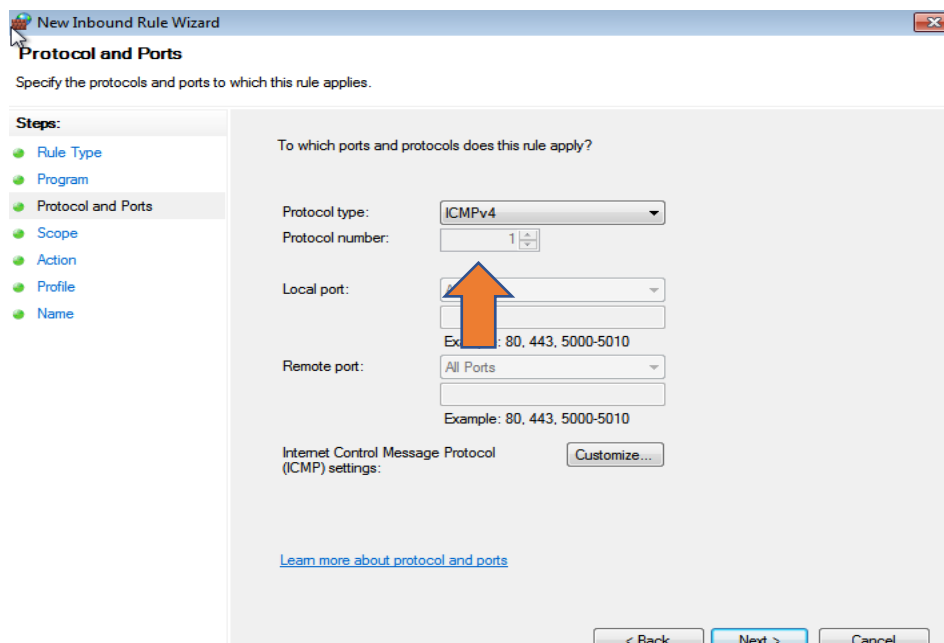


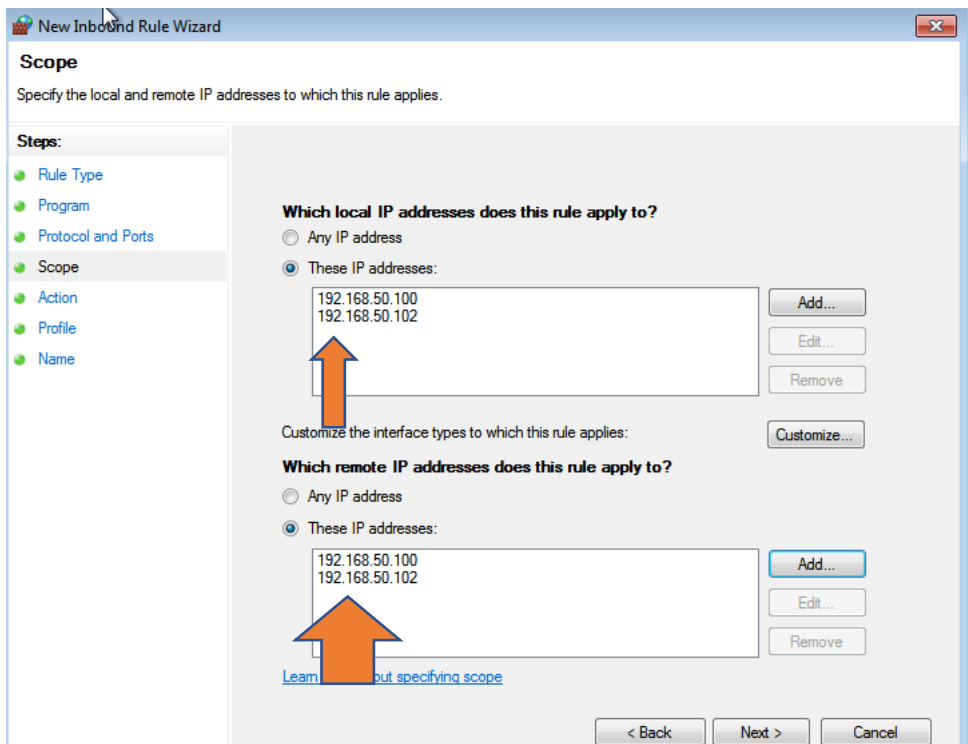
Comunicazione tra Kali e Windows tramite policy e utilizzo di InetSim e cattura di pacchetti tramite Wireshark

