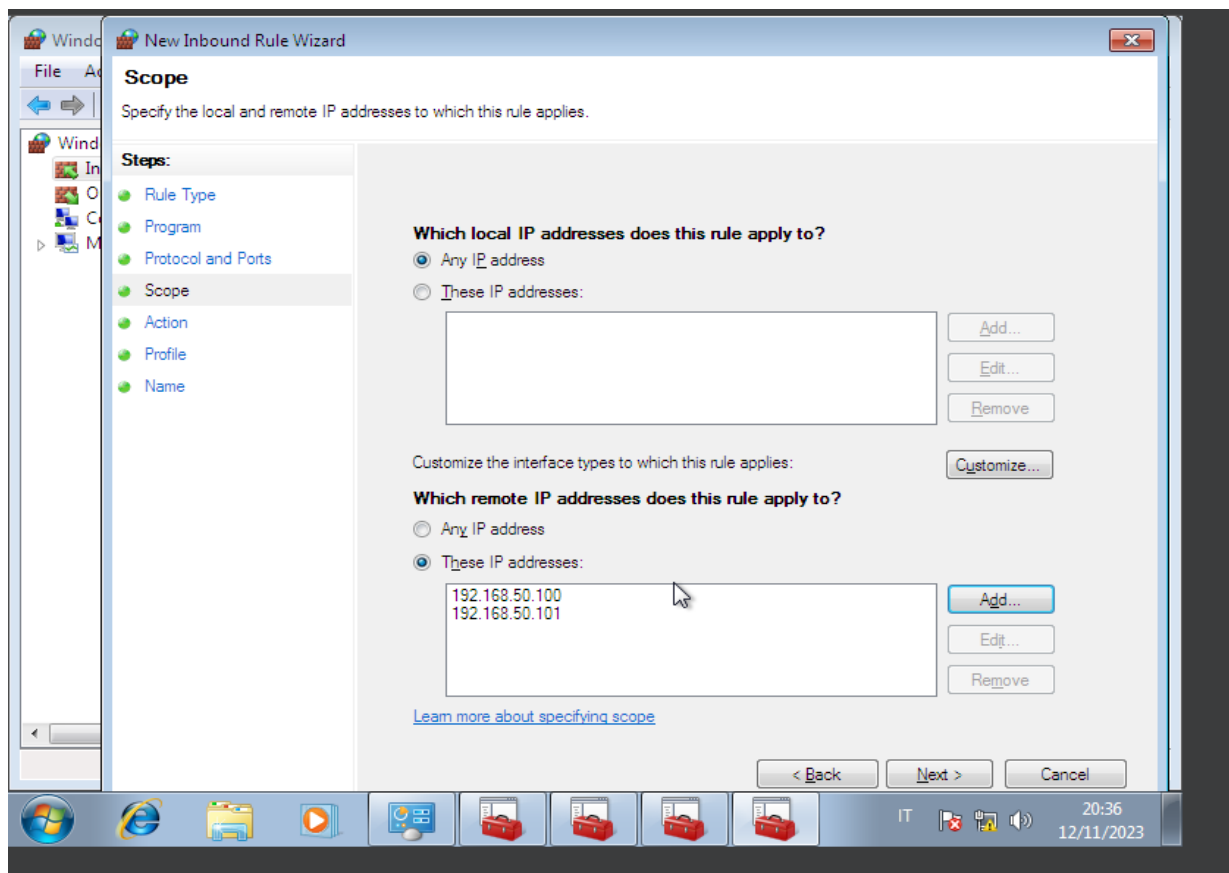
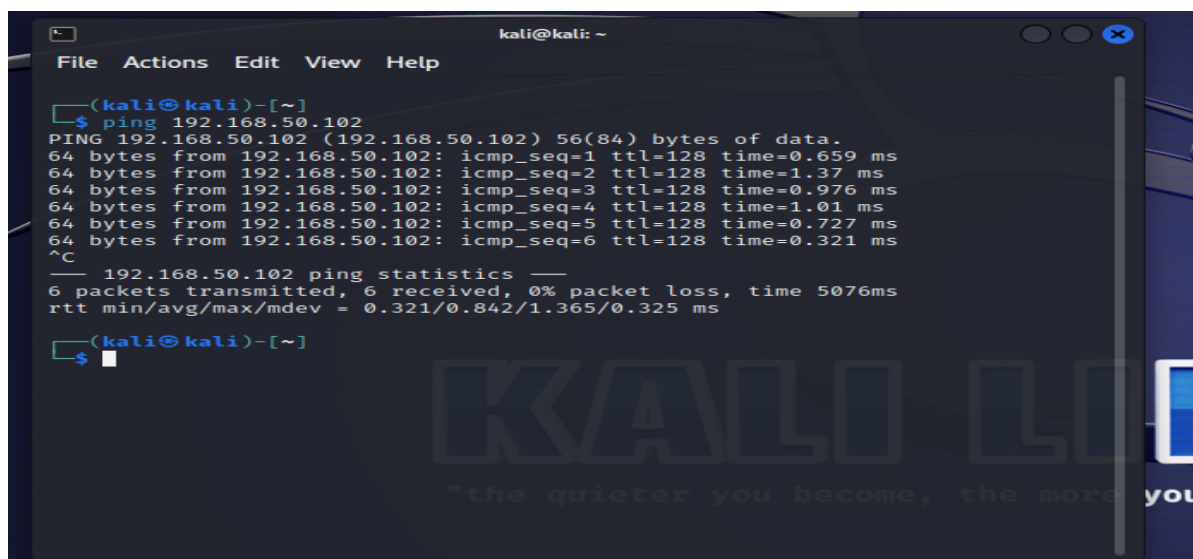


