

# Report M1W3D5

L'esercizio di oggi mira a consolidare le conoscenze acquisite.

Vedremo due esercizi: I) la configurazione di una policy sul firewall windows; II) una packet capture con Wireshark.

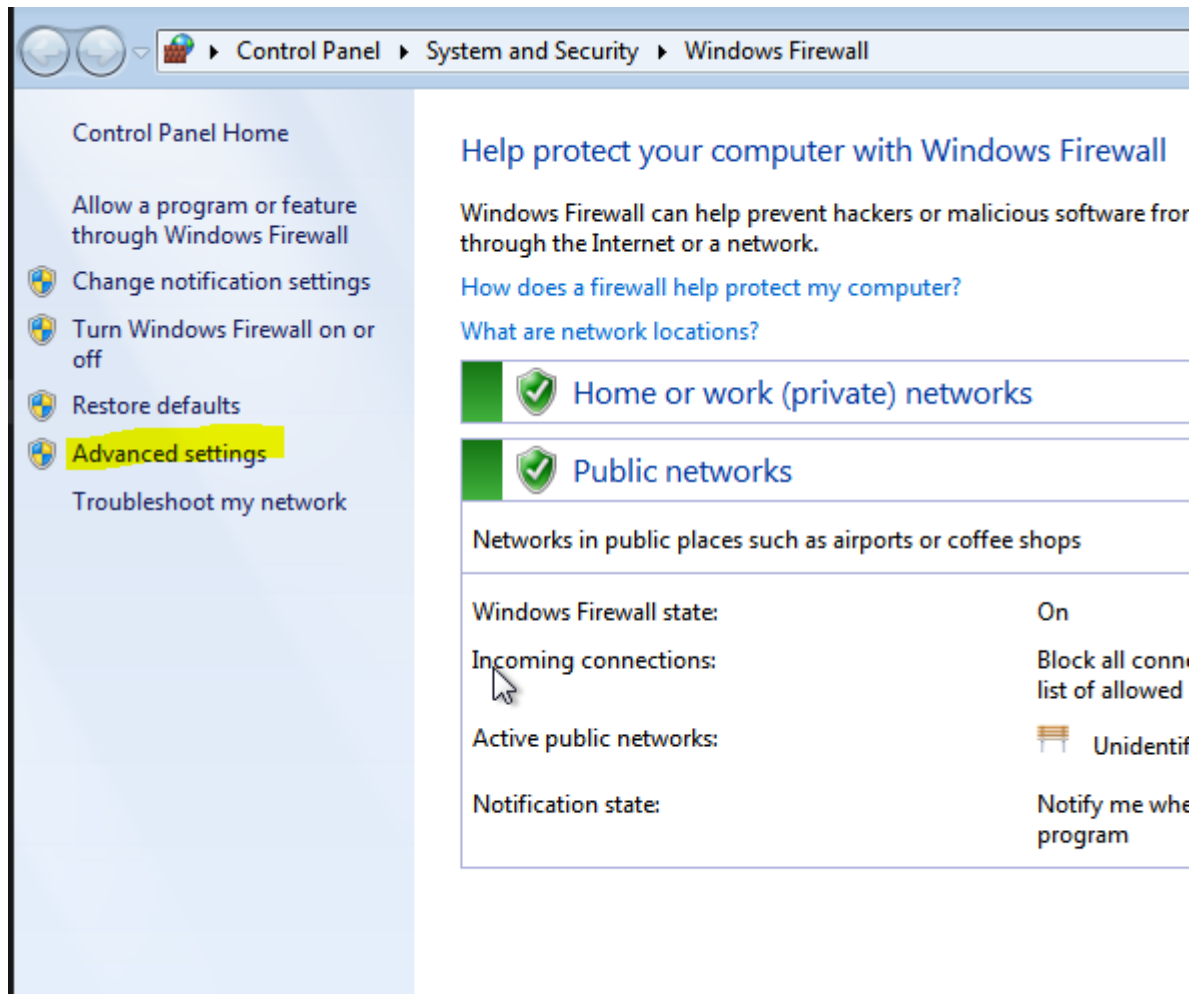
Vedremo anche come simulare alcuni servizi di rete con un tool pre-installato su Kali Linux (InetSim)

