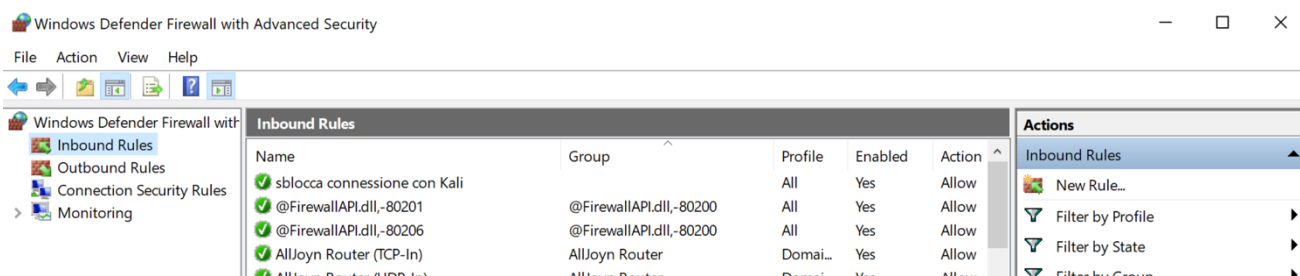


## WIRESHARK

Il compito di oggi riguarda la configurazione di una policy di firewall sulla macchina windows, la simulazione di servizi di rete con InetSim e la cattura di pacchetti con il tool WireShark sulla macchina Kali.

Per prima cosa ho creato una policy di firewall inbound su windows per permettere la connessione da Kali a Windows:



Dopodiché ho verificato che la connessione effettivamente funzionasse tramite il comando Ping:

```
raul@192: ~  
  
(raul@192)-[~]  
$ ping 192.168.50.102  
PING 192.168.50.102 (192.168.50.102) 56(84) bytes of data.  
^C  
--- 192.168.50.102 ping statistics ---  
10 packets transmitted, 0 received, 100% packet loss, time 9222ms  
  
(raul@192)-[~]  
$ ping 192.168.50.102  
PING 192.168.50.102 (192.168.50.102) 56(84) bytes of data.  
64 bytes from 192.168.50.102: icmp_seq=1 ttl=128 time=7.43 ms  
64 bytes from 192.168.50.102: icmp_seq=2 ttl=128 time=4.80 ms  
64 bytes from 192.168.50.102: icmp_seq=3 ttl=128 time=4.47 ms  
64 bytes from 192.168.50.102: icmp_seq=4 ttl=128 time=1.79 ms  
64 bytes from 192.168.50.102: icmp_seq=5 ttl=128 time=3.46 ms  
^C  
--- 192.168.50.102 ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 4014ms  
rtt min/avg/max/mdev = 1.794/4.392/7.433/1.845 ms  
  
(raul@192)-[~]  
$
```

Raul Pastor

Per continuare ho modificato il file inetsim.conf attraverso il comando da root:

```
nano /etc/inetsim/inetsim.conf
```

Commentando i servizi non necessari e mantenendo solo HTTP e HTTPS e cambiando l'indirizzo IP.

Infine ho utilizzato WireShark per sniffare le comunicazioni passanti sulla scheda di rete e per vedere la differenza tra i diversi protocolli e le loro utilità.