ESERCITAZIONE 10/11/2023

- Configurazione del firewall

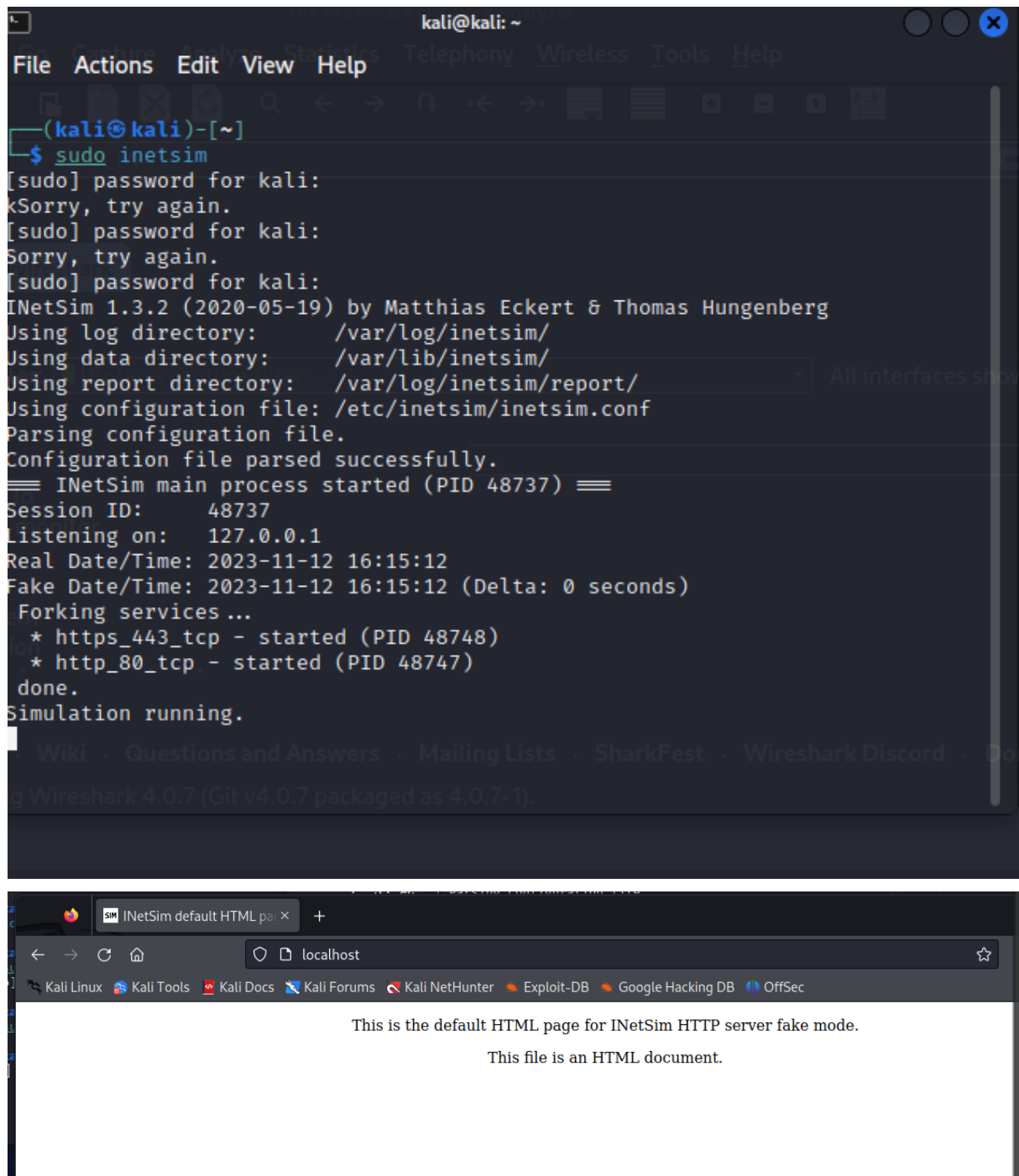


Nelle impostazioni avanzate del firewall indico l'ip di Kali e Meta, per far sì che esse possano comunicare tra di loro.