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

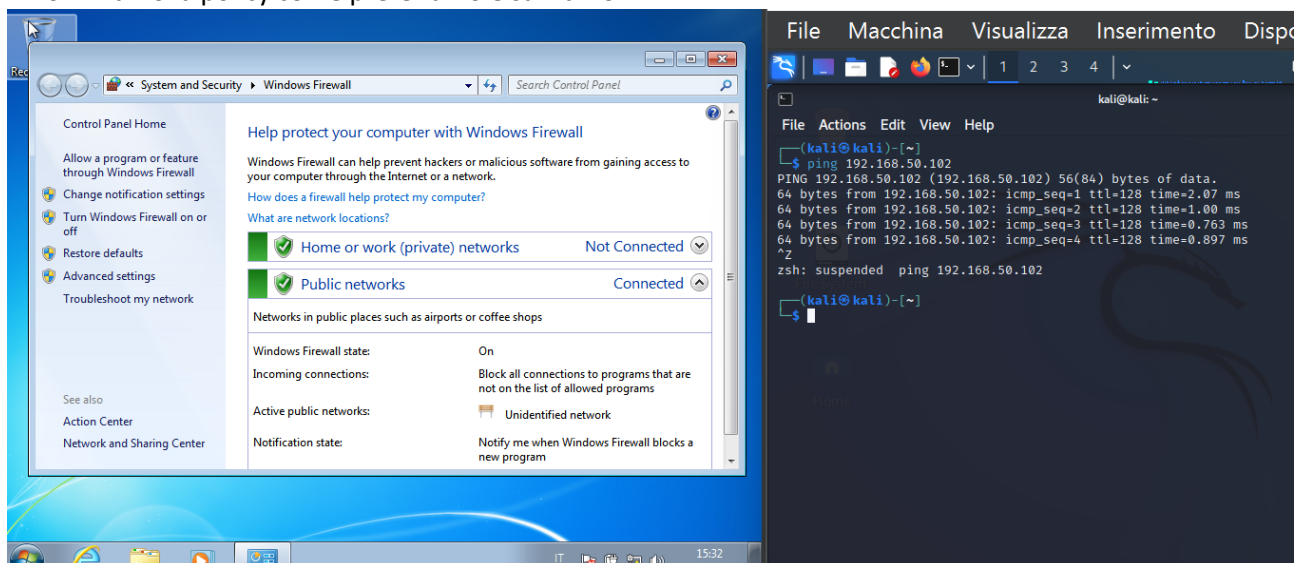
- Andiamo come prima cosa ad attivare i firewall se questi sono disattivati
- Adesso nella stessa schermata c'è la voce "advanced settings" la selezioniamo
- Clicchiamo su "inbound rules" quindi sulla destra troveremo "new rules"
- Il tipo sarà "others".



- 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

```
(kali㉿kali)-[~]
└─$ sudo inetSim
[sudo] password for kali:
INetSim 1.3.2 (2020-05-19) by Matthias Eckert & Thomas Hungenberg
Main logfile '/var/log/inetSim/main.log' does not exist. Trying to create it.
..
Main logfile '/var/log/inetSim/main.log' successfully created.
Sub logfile '/var/log/inetSim/service.log' does not exist. Trying to create i
t ...
Sub logfile '/var/log/inetSim/service.log' successfully created.
Debug logfile '/var/log/inetSim/debug.log' does not exist. Trying to create i
t ...
Debug logfile '/var/log/inetSim/debug.log' successfully created.
Using log directory:      /var/log/inetSim/
Using data directory:    /var/lib/inetSim/
Using report directory:  /var/log/inetSim/report/
Using configuration file: /etc/inetSim/inetSim.conf
Parsing configuration file.
Configuration file parsed successfully.
== INetSim main process started (PID 9625) ==
Session ID:      9625
Listening on:    127.0.0.1
Real Date/Time: 2022-10-27 08:51:38
Fake Date/Time: 2022-10-27 08:51:38 (Delta: 0 seconds)
Forking services ...
* dns_53_tcp_udp - started (PID 9631)
* ntp_123_udp - started (PID 9642)
* irc_6667_tcp - started (PID 9641)
* chargen_19_udp - started (PID 9657)
* time_37_tcp - started (PID 9646)
* tftp_69_udp - started (PID 9640)
* dummy_1_udp - started (PID 9659)
* discard_9_tcp - started (PID 9652)
* quotd_17_tcp - started (PID 9654)
* daytime_13_udp - started (PID 9649)
* quotd_17_udp - started (PID 9655)
* ident_113_tcp - started (PID 9644)
* pop3_110_tcp - started (PID 9636)
* discard_9_udp - started (PID 9653)
* pop3s_995_tcp - started (PID 9637)
* echo_7_udp - started (PID 9651)
* ftp_21_tcp - started (PID 9638)
* syslog_514_udp - started (PID 9645)
* ftps_990_tcp - started (PID 9639)
* finger_79_tcp - started (PID 9643)
* smtp_25_tcp - started (PID 9634)
* chargen_19_tcp - started (PID 9656)
* http_80_tcp - started (PID 9632)
* https_443_tcp - started (PID 9633)
```

- Iniziamo con l'aprire la console di Kali che si trova nella barra delle applicazioni in alto
- Inseriamo il comando "sudo inetSim" ci chiederà la password del nostro kali la inseriamo
- Abbiamo così attivato la nostra rete virtuale.

