# ESERCITZAIONE 8 FIREWALL-INETSIM-WIRESHARK

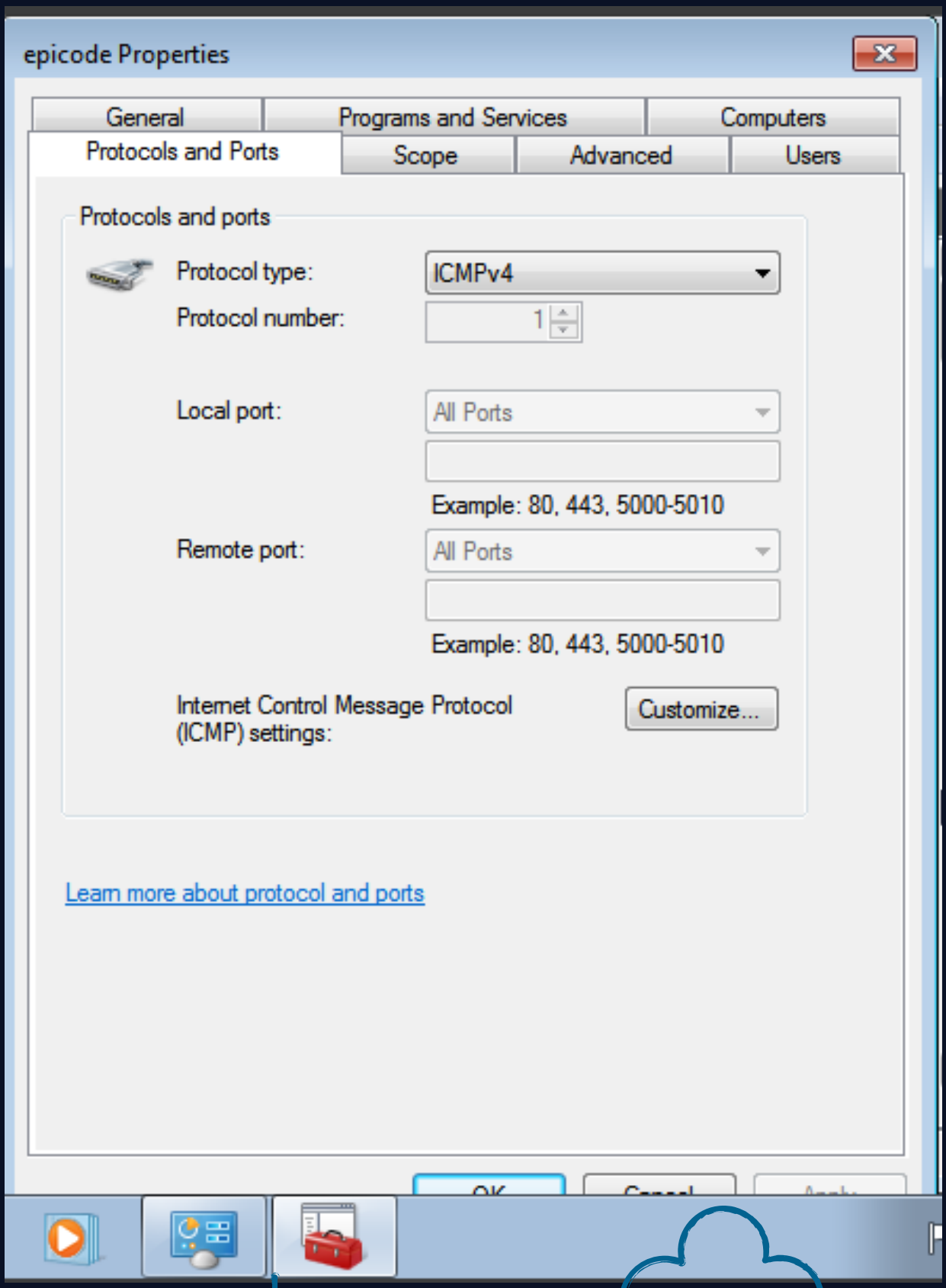
Andrea Ferrantino

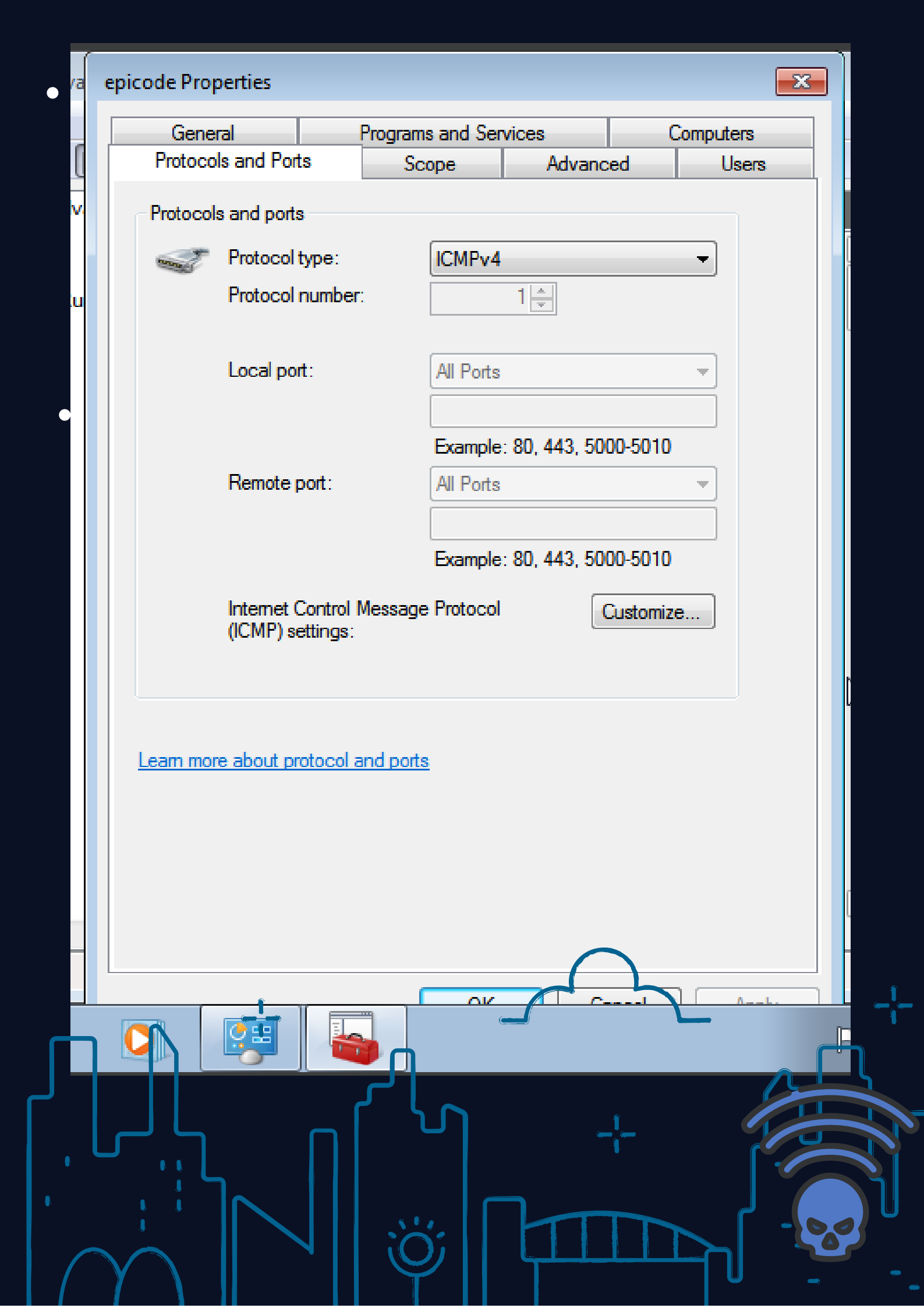
*L'esercizio consiste nella configurazione del firewall di WIN 7 e in una packet capture con Wireshark attraverso l'utilizzo di InetSim su Kali Linux.*

## Configurazione win 7 firewall

Per permettere il ping tra le due macchine è necessario stabilire una policy su Win 7,per prima cosa andiamo nel pannello di controllo ed eseguiamo questi passaggi:

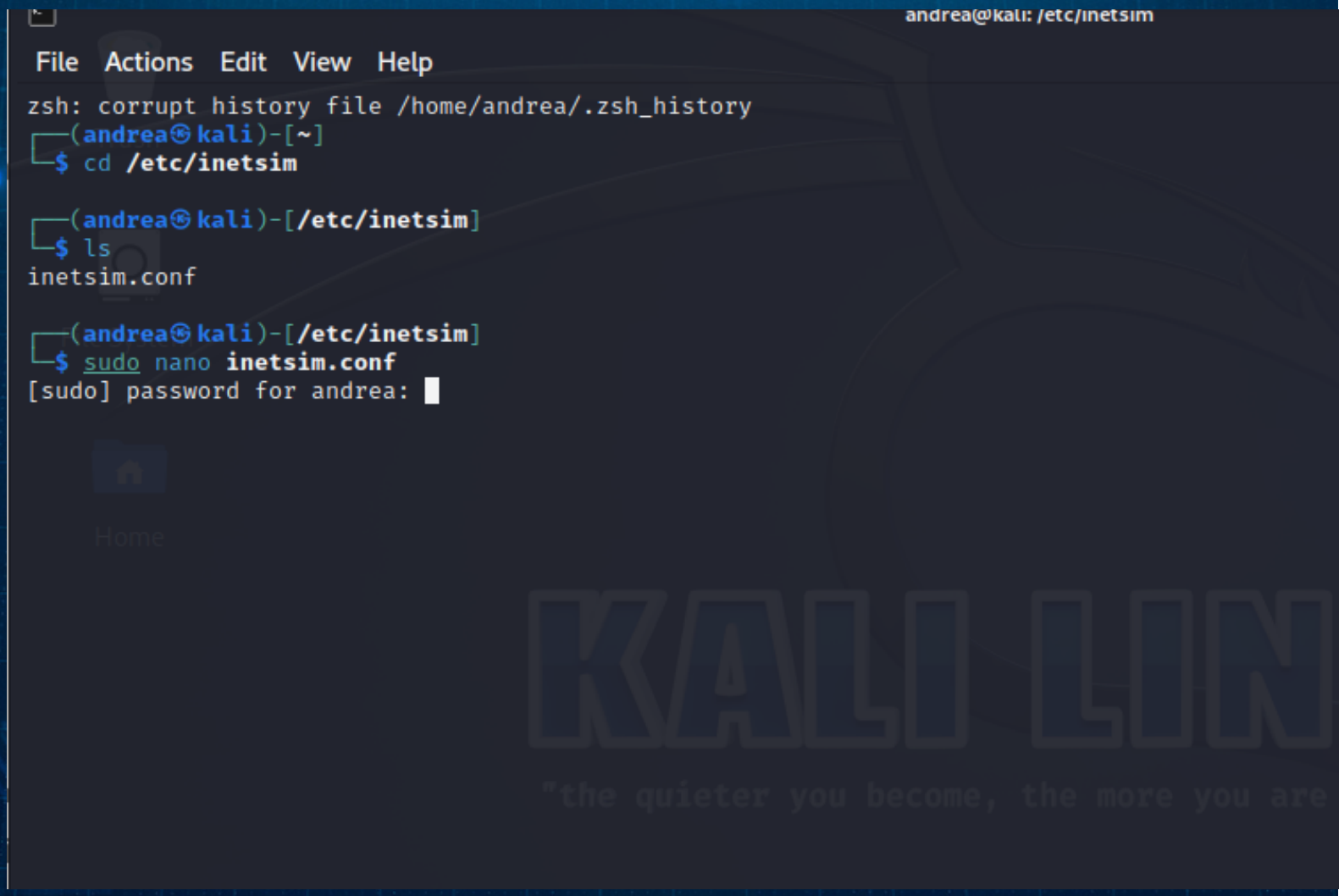
- **Control Panel System and Security Firewall Advanced Settings Inbound Rules New Rule Custom Rule**
- *Fatto ciò impostiamo la seguente configurazione:*


epicode Properties
General
Programs and Services
Computers
Protocols and Ports
Scope
Advanced
Users
Protocols and ports
Protocol type:
ICMPv4
Protocol number:
1
Local port:
All Ports
Example: 80, 443, 5000-5010
Remote port:
All Ports
Example: 80, 443, 5000-5010
Internet Control Message Protocol (ICMP) settings:
Customize...
Learn more about protocol and ports

