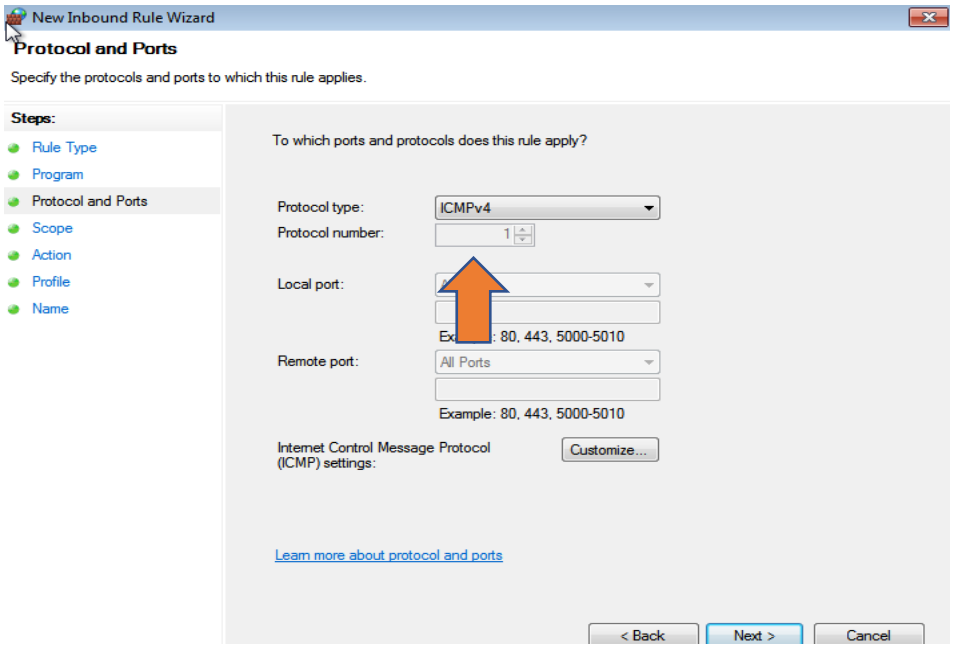
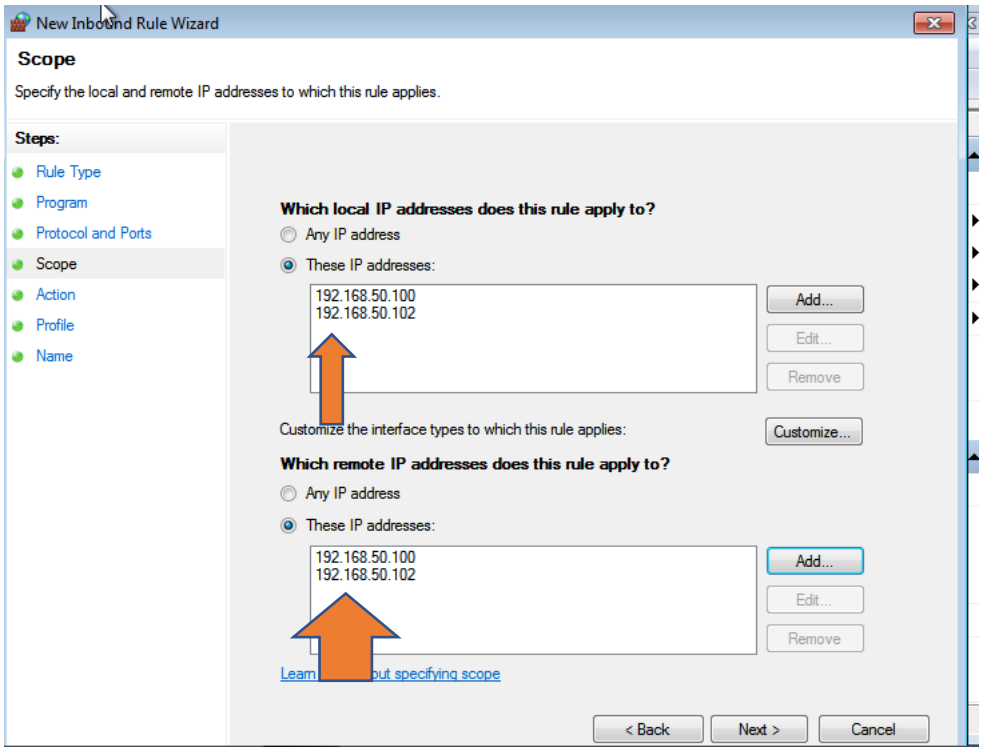
Comunicazione tra Kali e Windows tramite policy e utilizzo di InetSim e cattura di pacchetti tramite Wireshark

1)Il primo punto del nostro compito di oggi era quello di permettere la comunicazione tra Windows e Kali senza pero disattivare i firewall di Windows vediamo come fare:

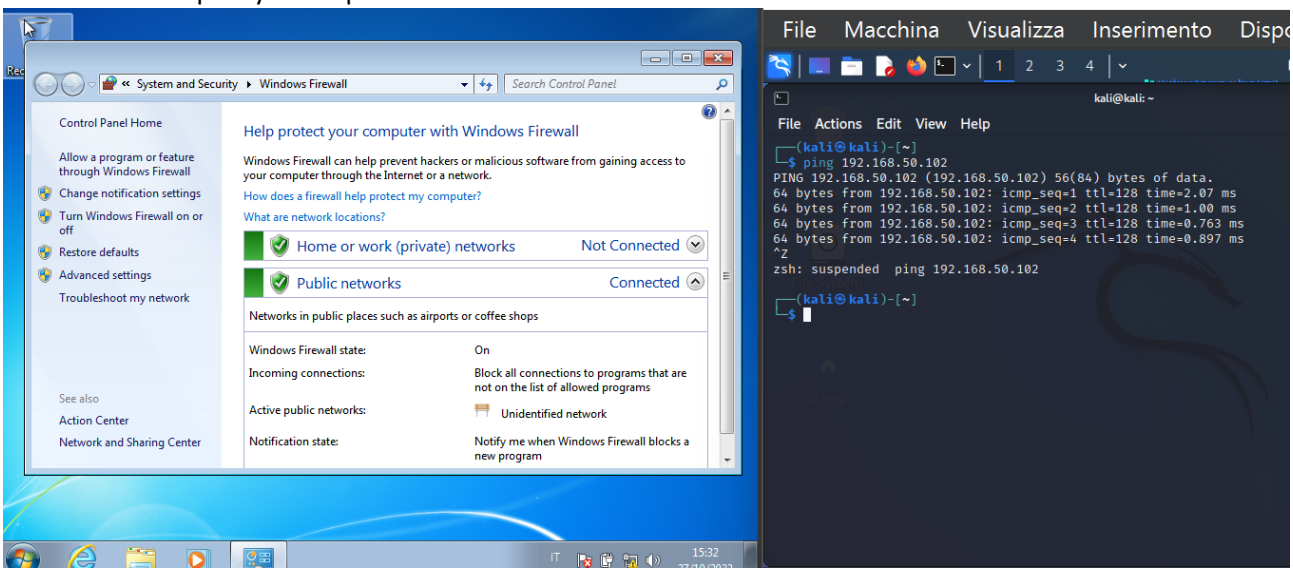
- Andiamo come prima cosa ad attivare i firewall se questi sono disattivati
- Adesso nella stessa schermata c'è la voce "advanced settings" la selezioniamo
- Clicchiamo su "inbound rules" quindi sulla destra troveremo "new rules"
- Il tipo sarà "others".



- Adesso andremo avanti nel menù a tendina selezioneremo quello in foto
- Le prossime impostazioni le lasciamo invariate fino a "scope".

