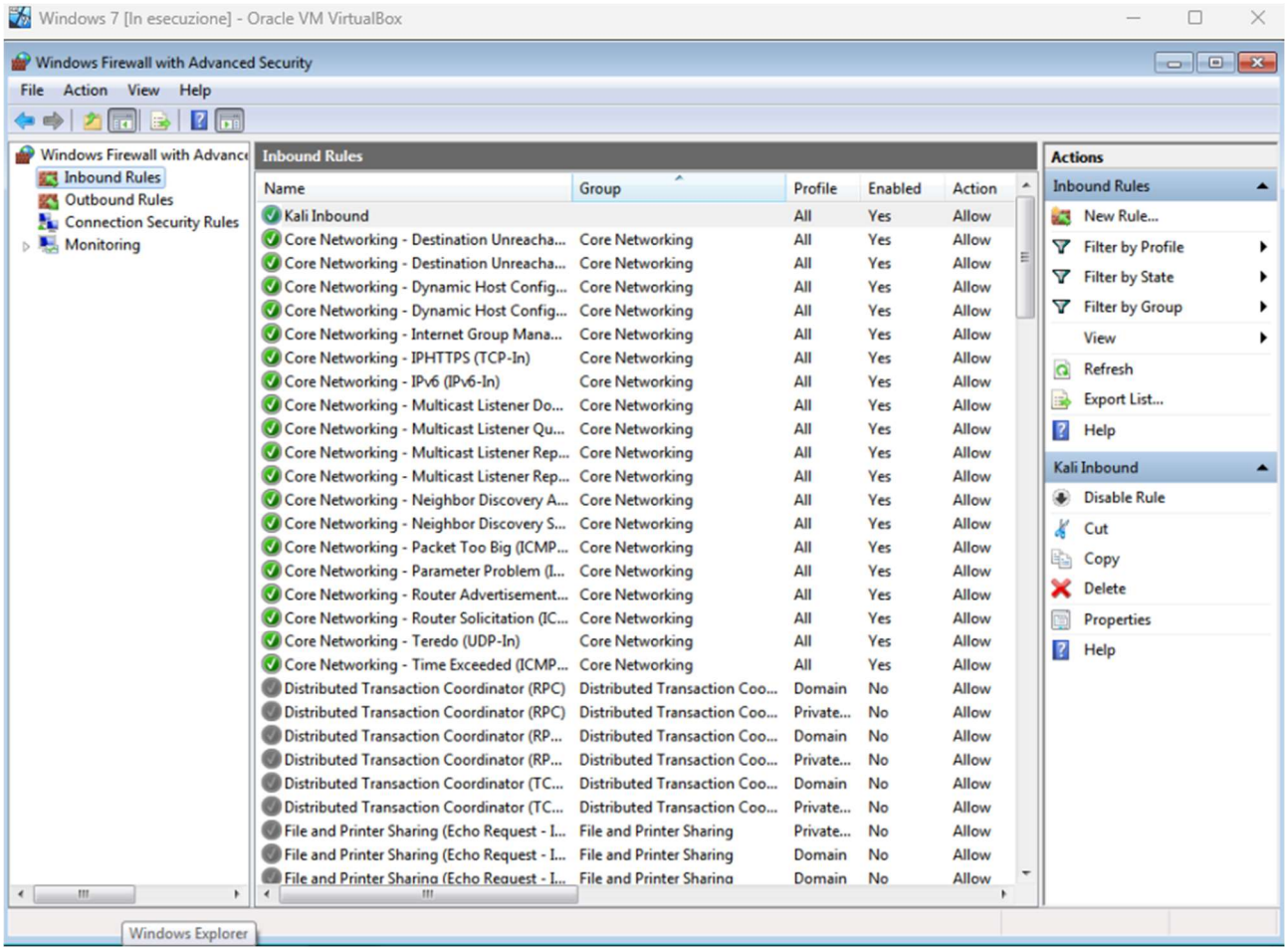
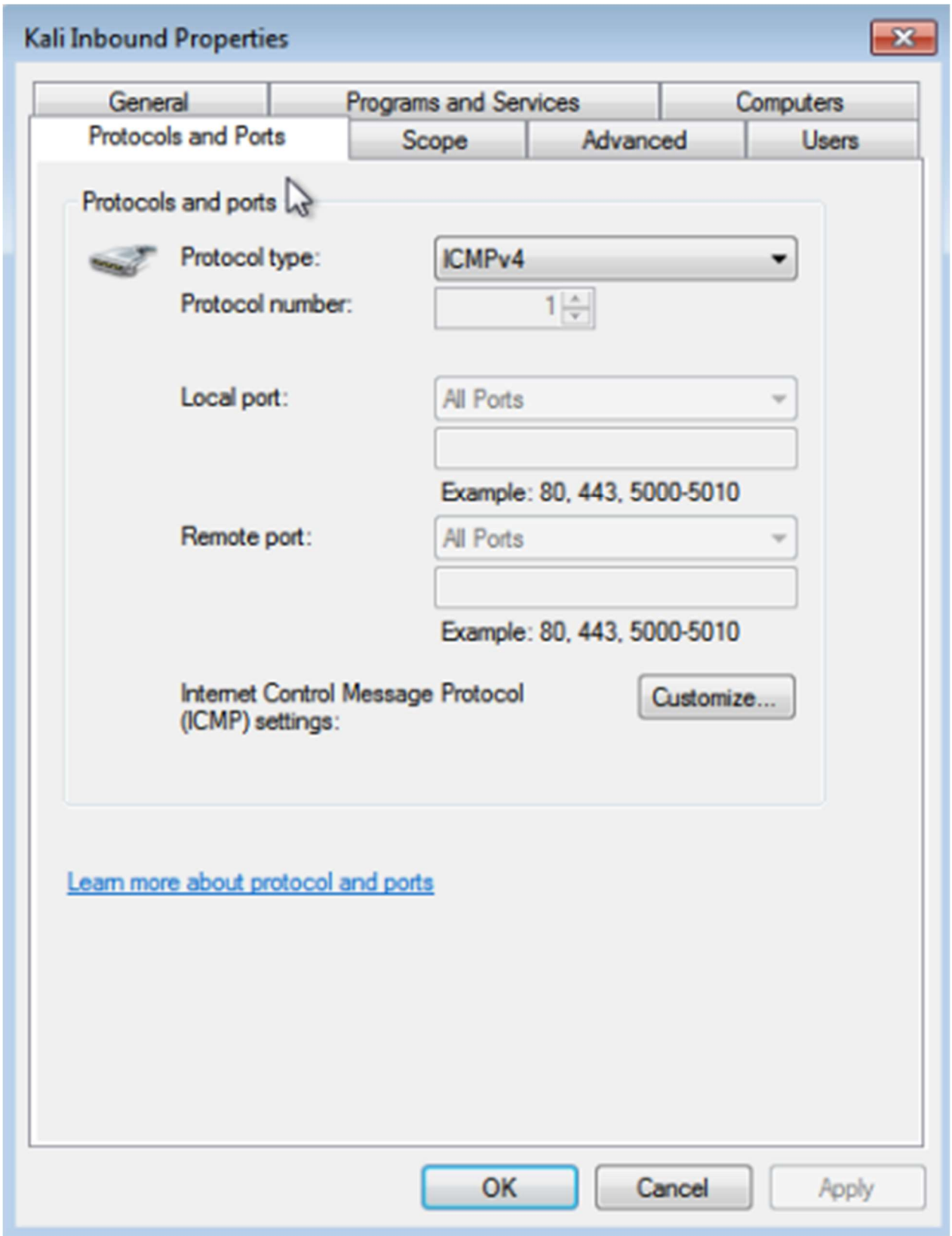
UTILIZZO DI FIREWALL WINDOWS E WIRESHARK

