Pfsense

ERNESTO ROBLES

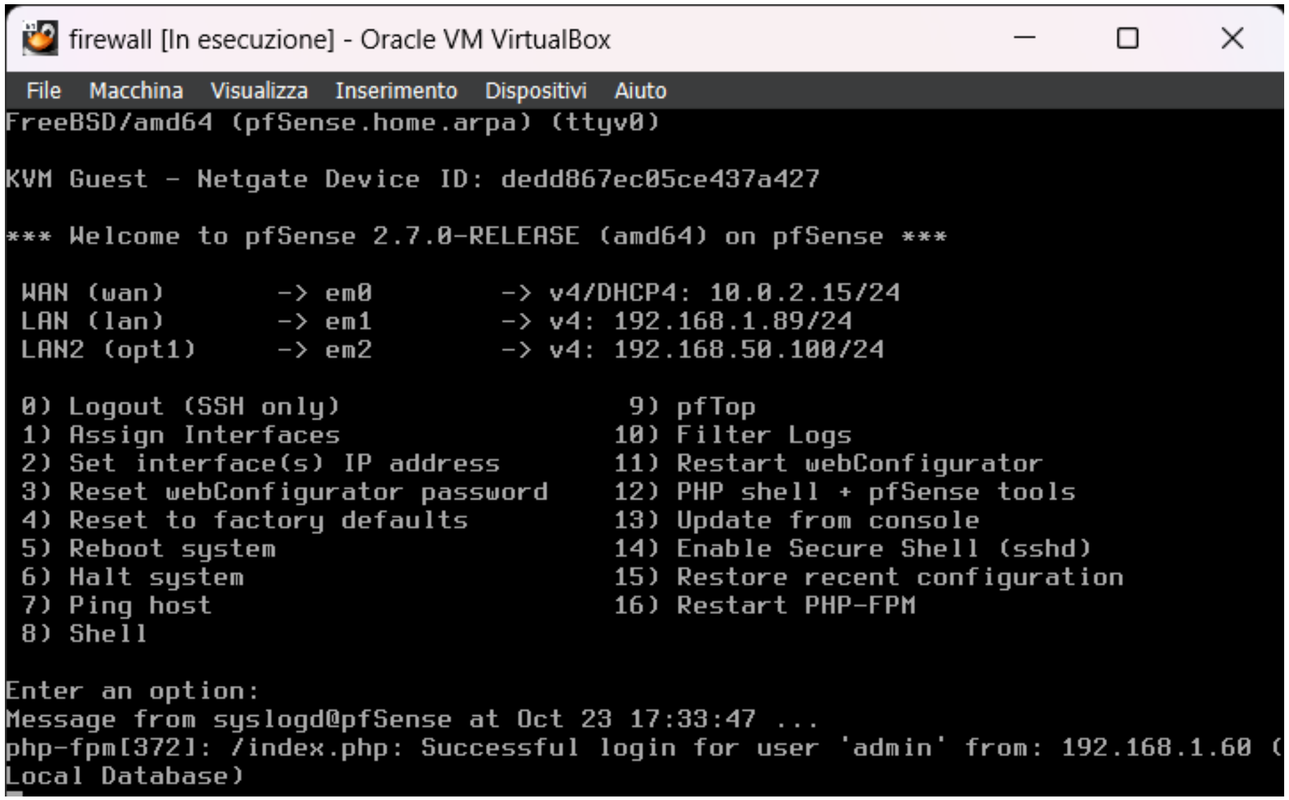
kali & metaspoitable

Sulla macchina kali è stato impostato
l'ip 192.168.1.60/24 con gateway 192.168.1.89
il quale è l'ip della lan Pfsense