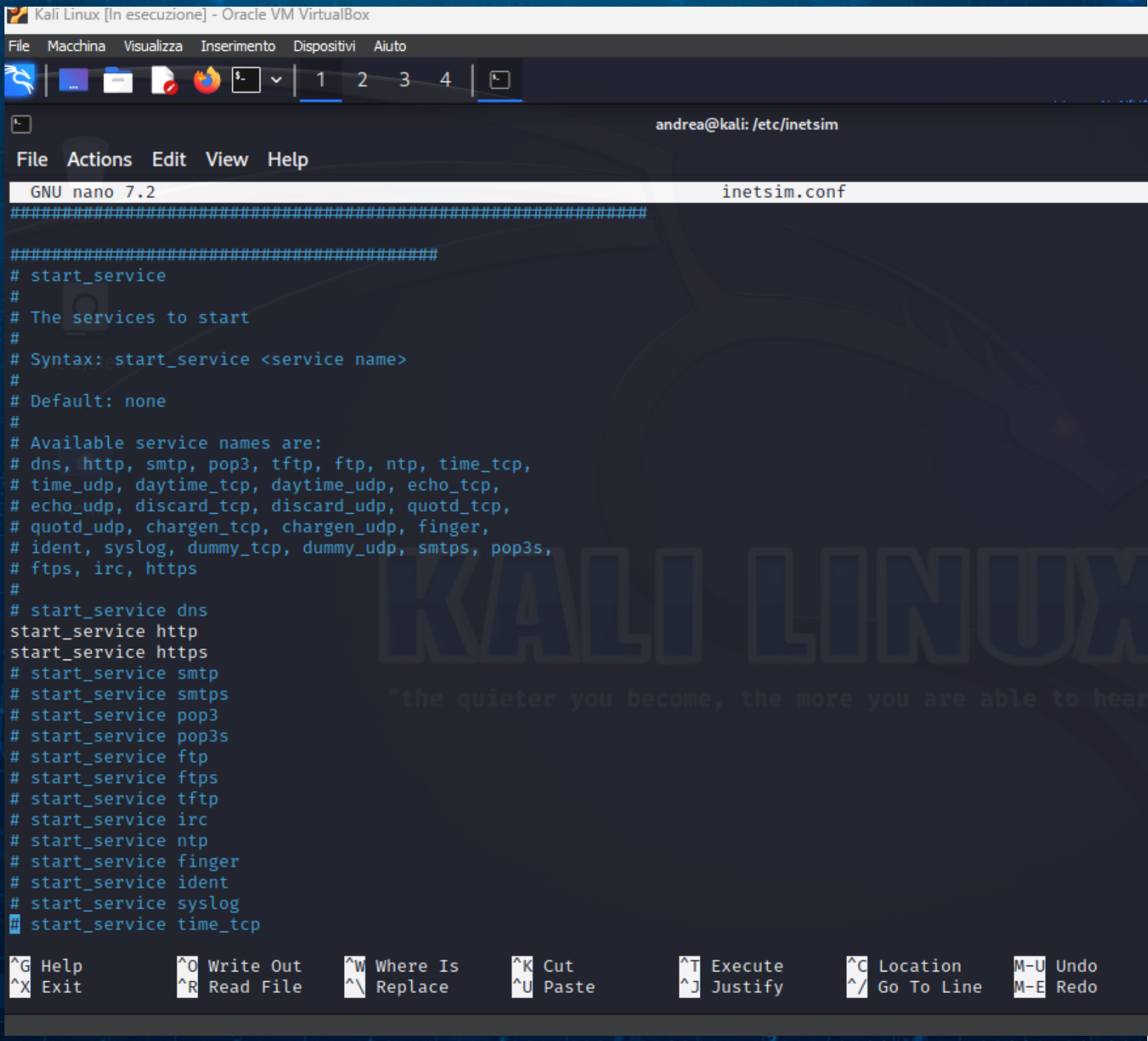

epicode Properties
General
Programs and Services
Computers
Protocols and Ports
Scope
Advanced
Users
Protocols and ports
Protocol type:
ICMPv4
Protocol number:
1
Local port:
All Ports
Example: 80, 443, 5000-5010
Remote port:
All Ports
Example: 80, 443, 5000-5010
Internet Control Message Protocol (ICMP) settings:
Customize...
Learn more about protocol and ports