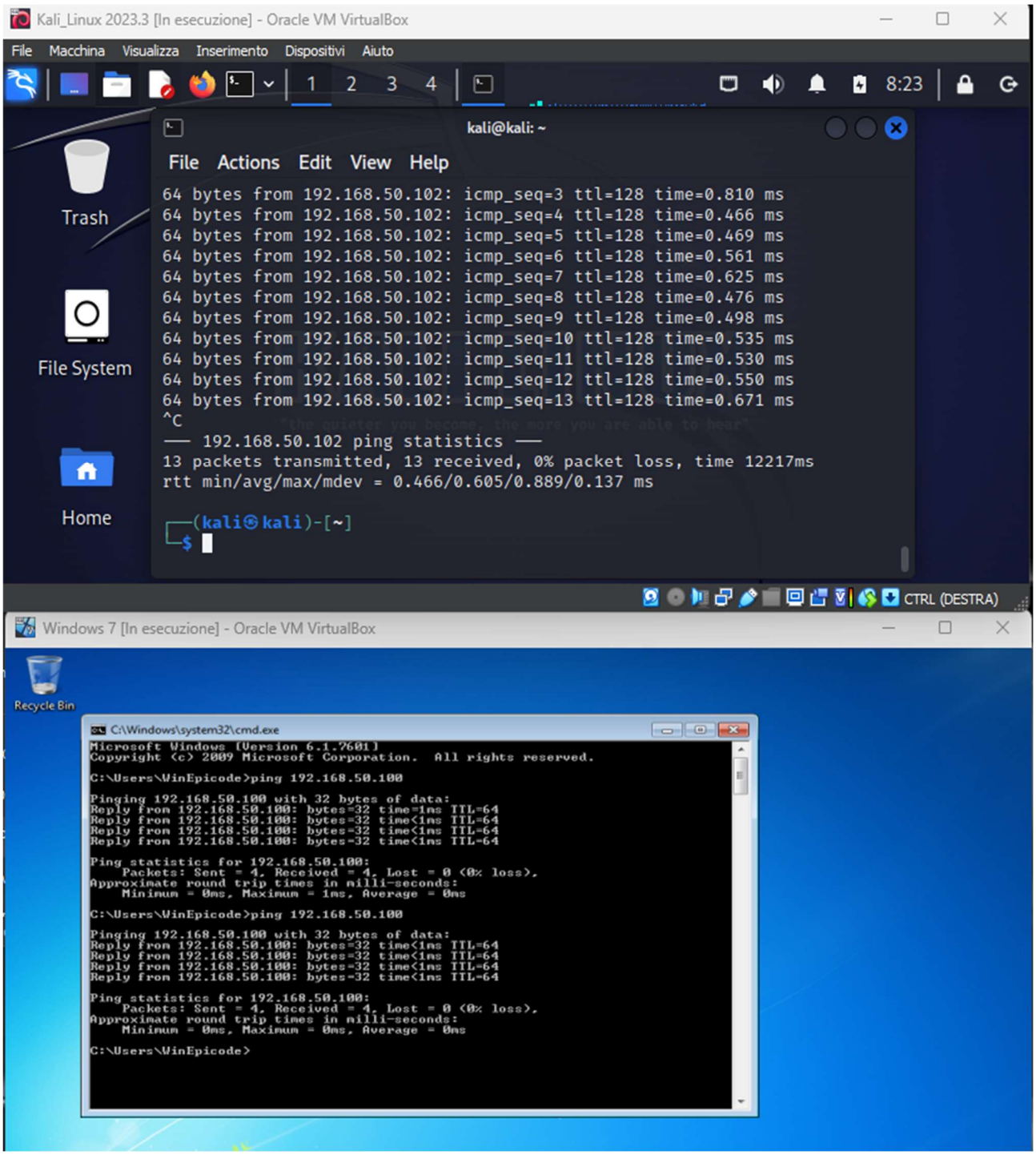
CONFIGURARE POLICY PER PERMETTERE IL PING DA FRA MACCHINE WINDOWS 7 E KALI LINUX.

