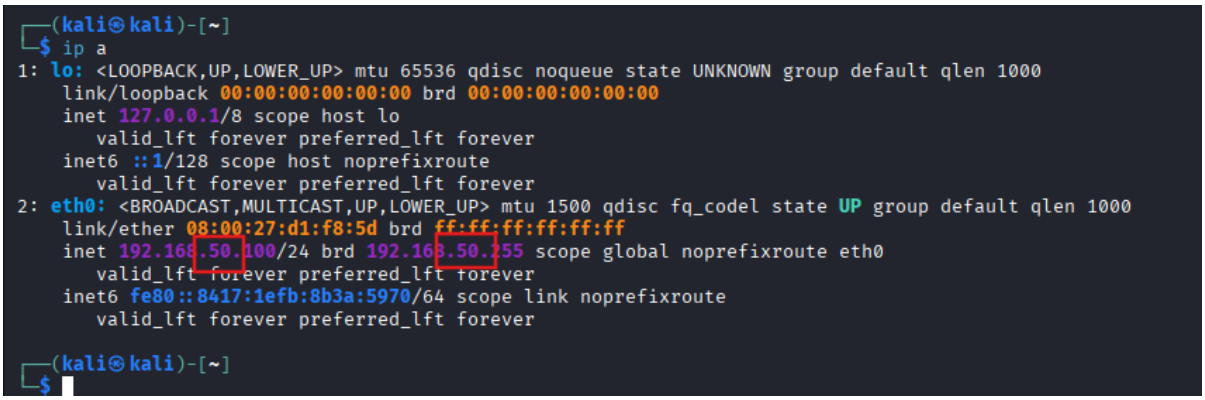
Metasploitable

Metasploitable si troverà dentro una rete (vedi immagine sotto).



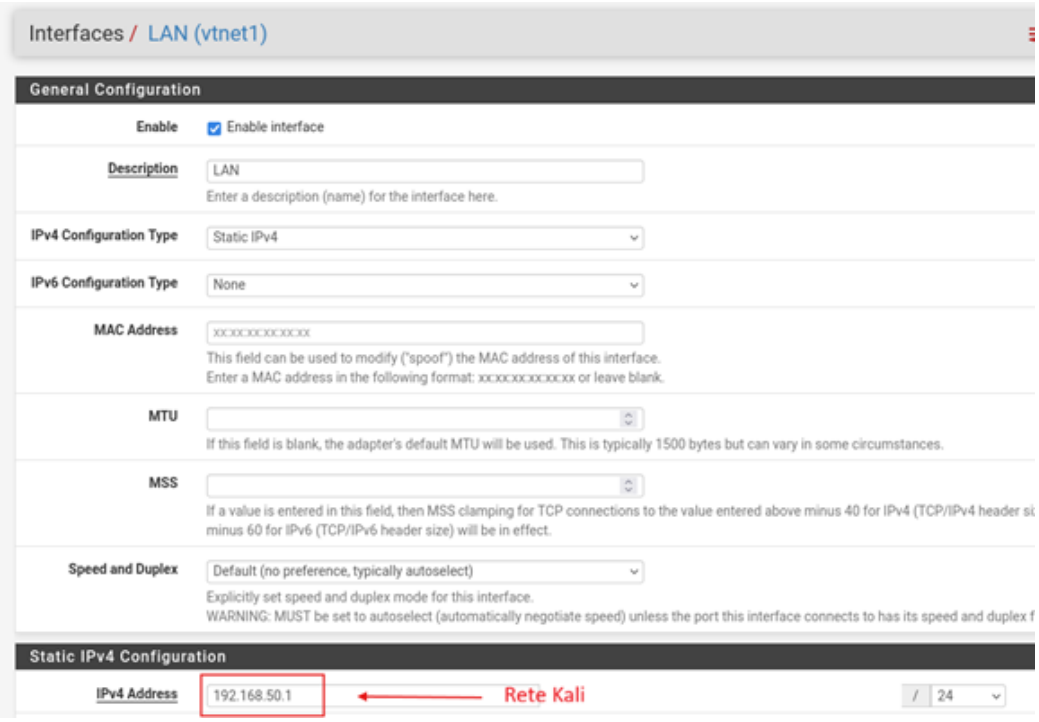
Kali

Kali si troverà dentro l'altra rete.