# Settagio Inetsim

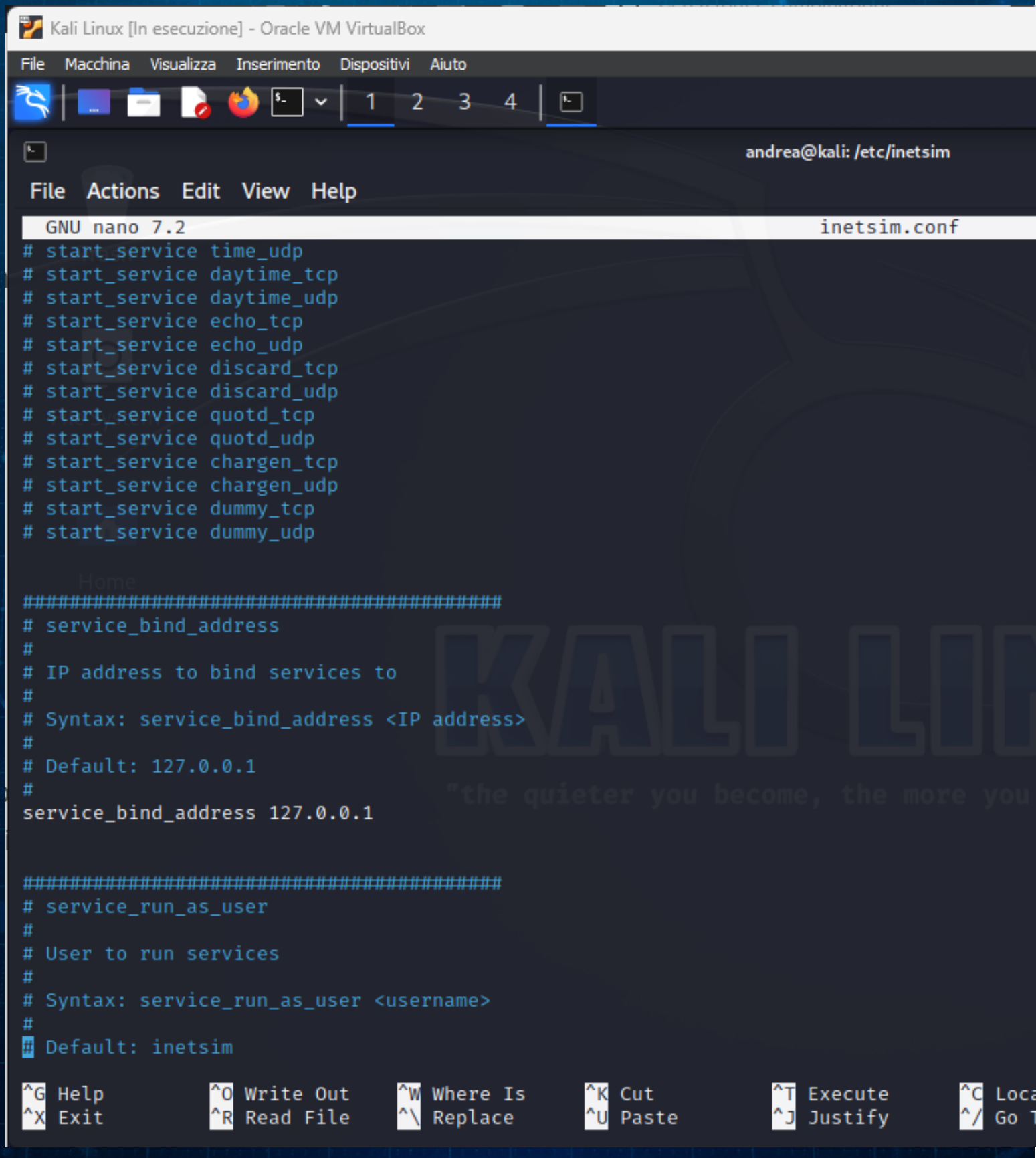
Apriamo il terminale di Kali Linux  e seguiamo questi passaggi per aprire il file inetsim.conf:



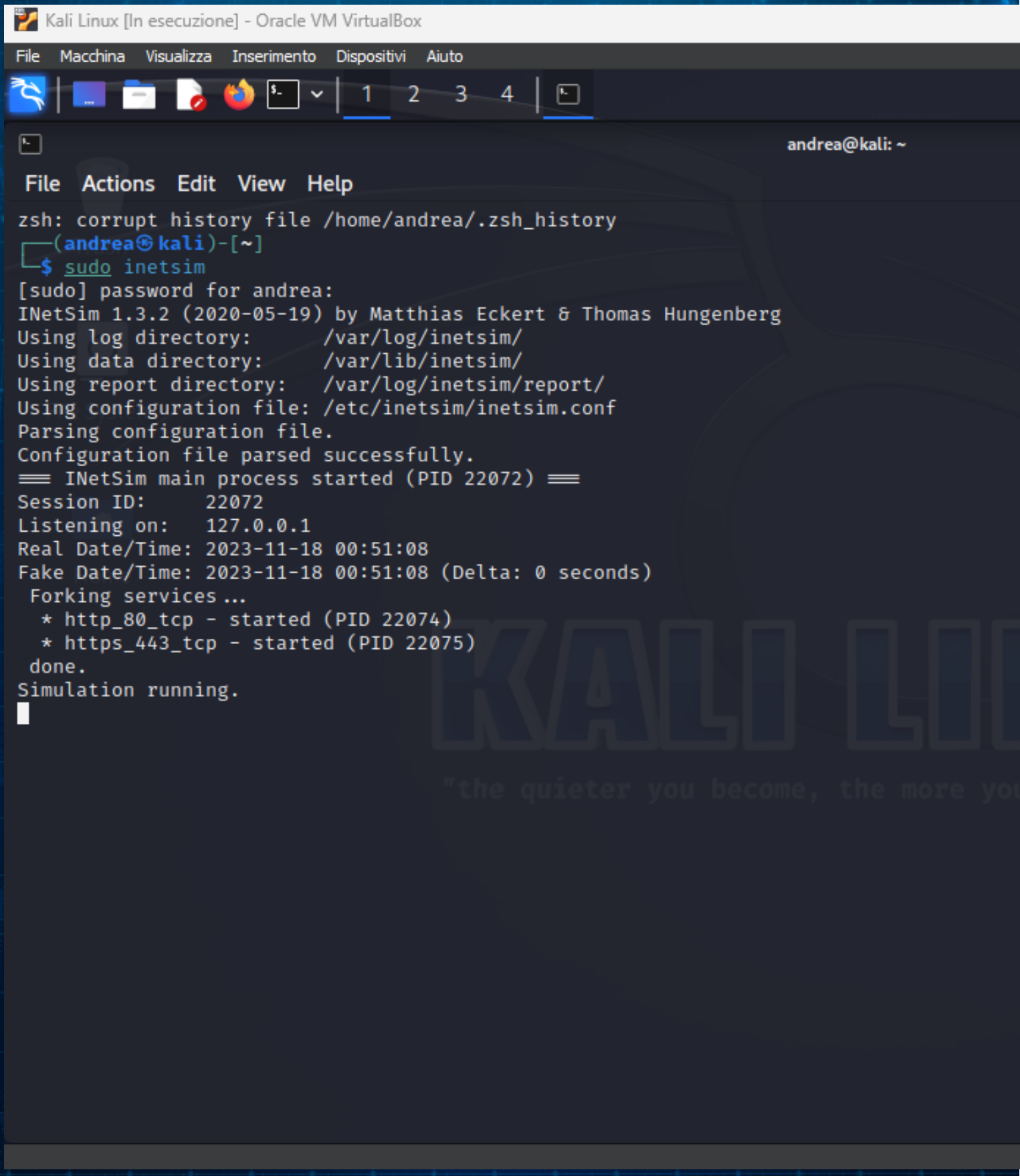
Inseriamo la password ci verrà data la possibilità il file “inetsim.conf” settandolo lascialndo attivi “http e https” inserendo il carattere “#”