Entro nella macchina virtuale di Windows 7 e accedo al Firewall di sistema per configurare una regola che permette la comunicazione TCP fra Windows e Kali Linux



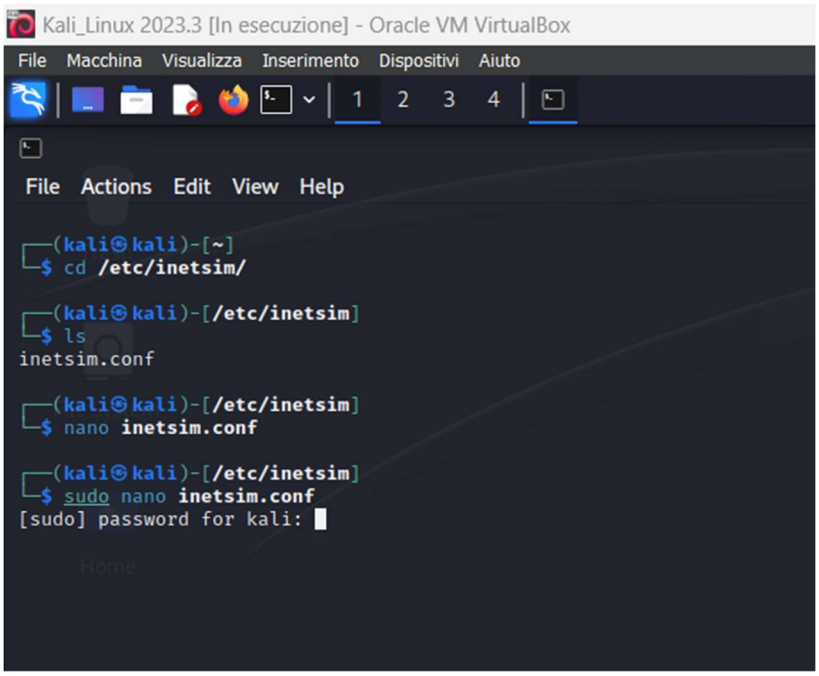
Ho creato una regola sia in ingresso che in uscita dalla macchina Windows7. Dopo di che sono entrato nelle Proprietà della regola e ho impostato il protocollo ICMPv4 (premetto che sulla pagina di creazionequesta voce non era presente fra le opzioni e ho dovuto fare così). Successivamente ho lanciato il comando PING su entrambe le macchine per verificarne la corretta configurazione.


Kali Inbound 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
OK
Cancel
Apply

