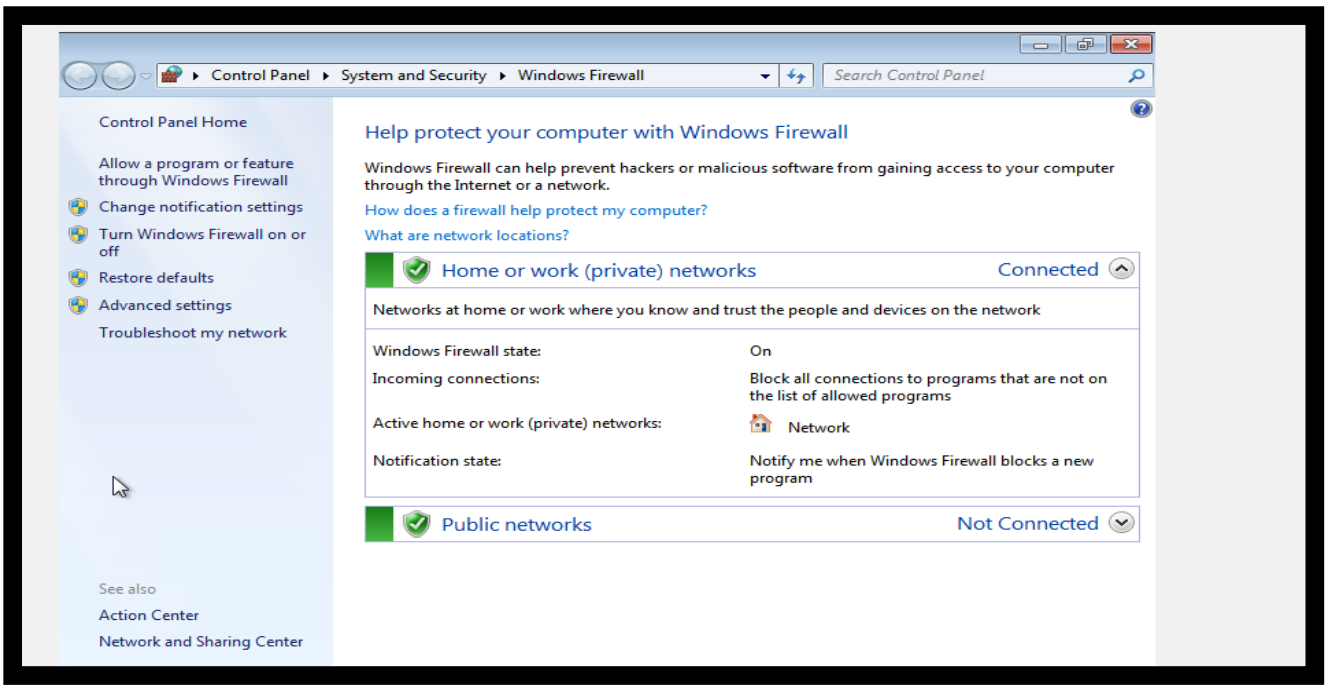
REPORT CONFIGURAZIONE POLICY\PACKET