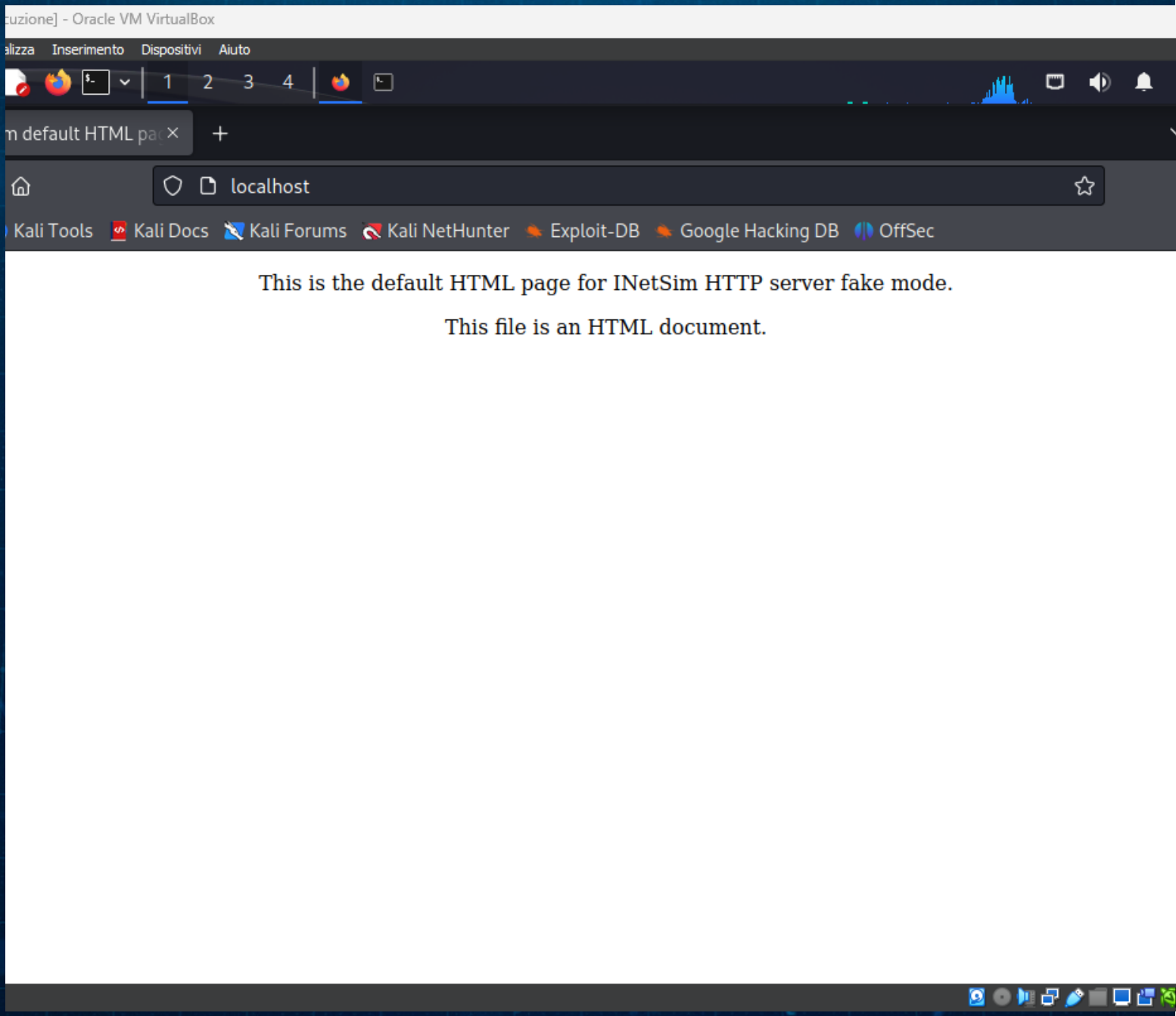
Andremo a impostare l'indirizzo 127.0.0.1 come IP address per il fake service che andremo ad utilizzare:



Salviamo il file con “Ctrl+X” , “Y” e digitiamo il comando “sudo inetsim”