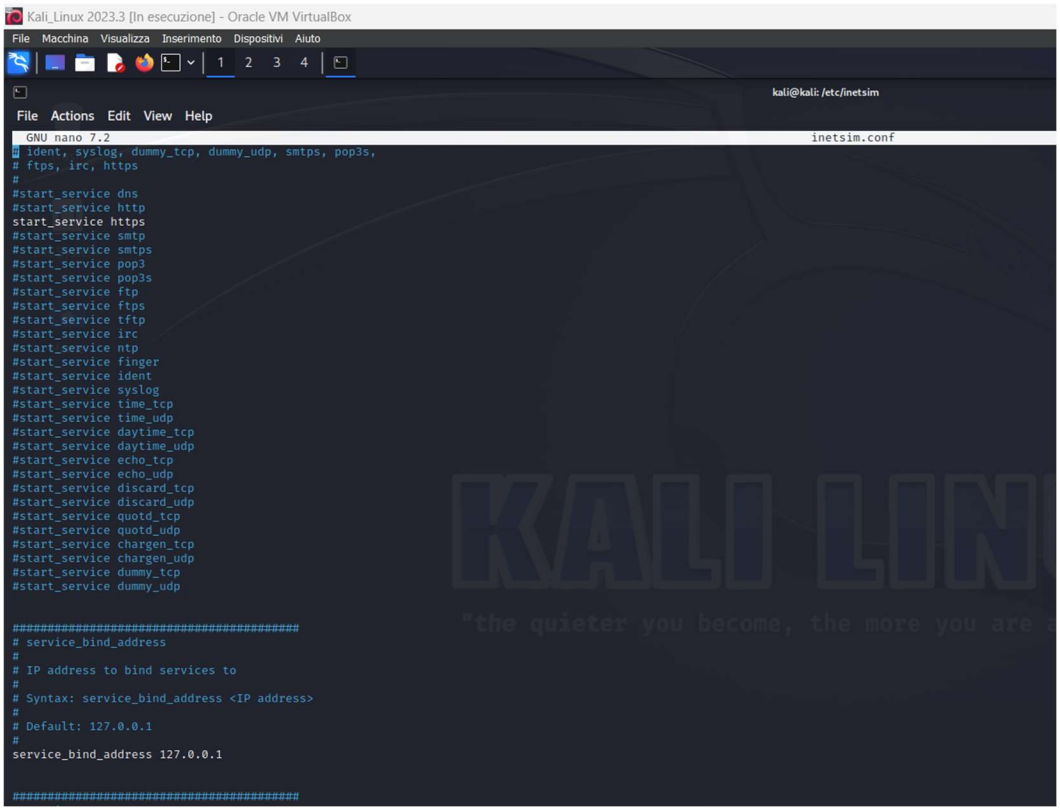

Kali_Linux 2023.3 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
1 2 3 4
8:23
kali@kali: ~
File Actions Edit View Help
64 bytes from 192.168.50.102: icmp_seq=3 ttl=128 time=0.810 ms
64 bytes from 192.168.50.102: icmp_seq=4 ttl=128 time=0.466 ms
64 bytes from 192.168.50.102: icmp_seq=5 ttl=128 time=0.469 ms
64 bytes from 192.168.50.102: icmp_seq=6 ttl=128 time=0.561 ms
64 bytes from 192.168.50.102: icmp_seq=7 ttl=128 time=0.625 ms
64 bytes from 192.168.50.102: icmp_seq=8 ttl=128 time=0.476 ms
64 bytes from 192.168.50.102: icmp_seq=9 ttl=128 time=0.498 ms
64 bytes from 192.168.50.102: icmp_seq=10 ttl=128 time=0.535 ms
64 bytes from 192.168.50.102: icmp_seq=11 ttl=128 time=0.530 ms
64 bytes from 192.168.50.102: icmp_seq=12 ttl=128 time=0.550 ms
64 bytes from 192.168.50.102: icmp_seq=13 ttl=128 time=0.671 ms
^C
— 192.168.50.102 ping statistics —
13 packets transmitted, 13 received, 0% packet loss, time 12217ms
rtt min/avg/max/mdev = 0.466/0.605/0.889/0.137 ms
(kali㉿kali)-[~]
$
Trash
File System
Home
CTRL (DESTRA)
Windows 7 [In esecuzione] - Oracle VM VirtualBox
Recycle Bin
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\WinEpicode>ping 192.168.50.100
Pinging 192.168.50.100 with 32 bytes of data:
Reply from 192.168.50.100: bytes=32 time=1ms TTL=64
Reply from 192.168.50.100: bytes=32 time<1ms TTL=64
Reply from 192.168.50.100: bytes=32 time<1ms TTL=64
Reply from 192.168.50.100: bytes=32 time<1ms TTL=64
Ping statistics for 192.168.50.100:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\Users\WinEpicode>ping 192.168.50.100
Pinging 192.168.50.100 with 32 bytes of data:
Reply from 192.168.50.100: bytes=32 time<1ms TTL=64
Reply from 192.168.50.100: bytes=32 time<1ms TTL=64
Reply from 192.168.50.100: bytes=32 time<1ms TTL=64
Reply from 192.168.50.100: bytes=32 time<1ms TTL=64
Ping statistics for 192.168.50.100:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\Users\WinEpicode>