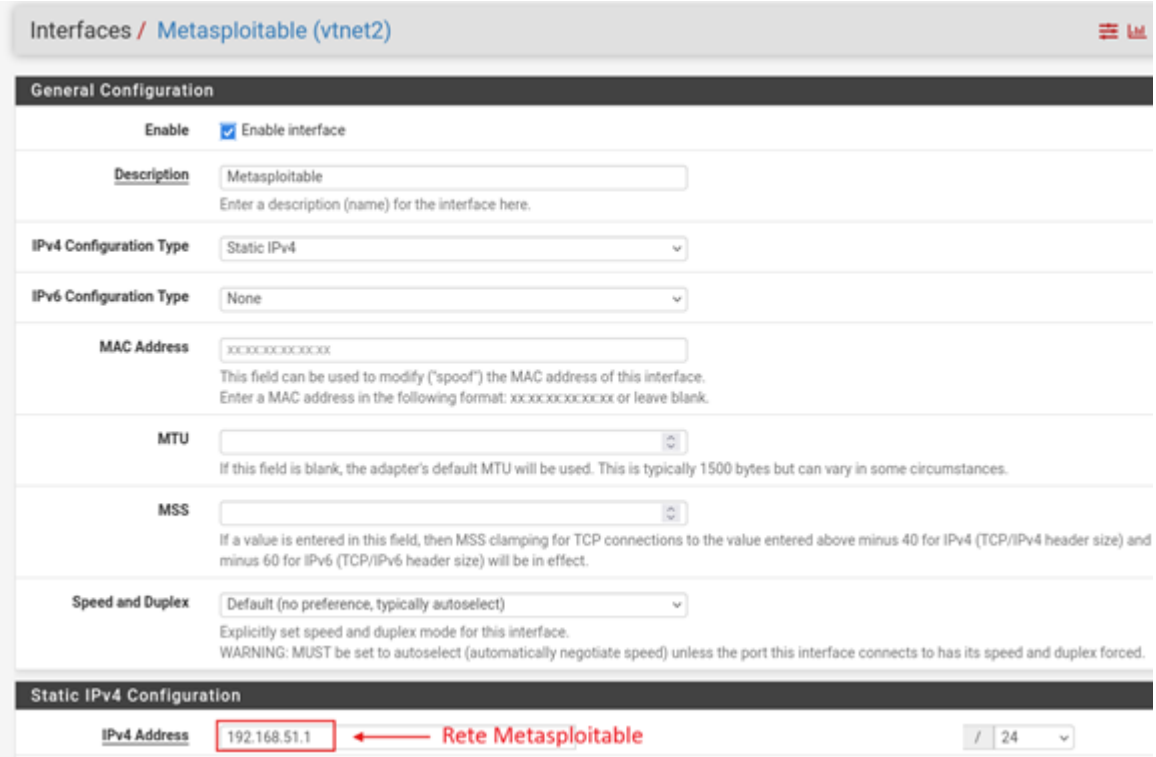


Configurazione pfSense

Kali



Metasploitable



Test Kali > Metasploitable senza regole di firewall

Ping

Facendo un ping da Kali a Metasploitable vediamo che le due macchine comunicano

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.51.101
PING 192.168.51.101 (192.168.51.101) 56(84) bytes of data.
64 bytes from 192.168.51.101: icmp_seq=1 ttl=63 time=3.91 ms
64 bytes from 192.168.51.101: icmp_seq=2 ttl=63 time=3.17 ms
64 bytes from 192.168.51.101: icmp_seq=3 ttl=63 time=4.80 ms
^C
── 192.168.51.101 ping statistics ──
3 packets transmitted, 3 received, 0% packet loss, time 2001ms
rtt min/avg/max/mdev = 3.173/3.959/4.799/0.664 ms
```

Traceroute

Con il Traceroute da Kali a Metasploitable notiamo che la comunicazione passa per il firewall pfSense