SPOOFING

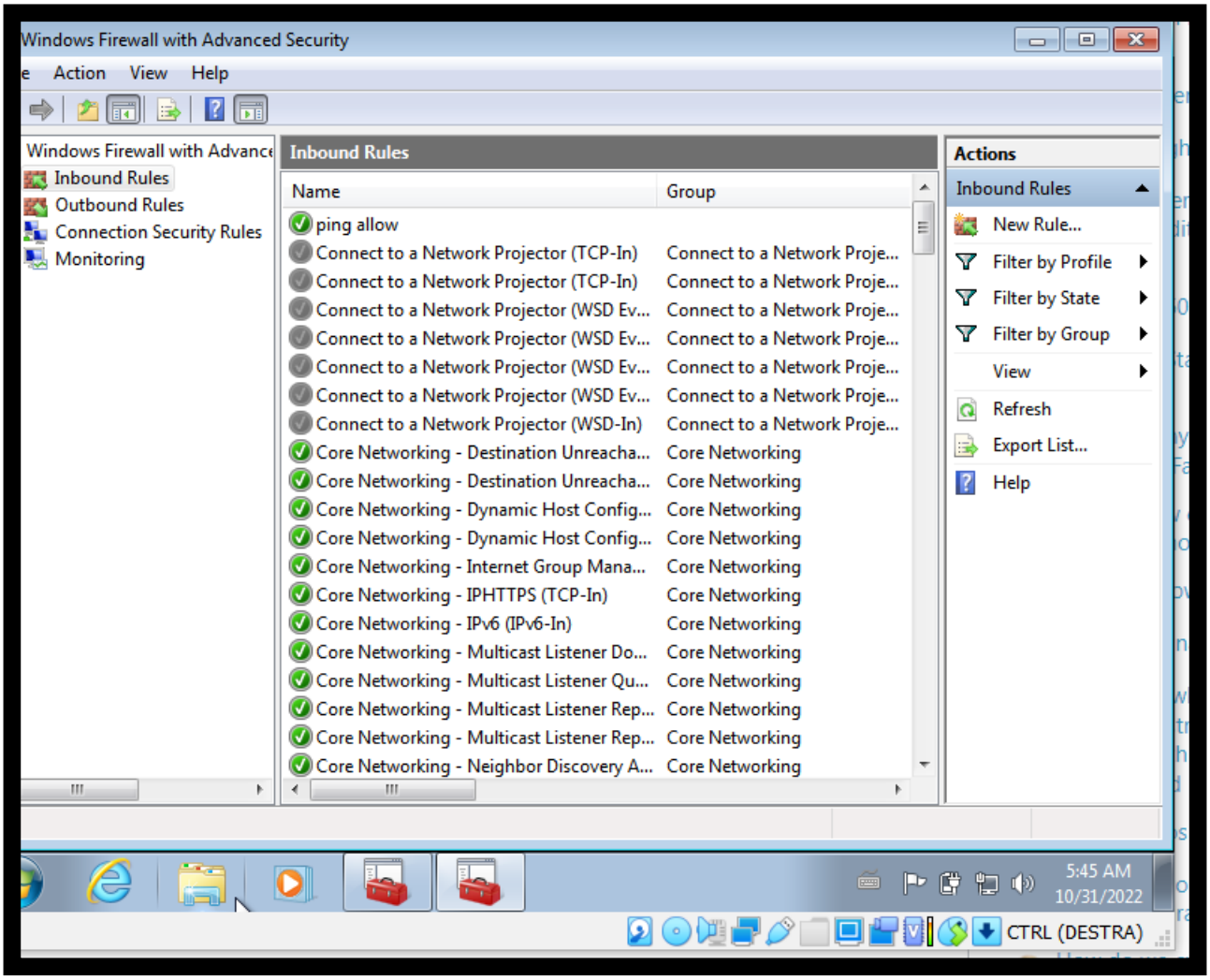
LE TASK RICHIEDONO:

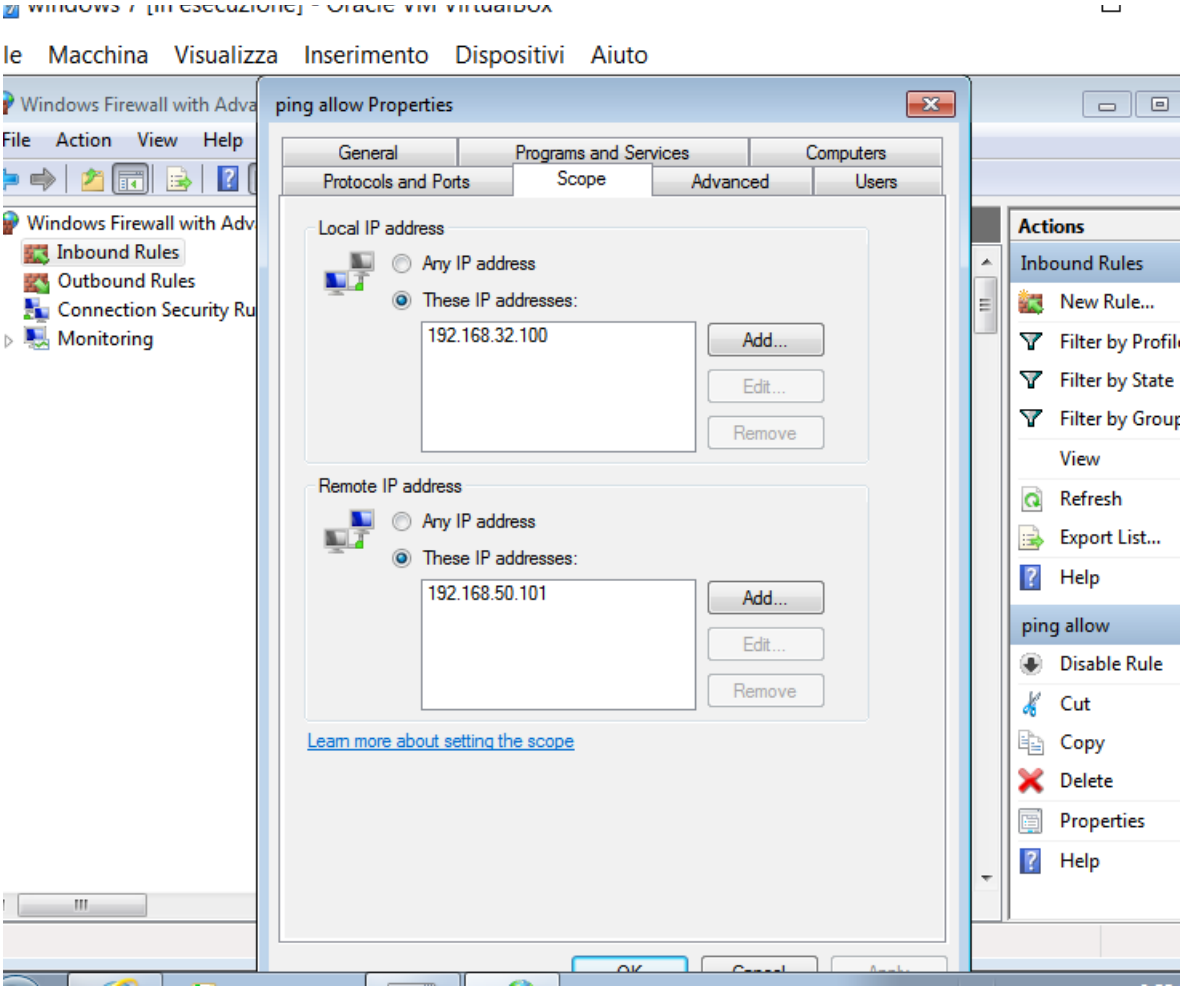
1. La configurazione di firewall policy per il pinginng delle macchine Linux e windows7 in virtual lab.
2. Utilizzo inetsim per la simulazione di servizi internet standard
3. Packet spoofing tramite tool wireshark

Primo step fondamentale è l'attivazione dei firewall windows, step senza la quale non avremmo alcun ping tra le macchine:

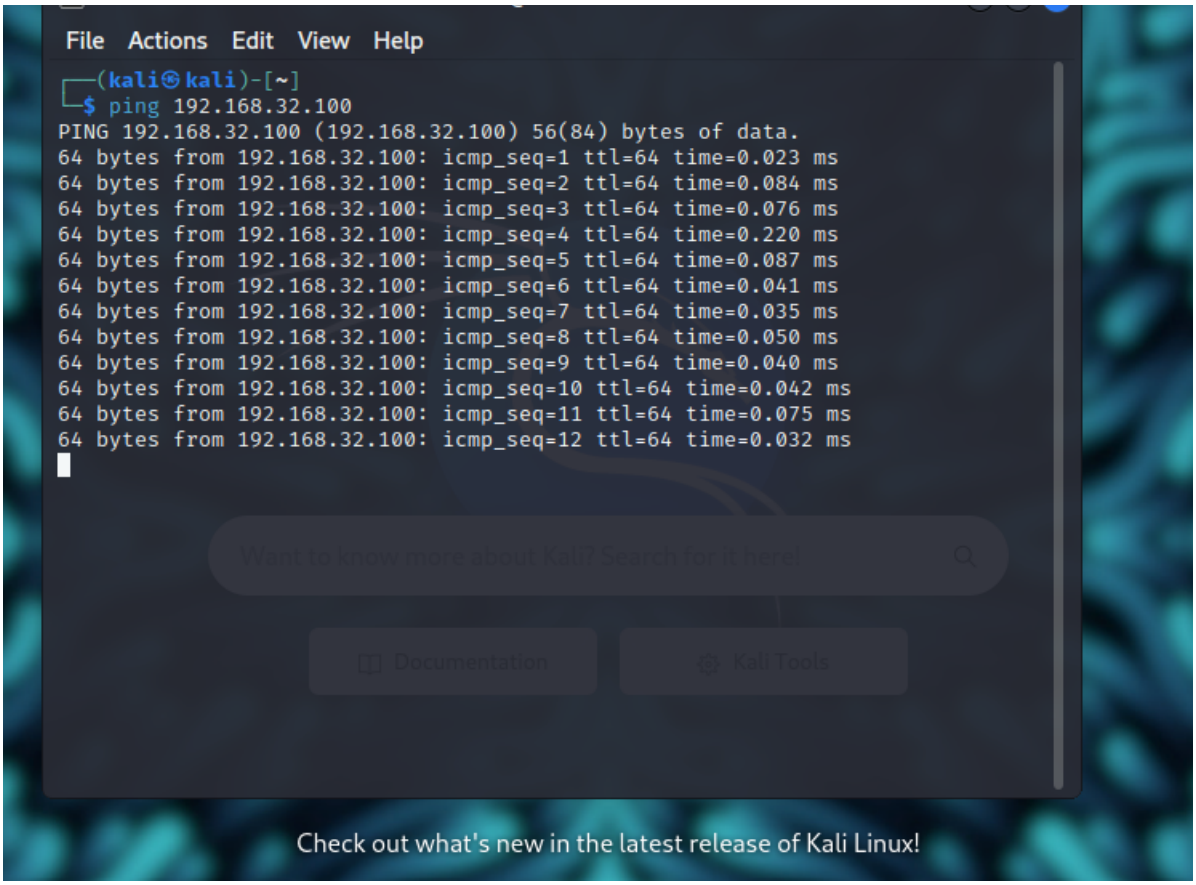


Impostiamo quindi una firewall policy dedicata, aggiungendo alla sezione "These IP address" gli indirizzi delle macchine di cui siamo interessati alla connessione.

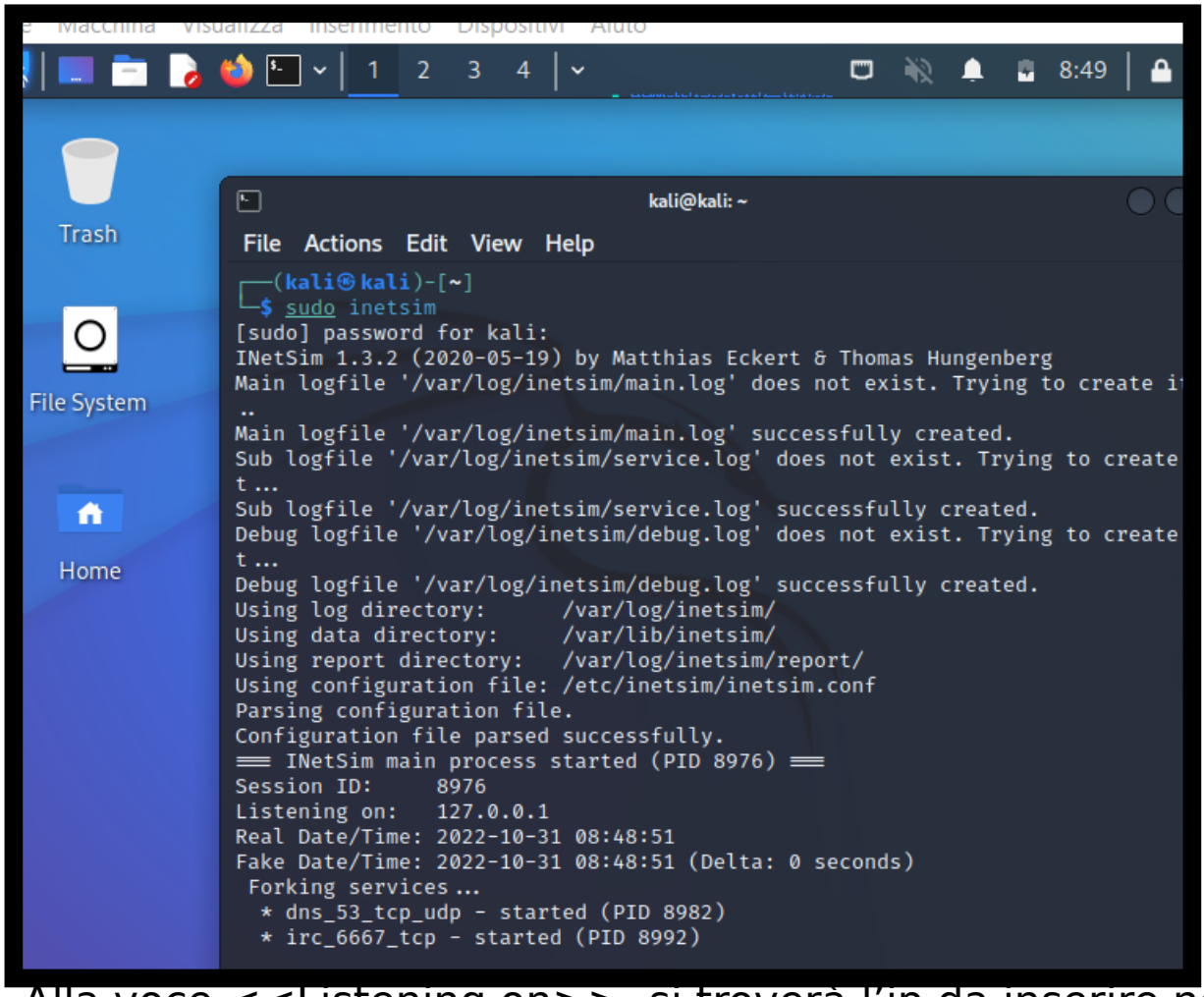