UTILIZZO DELLA UTILITY DELL'INETSIM PER L'EMULAZIONE DI SERVIZI INTERNET

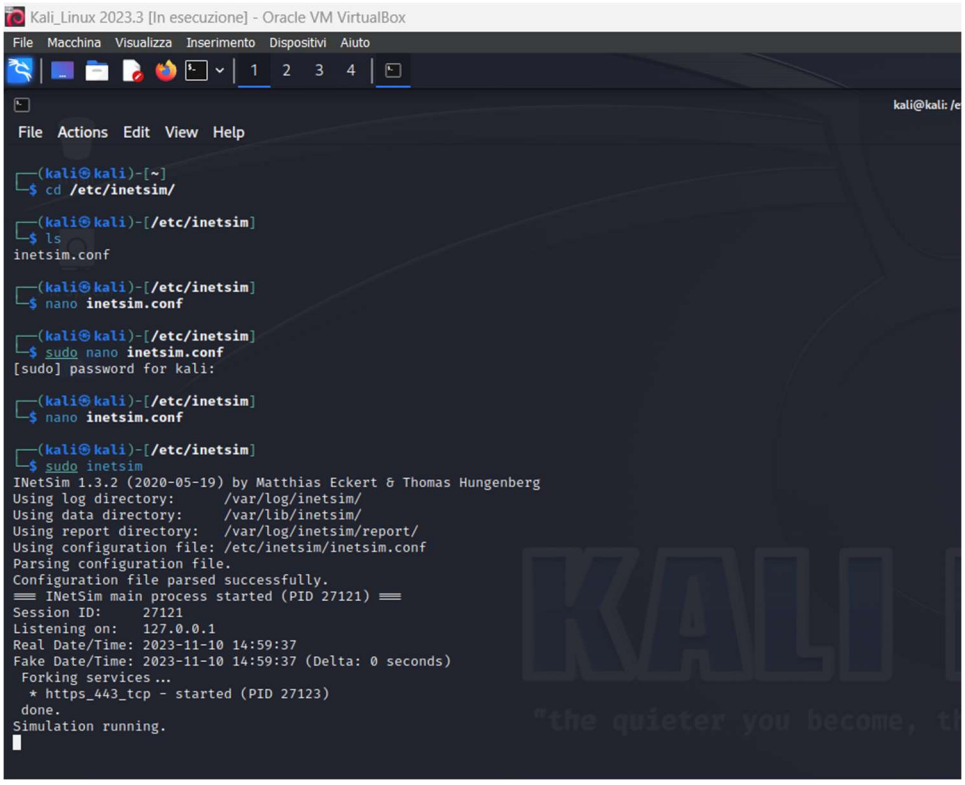
Avvio la macchina virtuale Kali-Linux e command prompt per accedere alla modifica del file inetsim.conf



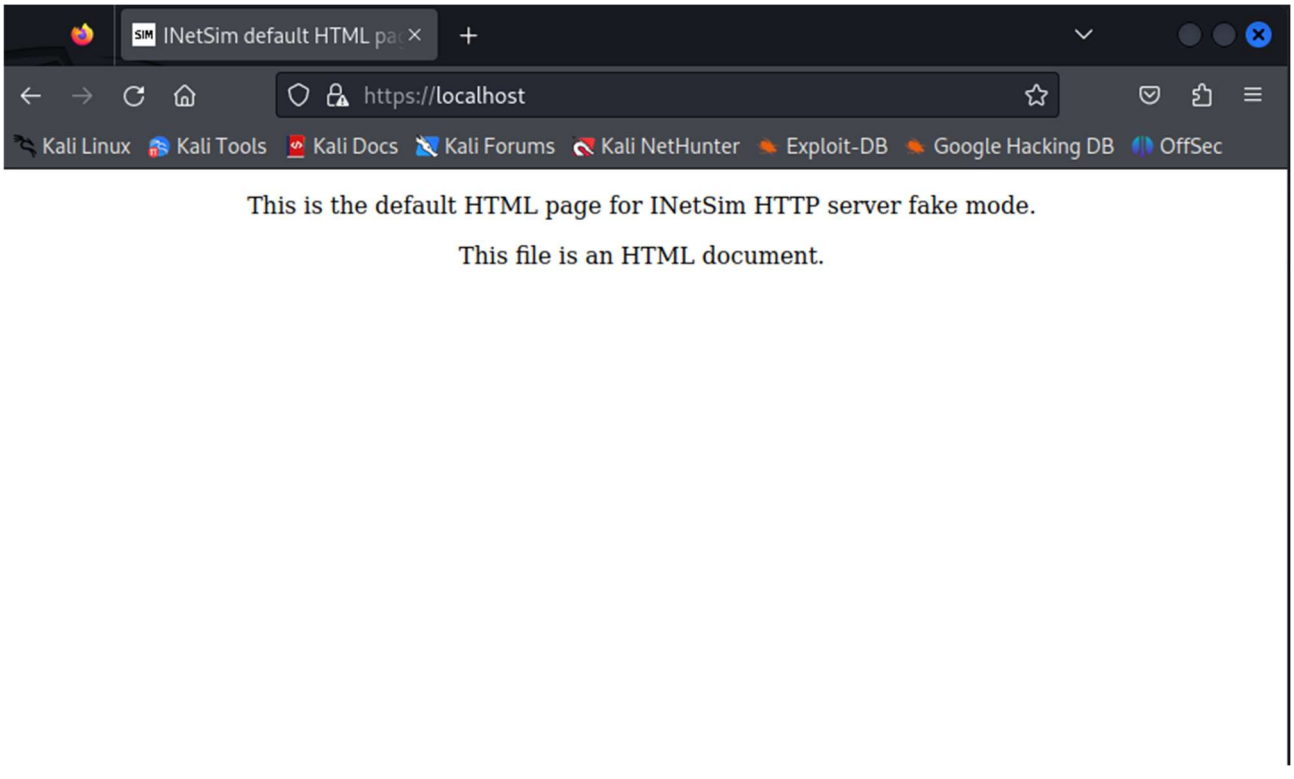
Per praticità, mostro la schermata con la modifica dei servizi offerti solo su http e https. Forzo la porta su quella di localhost=127.0.0.1