```
┌──(kali㉿kali)-[~]
└─$ traceroute 192.168.51.101
traceroute to 192.168.51.101 (192.168.51.101), 30 hops max, 60 byte packets
 1  pfSense.home.arpa (192.168.50.1)  4.911 ms  4.634 ms  4.415 ms
 2  192.168.51.101 (192.168.51.101)  6.442 ms  6.224 ms  5.957 ms
```

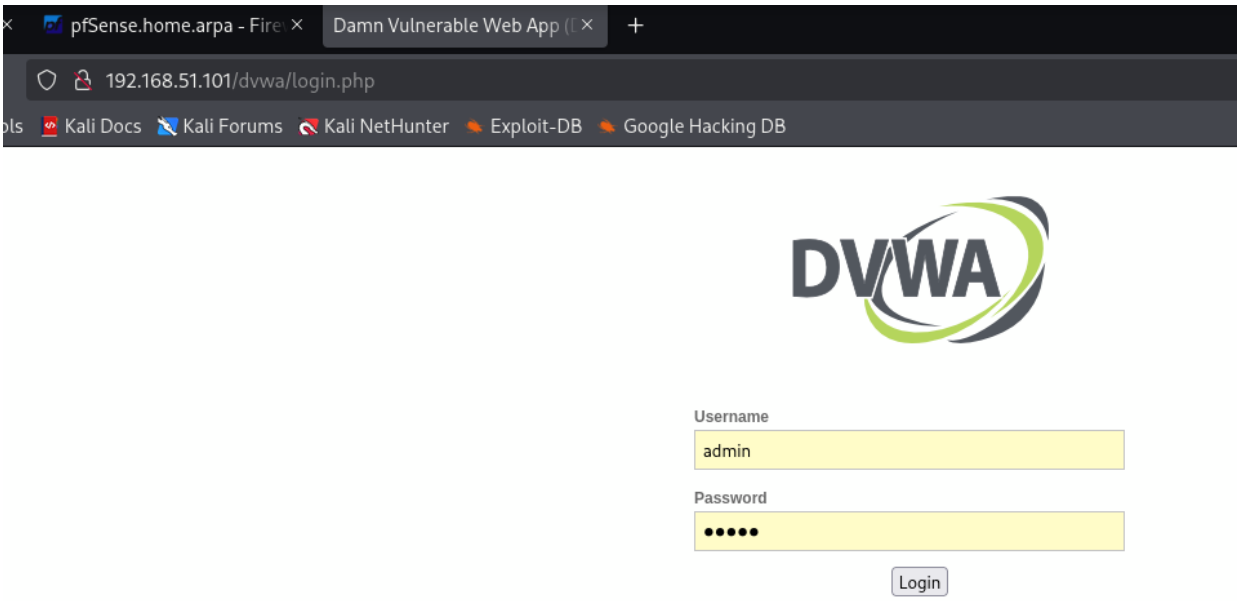
Wireshark

Anche monitorando i pacchetti del ping su Wireshark notiamo che la destinazione risponde