Windows Firewall with Advanced Security
e Action View Help
Windows Firewall with Advanc
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Inbound Rules
Name
Group
ping allow
Connect to a Network Projector (TCP-In)
Connect to a Network Proje...
Connect to a Network Projector (TCP-In)
Connect to a Network Proje...
Connect to a Network Projector (WSD Ev...
Connect to a Network Proje...
Connect to a Network Projector (WSD Ev...
Connect to a Network Proje...
Connect to a Network Projector (WSD Ev...
Connect to a Network Proje...
Connect to a Network Projector (WSD Ev...
Connect to a Network Proje...
Connect to a Network Projector (WSD-In)
Connect to a Network Proje...
Core Networking - Destination Unreacha...
Core Networking
Core Networking - Destination Unreacha...
Core Networking
Core Networking - Dynamic Host Config...
Core Networking
Core Networking - Dynamic Host Config...
Core Networking
Core Networking - Internet Group Mana...
Core Networking
Core Networking - IPHTTPS (TCP-In)
Core Networking
Core Networking - IPv6 (IPv6-In)
Core Networking
Core Networking - Multicast Listener Do...
Core Networking
Core Networking - Multicast Listener Qu...
Core Networking
Core Networking - Multicast Listener Rep...
Core Networking
Core Networking - Multicast Listener Rep...