Una volta salvato ed effettuato la modifica (ovviamente il file aperto con il comando sudo, altrimenti non sarebbe possibile salvarlo) avvio il servizio InetSim tramite comando **sudo inetsim.**

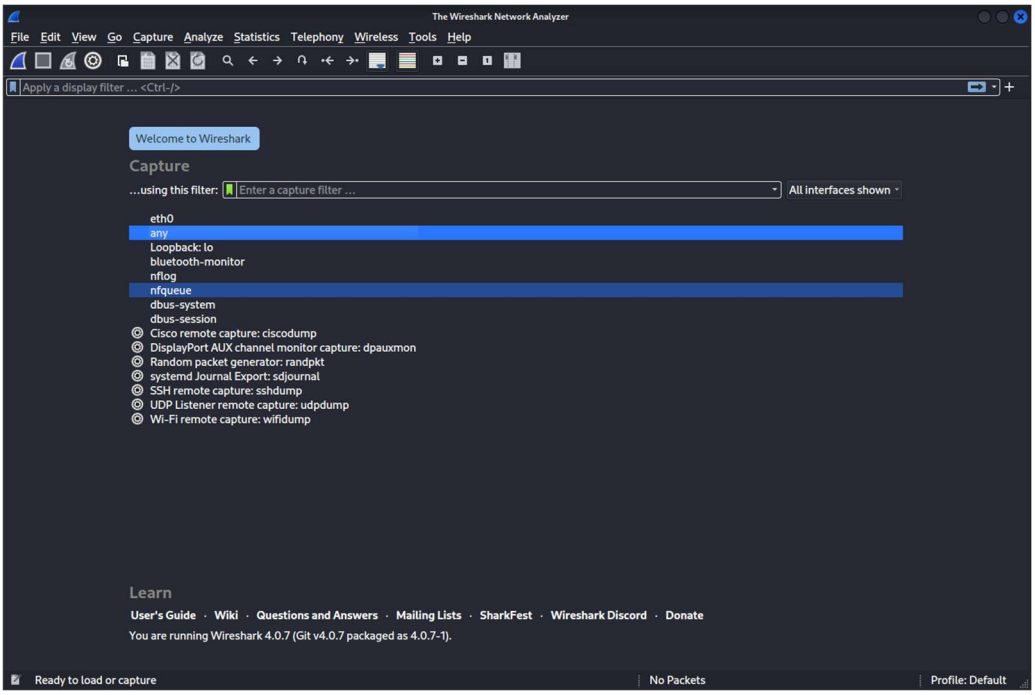


Per verificare che la sia effettivamente avviato, apro una pagina web puntando la ricerca su https://localhost.