```
    22 21.092478372  192.168.51.101          192.168.50.100          ICMP       98 Echo (ping) reply    id=0x0006, seq=4/1024, ttl=63 (request in 21)
    23 22.090942334  192.168.50.100          192.168.51.101          ICMP       98 Echo (ping) request  id=0x0006, seq=5/1280, ttl=64 (reply in 24)
    24 22.093706053  192.168.51.101          192.168.50.100          ICMP       98 Echo (ping) reply    id=0x0006, seq=5/1280, ttl=63 (request in 23)
    25 23.096685756  192.168.50.100          192.168.51.101          ICMP       98 Echo (ping) request  id=0x0006, seq=6/1536, ttl=64 (reply in 26)
    26 23.101350419  192.168.51.101          192.168.50.100          ICMP       98 Echo (ping) reply    id=0x0006, seq=6/1536, ttl=63 (request in 25)
    27 24.098765789  192.168.50.100          192.168.51.101          ICMP       98 Echo (ping) request  id=0x0006, seq=7/1792, ttl=64 (reply in 28)
    28 24.102642918  192.168.51.101          192.168.50.100          ICMP       98 Echo (ping) reply    id=0x0006, seq=7/1792, ttl=63 (request in 27)
    29 25.100532812  192.168.50.100          192.168.51.101          ICMP       98 Echo (ping) request  id=0x0006, seq=8/2048, ttl=64 (reply in 30)
    30 25.103854871  192.168.51.101          192.168.50.100          ICMP       98 Echo (ping) reply    id=0x0006, seq=8/2048, ttl=63 (request in 29)
    31 26.177919760  192.168.50.100          192.168.51.101          ICMP       98 Echo (ping) request  id=0x0006, seq=9/2304, ttl=64 (reply in 32)
    32 26.180732272  192.168.51.101          192.168.50.100          ICMP       98 Echo (ping) reply    id=0x0006, seq=9/2304, ttl=63 (request in 31)
    33 27.193514901  192.168.50.100          192.168.51.101          ICMP       98 Echo (ping) request  id=0x0006, seq=10/2560, ttl=64 (reply in 34)
    34 27.196226124  192.168.51.101          192.168.50.100          ICMP       98 Echo (ping) reply    id=0x0006, seq=10/2560, ttl=63 (request in 33)
```

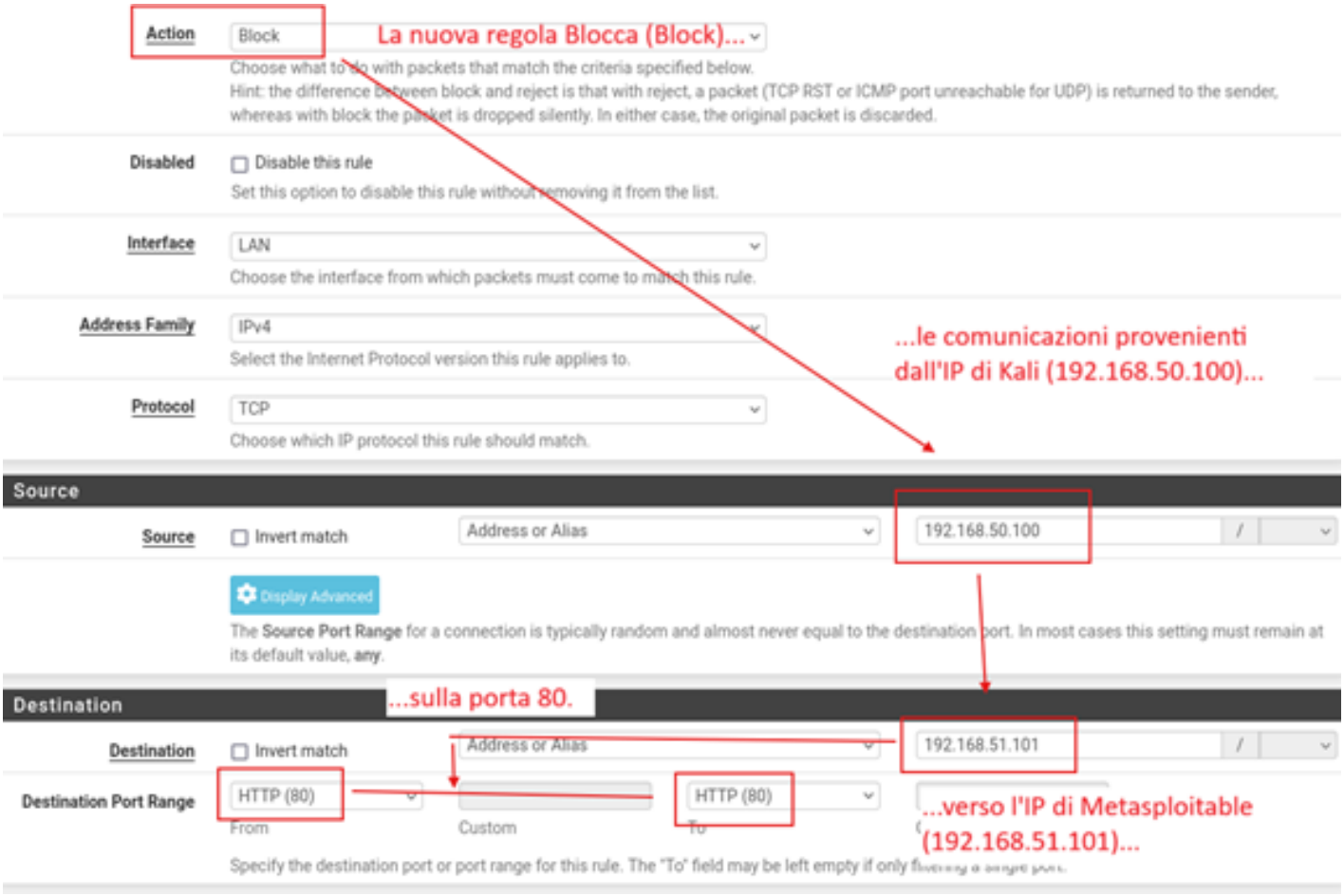
DVWA

Accediamo regolarmente a DVWA



Regola di firewall che impedisce a Kali di raggiungere Metasploitable

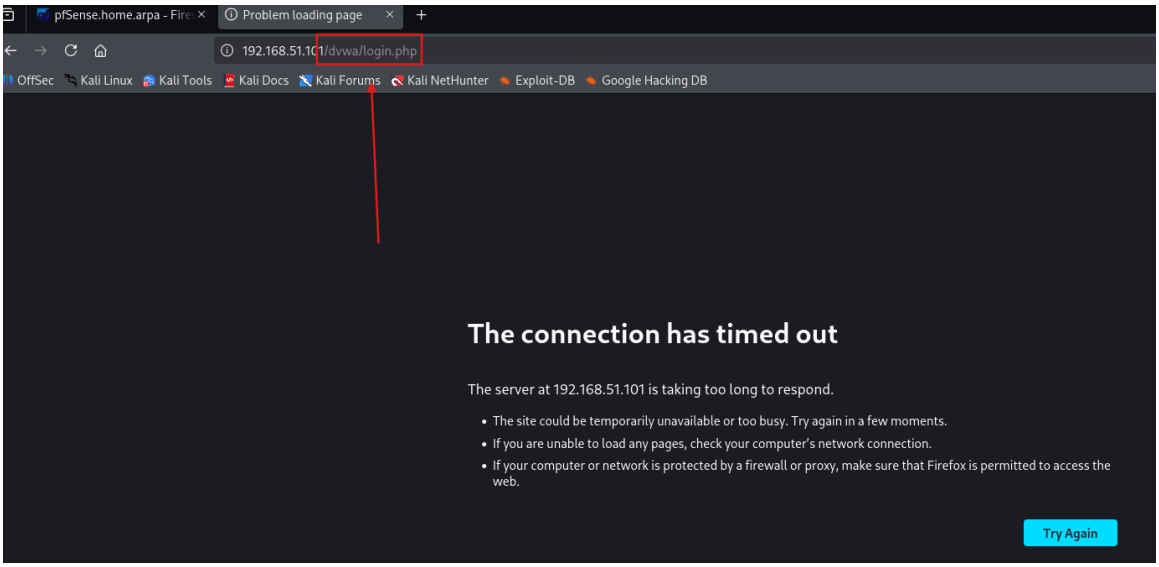
Configurazione regola in pfSense



Ping

Il ping funzionerà perché l'IP di Metasploitable è raggiungibile, ma non avremo accesso a DWA perché gira sulla porta 80

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.51.101
PING 192.168.51.101 (192.168.51.101) 56(84) bytes of data.
64 bytes from 192.168.51.101: icmp_seq=1 ttl=63 time=2.75 ms
64 bytes from 192.168.51.101: icmp_seq=2 ttl=63 time=4.39 ms
64 bytes from 192.168.51.101: icmp_seq=3 ttl=63 time=3.03 ms
```