Core Networking
Core Networking - Neighbor Discovery A...
Core Networking
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
5:45 AM
10/31/2022
CTRL (DESTRA)



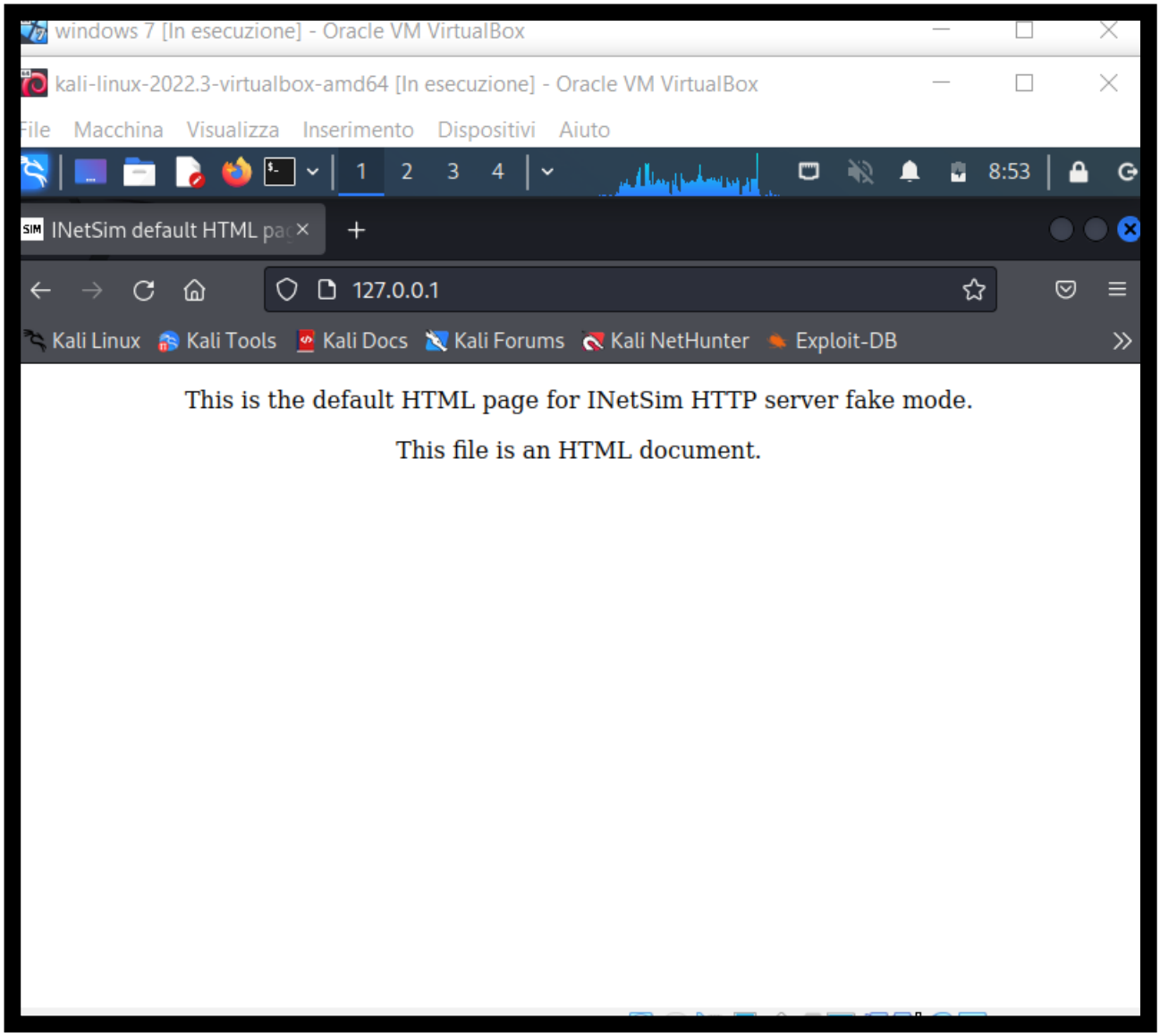
A questo punto, potremmo testare la comunicazione tra le due macchine



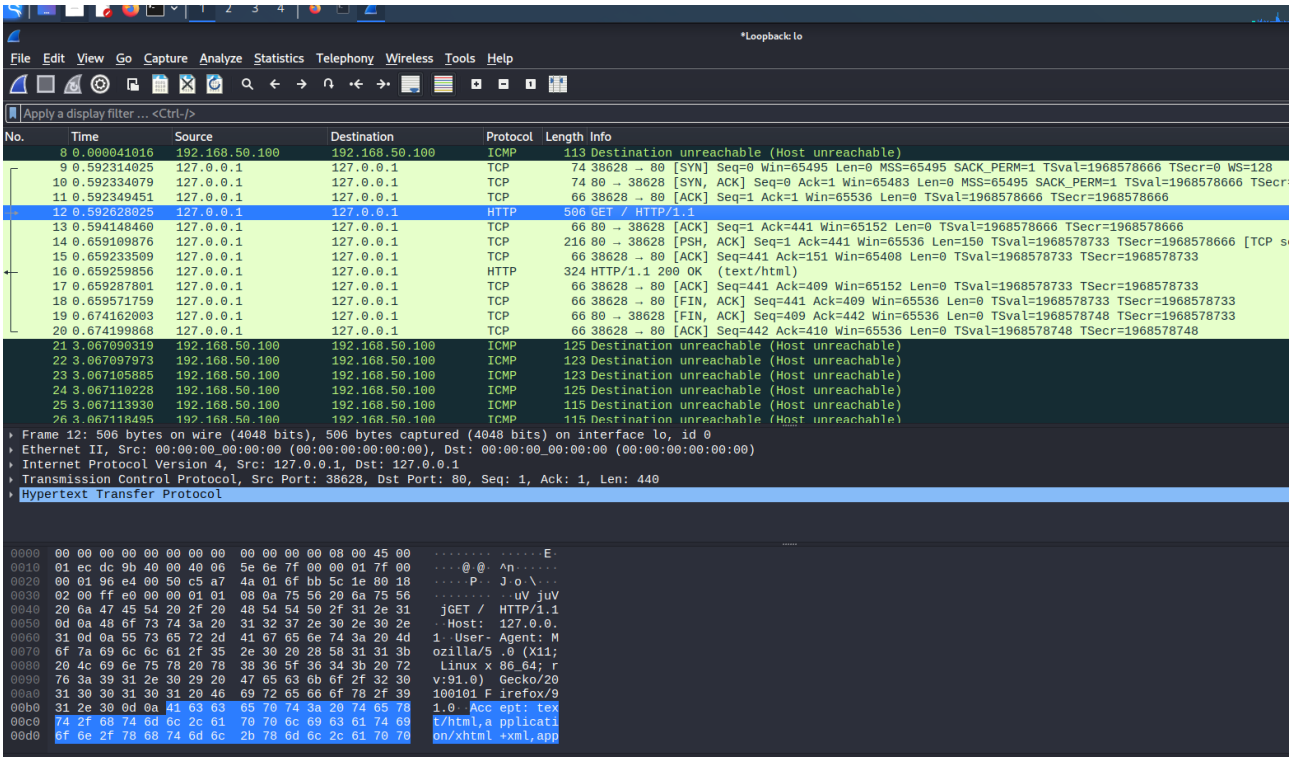
Una volta ottenuta la conferma sarà possibile attivare un server simulato con il comando <<sudo inetsim>> sul prompt comandi Kali.



Alla voce <<Listening on>> si troverà l'ip da inserire nella ricerca di Firefox in Kali



Adesso, aprendo wireshark ed effettuando una cattura del traffico intercorso otterremo questo risultato.



Dove sarà possibile osservare come tramite filtro protocollo TCP, i messaggi ICMP vengono trasmessi tramite connessione in three-way handshake (SYN|SYN-ACK|ACK) utilizzando un canale http, quindi con flusso di dati in chiaro.