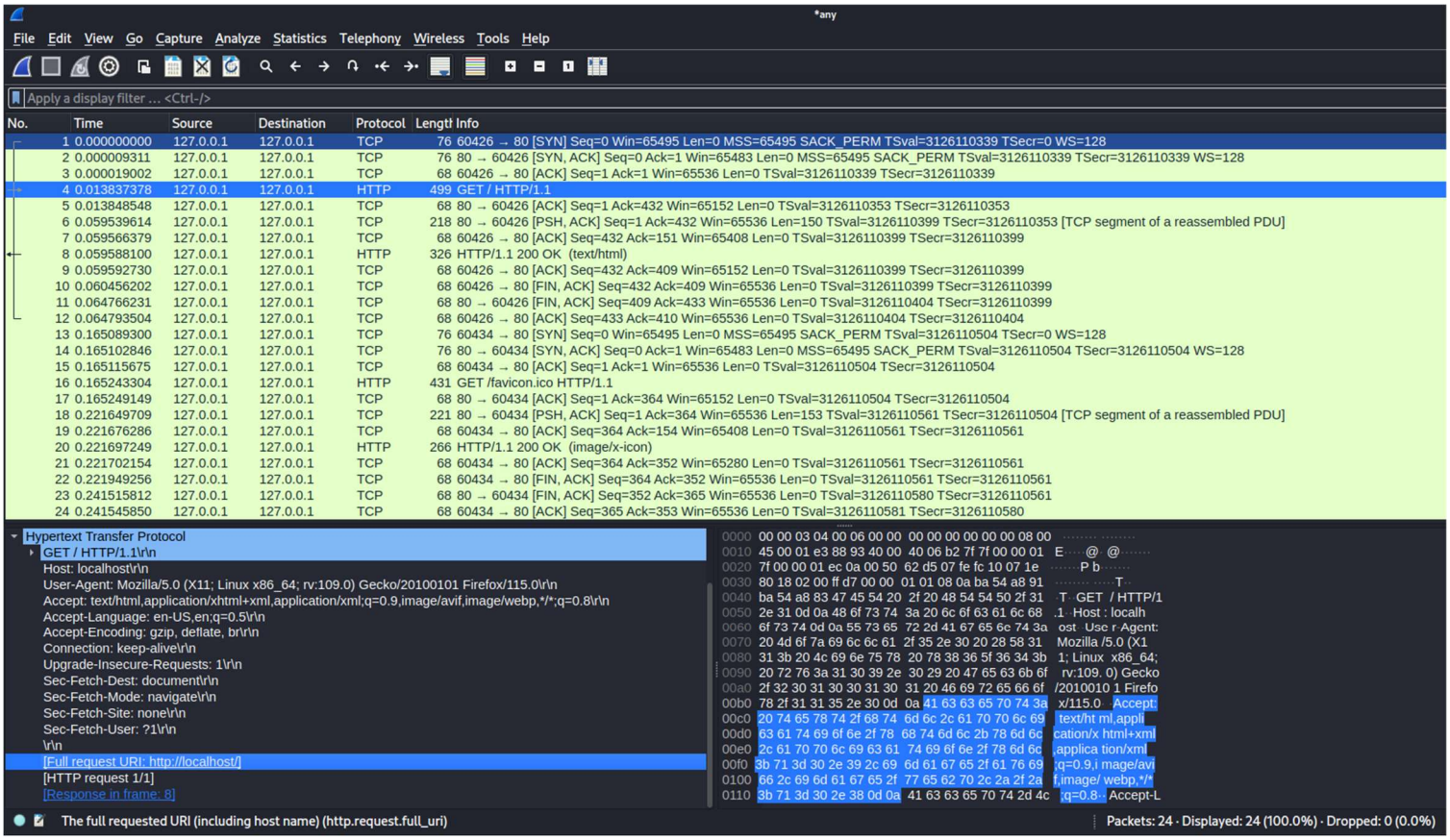


CATTURA DI PACCHETTI CON WIRESHARK

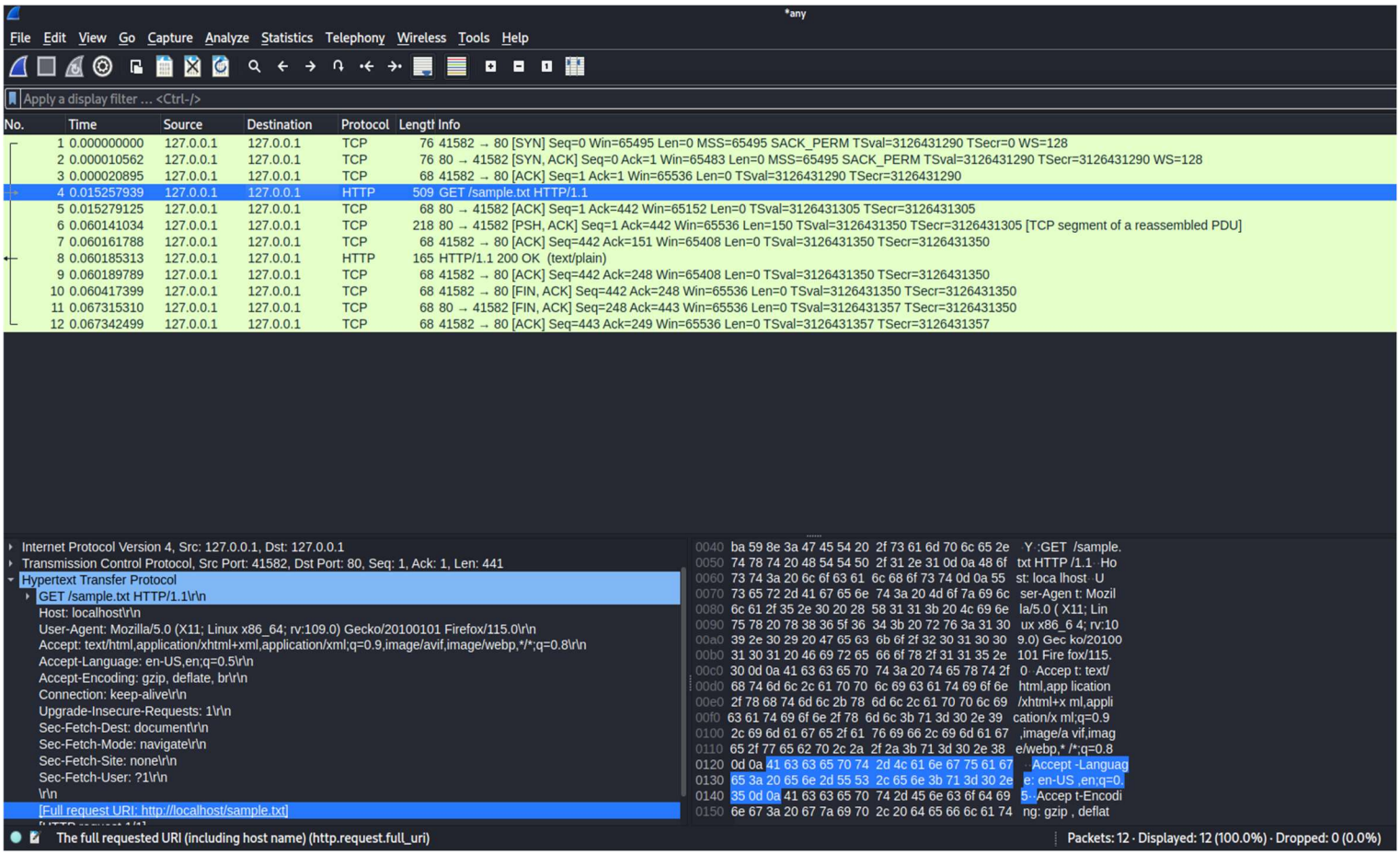
Lasciando configurato InetSim come in precedenza, ho avviato una pagina di ricerca in Kali-linux e avvia Wireshark in ascolto su tutte le porte di rete configurate.