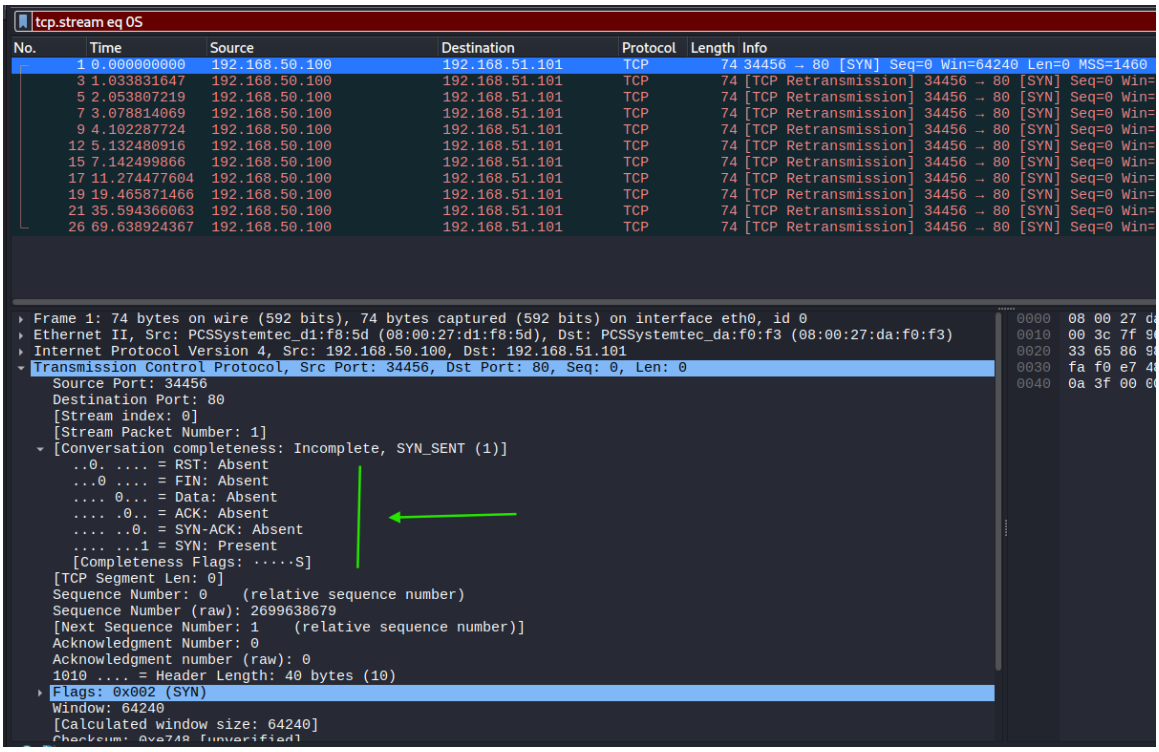
Facendo nmap notiamo che lo stato della porta 80 è **filtered**

```
┌──(kali㉿kali)-[~]
└─$ nmap -p 80 192.168.51.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-10 09:35 EDT
Nmap scan report for 192.168.51.101
Host is up (0.0021s latency).

PORT   STATE    SERVICE
80/tcp filtered http

Nmap done: 1 IP address (1 host up) scanned in 0.40 seconds
```