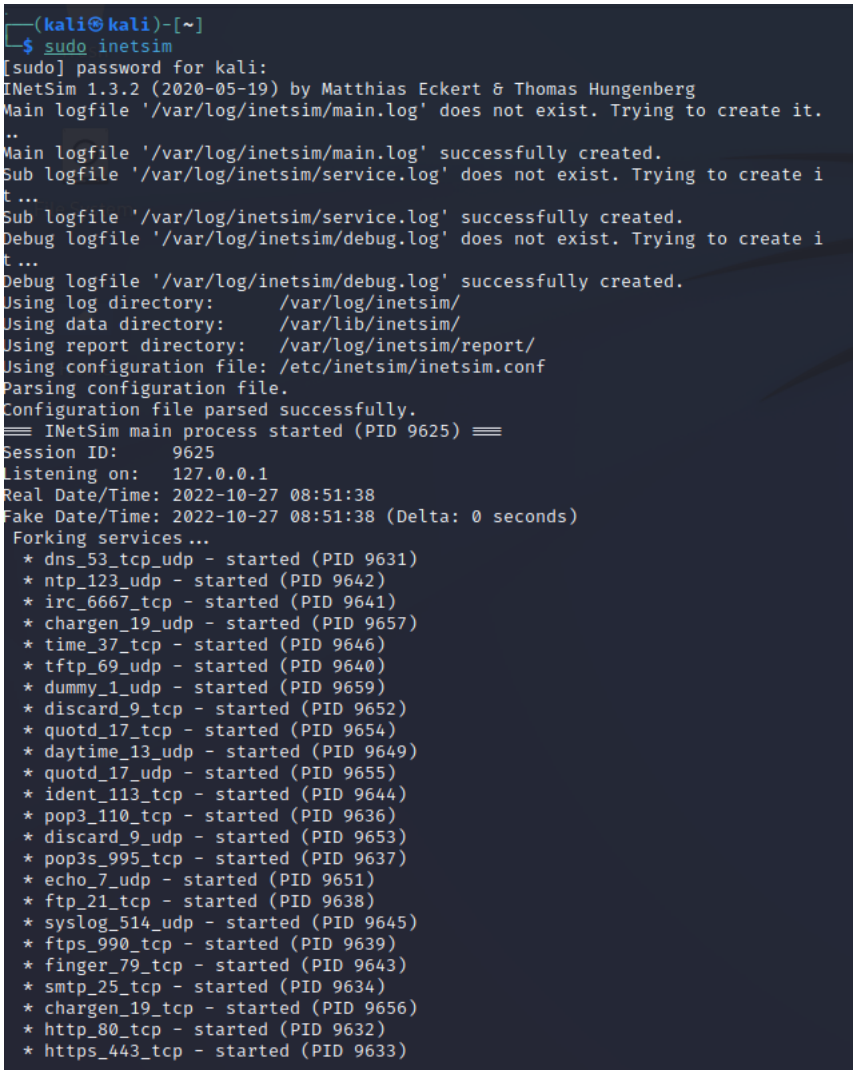


- Adesso per entrambi i campi inseriremo “these ip addresses” faremo “add”
- Quindi in entrambi inseriremo sia gli indirizzi sia di windows che di Kali
- Le prossime impostazioni le lasciamo invariate.
- Rinominiamo la policy come preferiamo e salviamo

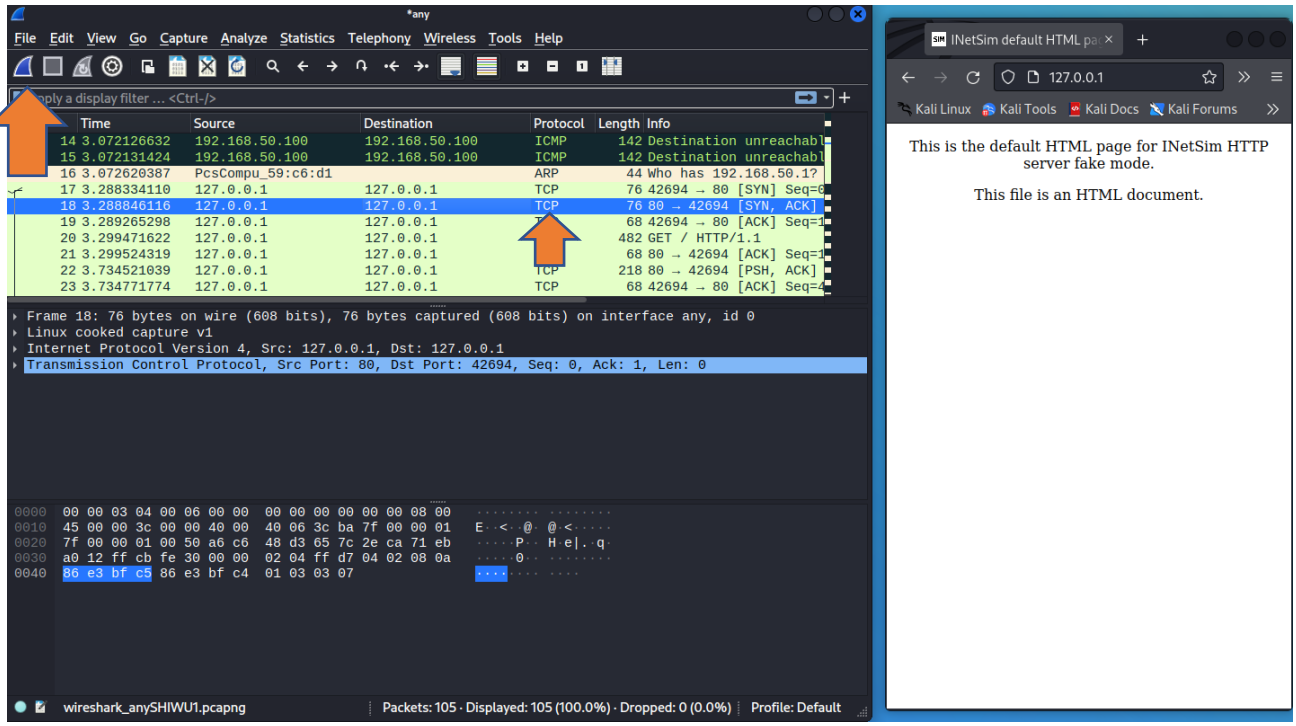


Come possiamo vedere adesso da kali possiamo fare un ping a Windows anche se questo ha i firewall attivati.

2)Utilizzo InetSim monitorare poi il traffico con WireShark



- Iniziamo con l’aprire la console di Kali che si trova nella barra delle applicazioni in alto
- Inseriamo il comando “sudo inestSim” ci chiederà la password del nostro kali la inseriamo
- Abbiamo cosi attivato la nostra rete virtuale.



- La prossima cosa da fare è avviare il nostro browser ed inserire nella barra di ricerca l'indirizzo ip della rete virtuale che sarà "127.0.0.1"
- Apriamo poi Wireshark selezioniamo *any come capture
- Iniziamo poi la cattura dei pacchetti cliccando sull' icona blu
- Vediamo adesso sotto i pacchetti che la nostra finta rete di InetSim sta generando.