Facendo il ping, vedo che Kali riesce comunque a inviare pacchetti a Windows7.

- Configurazione Inetsim

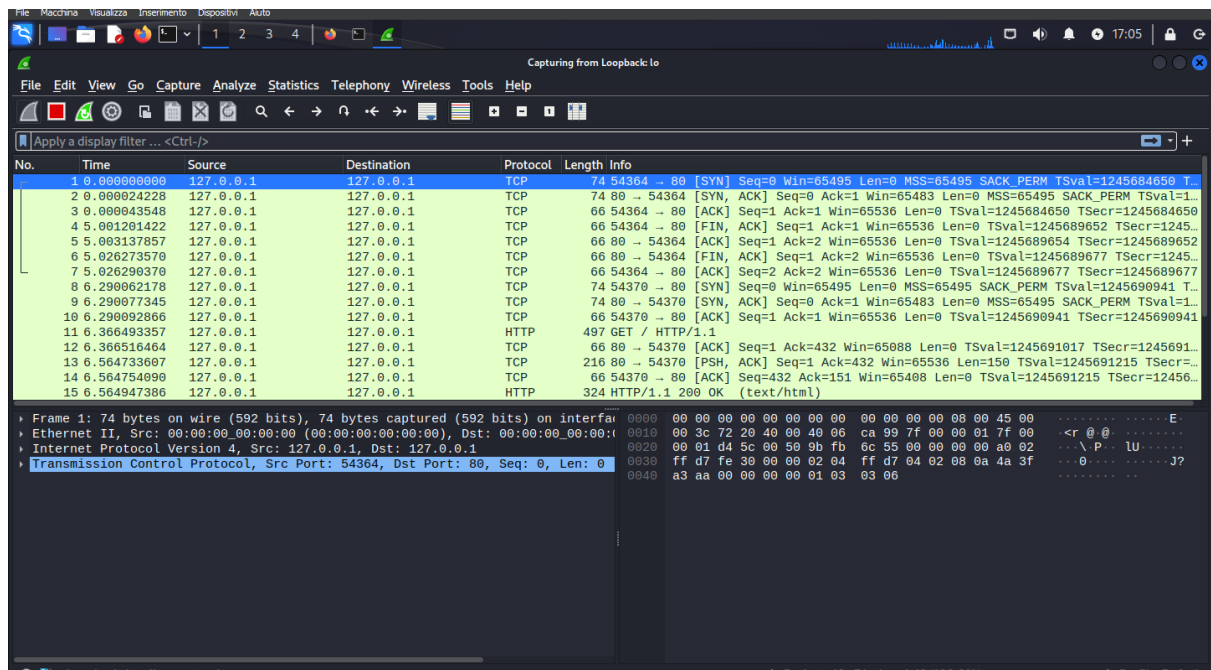


The image shows two screenshots from a Kali Linux system. The top screenshot is a terminal window titled 'kali@kali: ~' with a menu bar (File, Actions, Edit, View, Help) and a toolbar. It shows the execution of the 'sudo inetsim' command. The output indicates that InetSim 1.3.2 (2020-05-19) by Matthias Eckert & Thomas Hungenberg is running. It lists the log directory (/var/log/inetsim/), data directory (/var/lib/inetsim/), report directory (/var/log/inetsim/report/), and configuration file (/etc/inetsim/inetsim.conf). It also shows the session ID (48737), listening port (127.0.0.1), and the start of the simulation with services https_443_tcp (PID 48748) and http_80_tcp (PID 48747) running.

```
kali@kali: ~  
File Actions Edit View Help  
- (kali@kali)-[~]  
- $ sudo inetsim  
[sudo] password for kali:  
kSorry, try again.  
[sudo] password for kali:  
Sorry, try again.  
[sudo] password for kali:  
INetSim 1.3.2 (2020-05-19) by Matthias Eckert & Thomas Hungenberg  
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 48737) ==  
Session ID: 48737  
Listening on: 127.0.0.1  
Real Date/Time: 2023-11-12 16:15:12  
Fake Date/Time: 2023-11-12 16:15:12 (Delta: 0 seconds)  
Forking services...  
* https_443_tcp - started (PID 48748)  
* http_80_tcp - started (PID 48747)  
done.  
Simulation running.
```

The bottom screenshot is a web browser window titled 'INetSim default HTML page'. The address bar shows 'localhost'. The page content consists of two lines of text: 'This is the default HTML page for INetSim HTTP server fake mode.' and 'This file is an HTML document.'

Cattura pacchetti con Wireshark



Andando sul browser digitando <http://localhost>, su wireshark non riesco a leggerli perché sono cifrati nonostante io abbia fatto l'accesso con la porta 80.

Traffico facendo comunicare W7 e Kali, riusciamo a vederlo da Wireshark dagli ip di destinazione/sorgente. Entrambe le macchine comunicano.