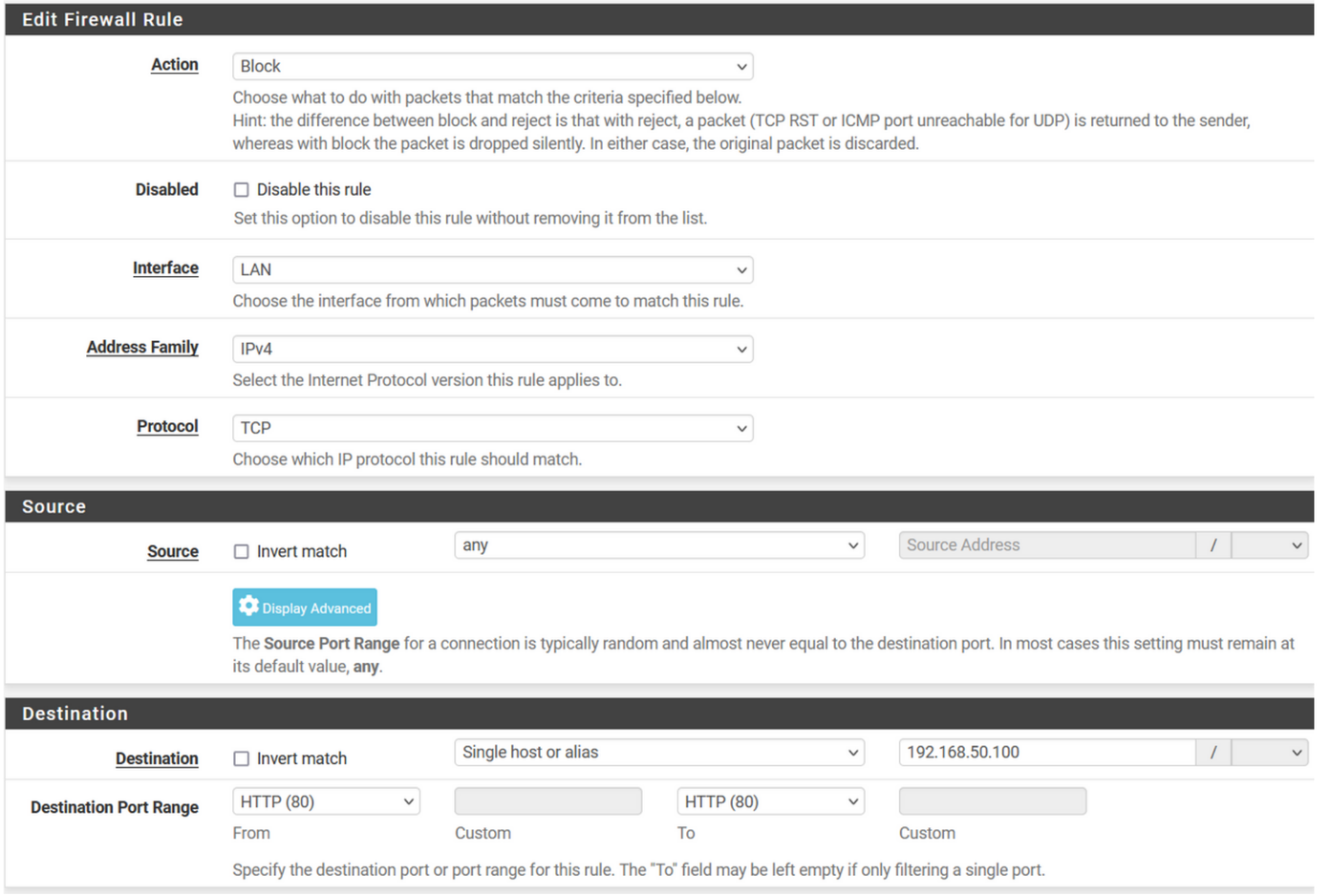
su metaspoitable l'ip 192.168.50.100/24

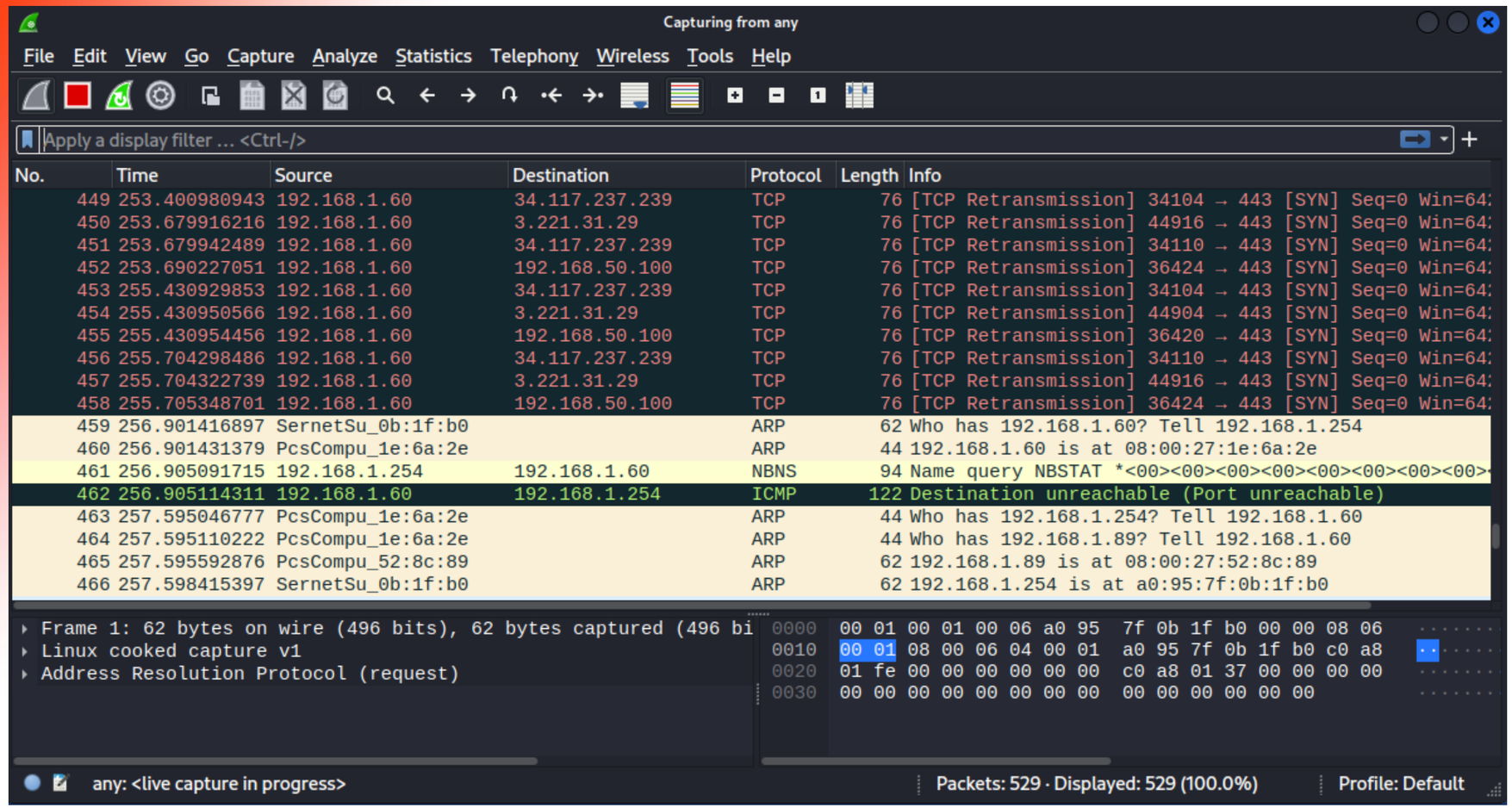
```
┌──(kali3㉿kali3)-[~]
└─$ sudo route
[sudo] password for kali3:
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         192.168.1.89    0.0.0.0         UG    0      0        0 eth0
192.168.1.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0

┌──(kali3㉿kali3)-[~]
└─$ 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=64 time=0.665 ms
64 bytes from 192.168.50.100: icmp_seq=2 ttl=64 time=0.257 ms
64 bytes from 192.168.50.100: icmp_seq=3 ttl=64 time=0.398 ms
64 bytes from 192.168.50.100: icmp_seq=4 ttl=64 time=0.425 ms
^C
── 192.168.50.100 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3149ms
rtt min/avg/max/mdev = 0.257/0.436/0.665/0.146 ms

┌──(kali3㉿kali3)-[~]
└─$ nmap -F 192.168.50.100
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-23 19:37 CEST
Nmap scan report for 192.168.50.100
Host is up (0.00076s latency).
Not shown: 97 filtered tcp ports (no-response)
PORT    STATE SERVICE
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 1.77 seconds
```

Le tre interfacce presenti nel firewall Pfsense sono:
wan 10.0.2.15/24
lan 192.168.1.89/24
lan2 192.168.50.100/24 (macchina metasoitable)



Viene impostata la regola di blocco che nega l'accesso alla dvwa da parte della macchina kali





Con wireshark possiamo confermare come non ci sia alcuna risposta da parte della destinazione

✕	Oct 23 17:54:38	LAN	(1698083493)	192.168.1.60:58686	192.168.50.100:80	TCP:S
✕	Oct 23 17:54:38	LAN	(1698083493)	192.168.1.60:38266	192.168.50.100:443	TCP:S
✕	Oct 23 17:54:40	LAN	(1698083493)	192.168.1.60:38278	192.168.50.100:443	TCP:S
✕	Oct 23 17:54:40	LAN	(1698083493)	192.168.1.60:58698	192.168.50.100:80	TCP:S

Il traffico da Kali viene effettivamente bloccato e possiamo vederlo grazie ai log

Dal browser si evidenzia come la dvwa non sia raggiungibile una volta digitato l'ip della macchina metaspoitable