Quello che riporto qui sotto è la cattura dei pacchetti ricercando sul browser http://localhost ed evidenziando il pacchetto GET.

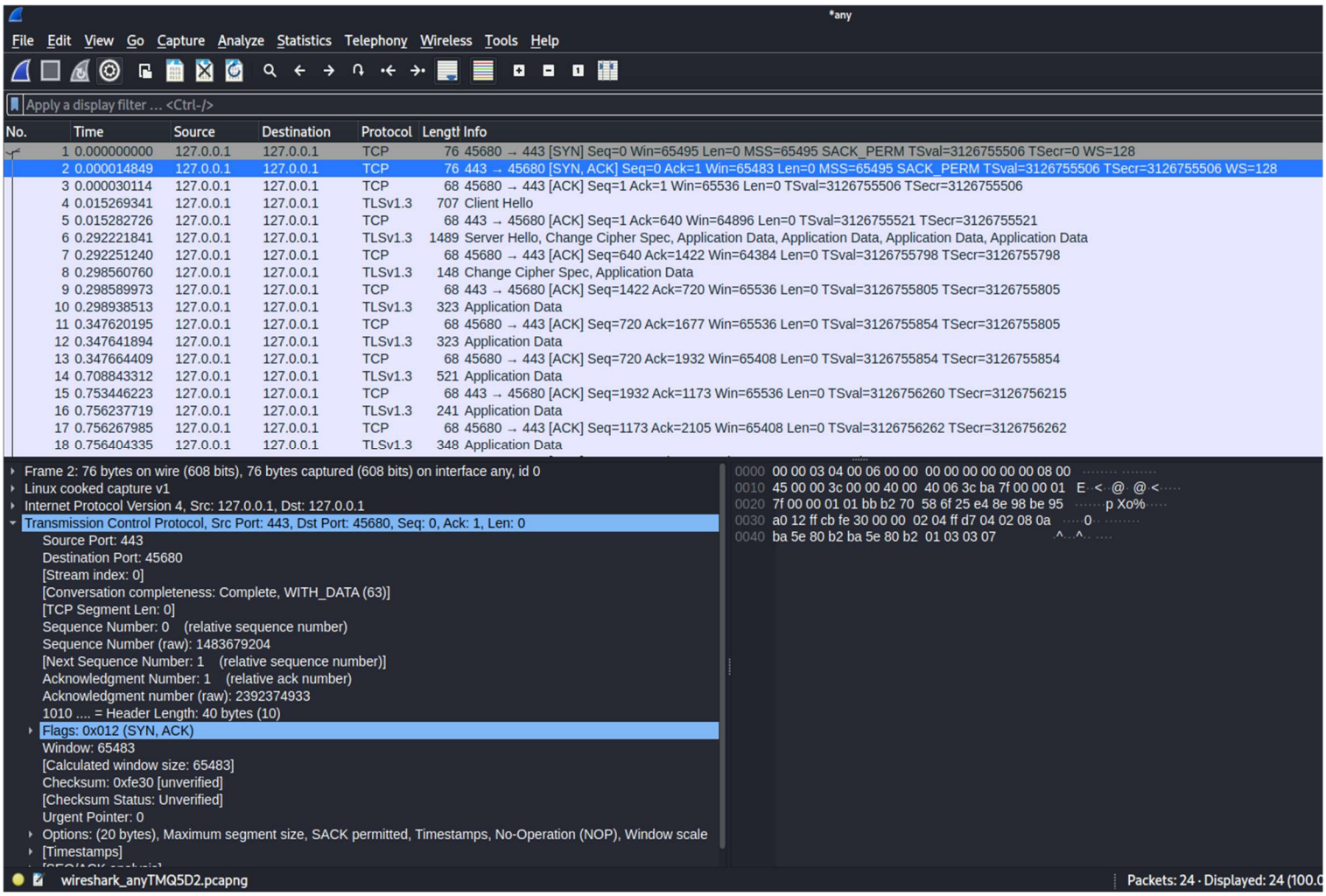


In questa schermata dopo ho effettuato una nuova ricerca su un file presente in localhost che è sample.txt sempre sotto protocollo http. In pratica ho ricercato questo: http://localhost/sample.txt



Quando si utilizza protocollo HTTP i pacchetti sono scritti in chiaro e quindi posso vederne il contenuto che il client ha richiesto al server.

Dopo di questa ho fatto la cattura dei pacchetti con protocollo HTTPS.
Riparto ricercando sul browser questa volta con: https://localhost



Ovviamente il discorso qui cambia in quanto si usa il protocollo HTTPS che cifra il contenuto del pacchetto in viaggio e di fatto non mi è possibile verificarne il contenuto che sta transitando. Di seguito provo a ricercare https://localhost/sample.txt

MATTIA SATTIN 11-11-2023 W3D5