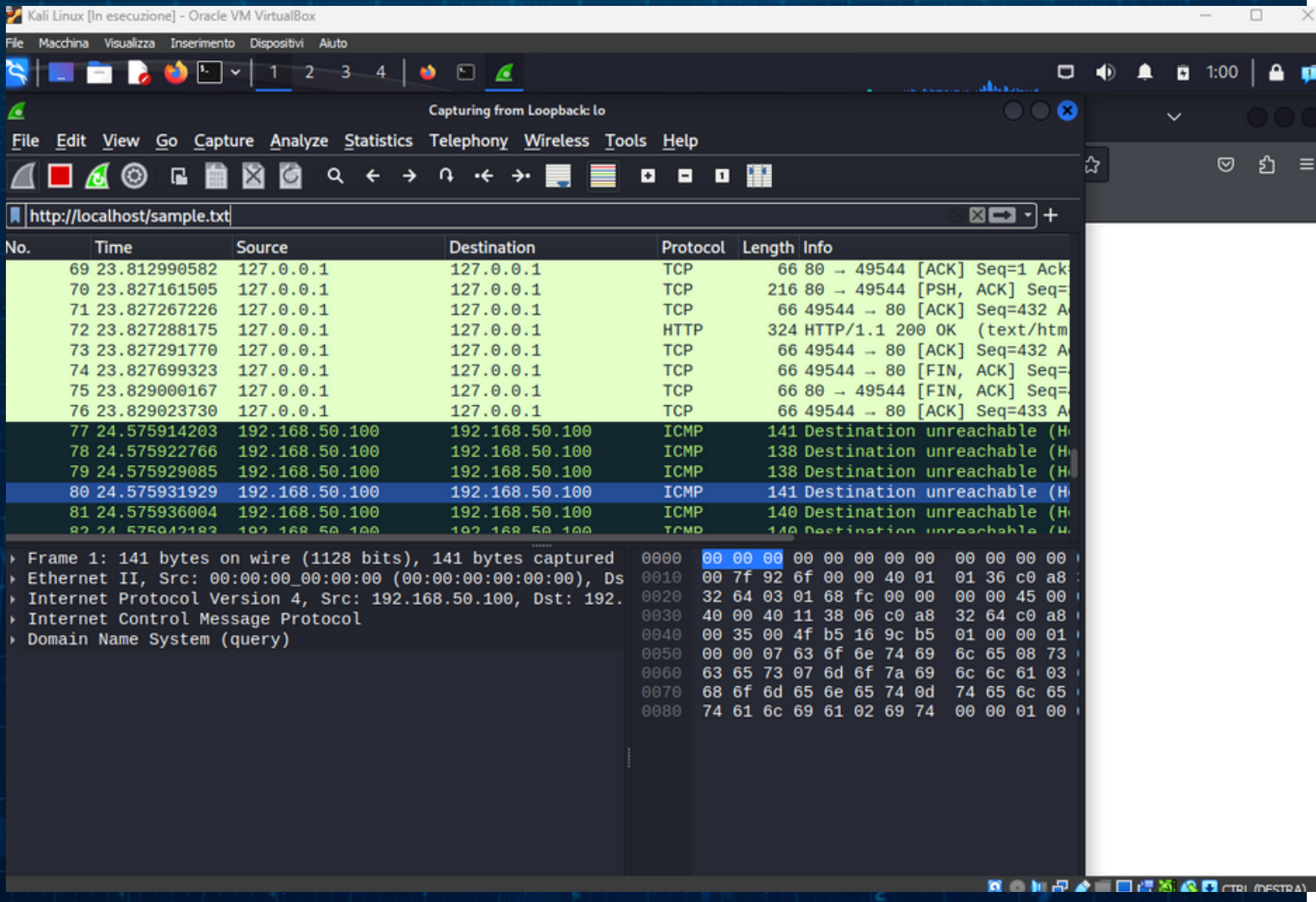


Ora apriamo Mozilla da Kali Linux sulla pagina “ http://localhost” cosi possiamo vedere che la risposta verrà visualizzata sulla pagina.



# Packet Capture con Wireshark

Avviamo adesso wireshark su kali linux  scegliendo di utilizzare la rete LOOPBACK.Andremo a richiamare delle magine su mozilla con il comando get “http://localhost/sample.txt”



Nella stessa maniera andremo a scegliere ANY anziche LOOPBACK come in precedenza e saremo in grado attraverso il comando ip.src == 127.0.0.1 verrranno visualizzati i pacchetti provenienti da quel IP sorgente.