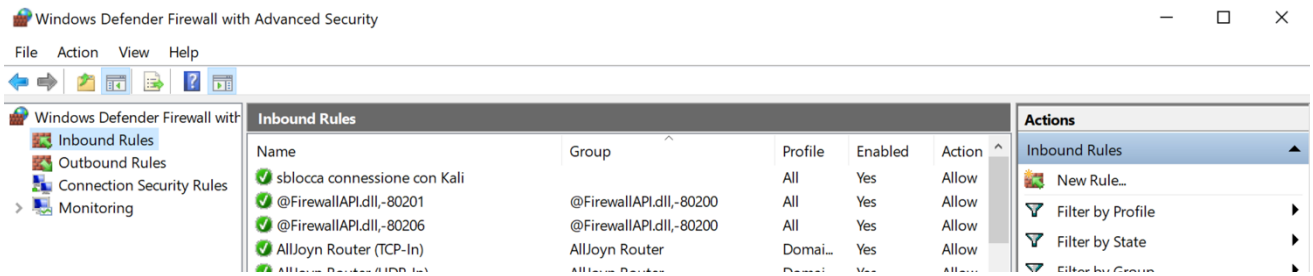
Raul Pastor

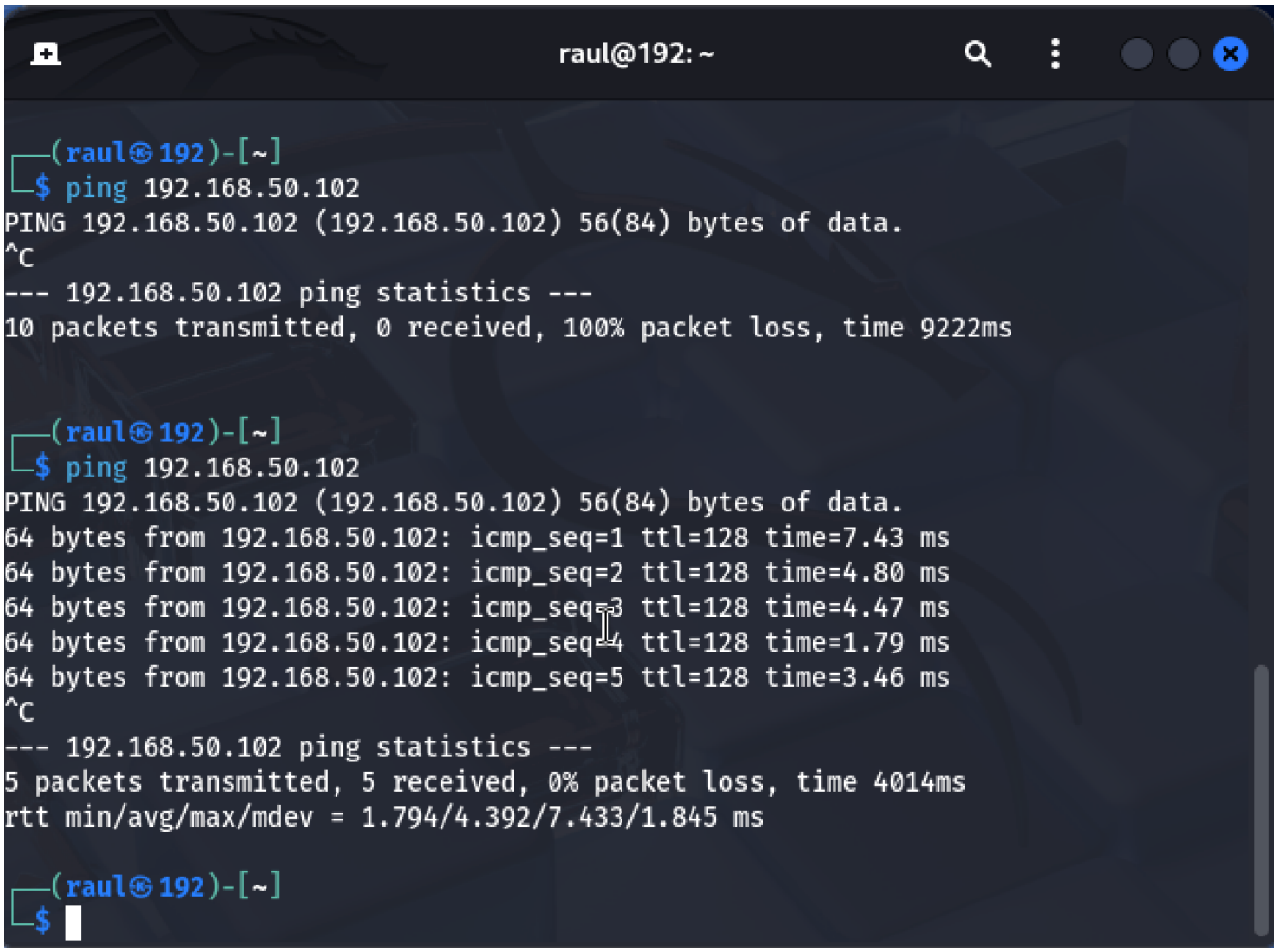
WIRESHARK

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 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.