Su Wireshark vedremo che il client invia richieste senza ricevere risposta dal server



Dal log di pfSense vedremo inoltre i tentativi di accesso bloccati

✕	Sep 9 21:16:29	WAN	Block private networks from WAN block 192.168/16 (12004)	192.168.1.17:17500	192.168.1.255:17500	UDP
✕	Sep 9 21:16:59	WAN	Block private networks from WAN block 192.168/16 (12004)	192.168.1.17:17500	192.168.1.255:17500	UDP
✕	Sep 9 21:17:29	WAN	Block private networks from WAN block 192.168/16 (12004)	192.168.1.17:17500	192.168.1.255:17500	UDP
✕	Sep 9 21:17:52	WAN	Block private networks from WAN block 192.168/16 (12004)	192.168.1.1	224.0.0.1	IGMP
✕	Sep 9 21:17:59	WAN	Block private networks from WAN block 192.168/16 (12004)	192.168.1.17:17500	192.168.1.255:17500	UDP
✕	Sep 9 21:18:29	WAN	Block private networks from WAN block 192.168/16 (12004)	192.168.1.17:17500	192.168.1.255:17500	UDP
✕	Sep 9 21:18:59	WAN	Block private networks from WAN block 192.168/16 (12004)	192.168.1.17:17500	192.168.1.255:17500	UDP
✕	Sep 9 21:19:29	WAN	Block private networks from WAN block 192.168/16 (12004)	192.168.1.17:17500	192.168.1.255:17500	UDP
✕	Sep 9 21:19:58	WAN	Block private networks from WAN block 192.168/16 (12004)	192.168.1.1	224.0.0.1	IGMP
✕	Sep 9 21:20:00	WAN	Block private networks from WAN block 192.168/16 (12004)	192.168.1.17:17500	192.168.1.255:17500	UDP
✕	Sep 9 21:20:30	WAN	Block private networks from WAN block 192.168/16 (12004)	192.168.1.17:17500	192.168.1.255:17500	UDP