## **Esercizio:**

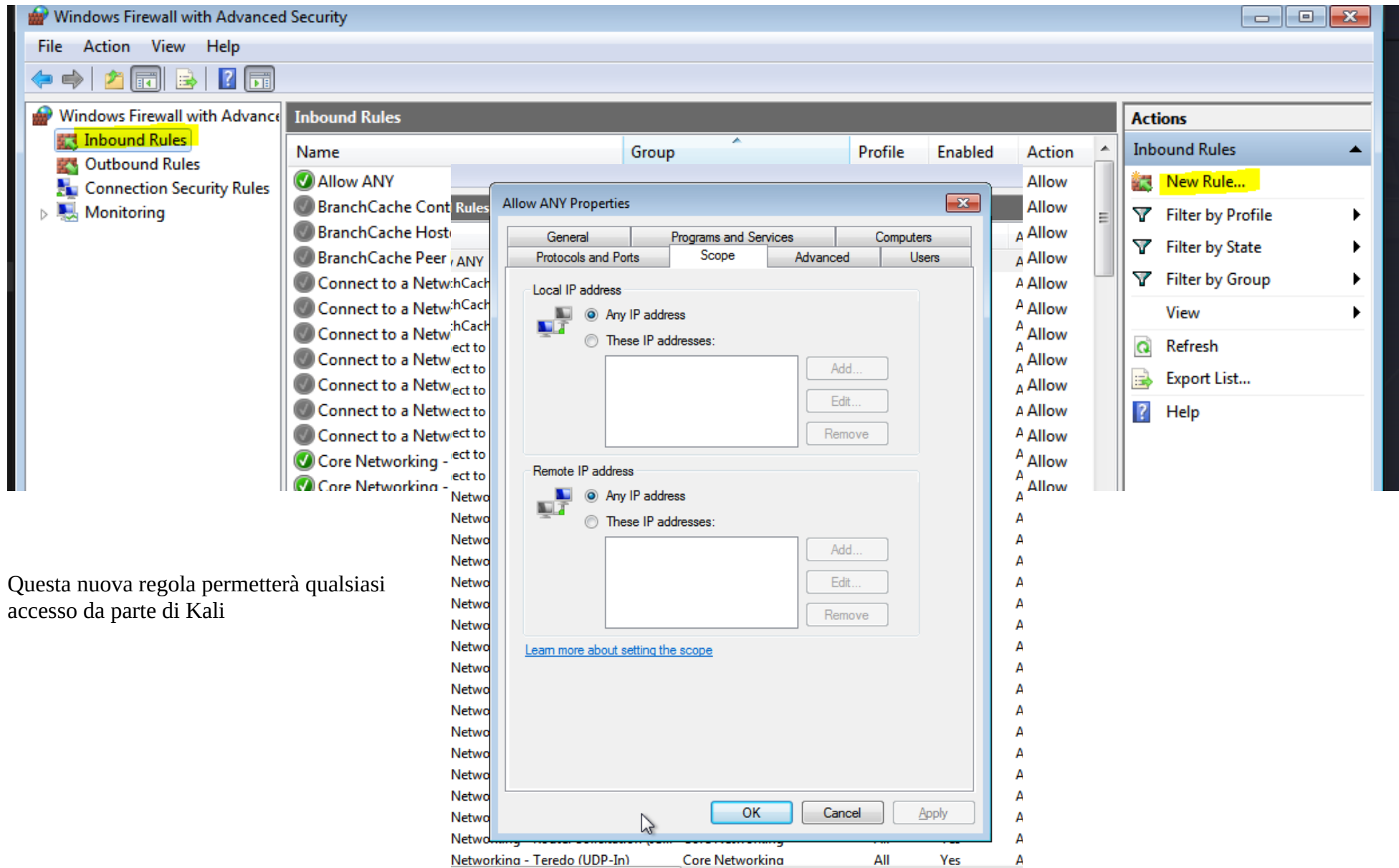
- Configurare policy per permettere il ping da macchine Linux a Macchina Windows 7 nel nostro laboratorio (Windows firewall)
- Utilizzo dell'utility InetSim per l'emulazione di servizi Internet
- Cattura di pacchetti con Wireshark

- **CONFIGURAZIONE DEL FIREWALL WINDOWS:**

Dal Pannello di controllo accedo alle impostazioni del firewall, dopodiché navigo nelle impostazioni avanzate

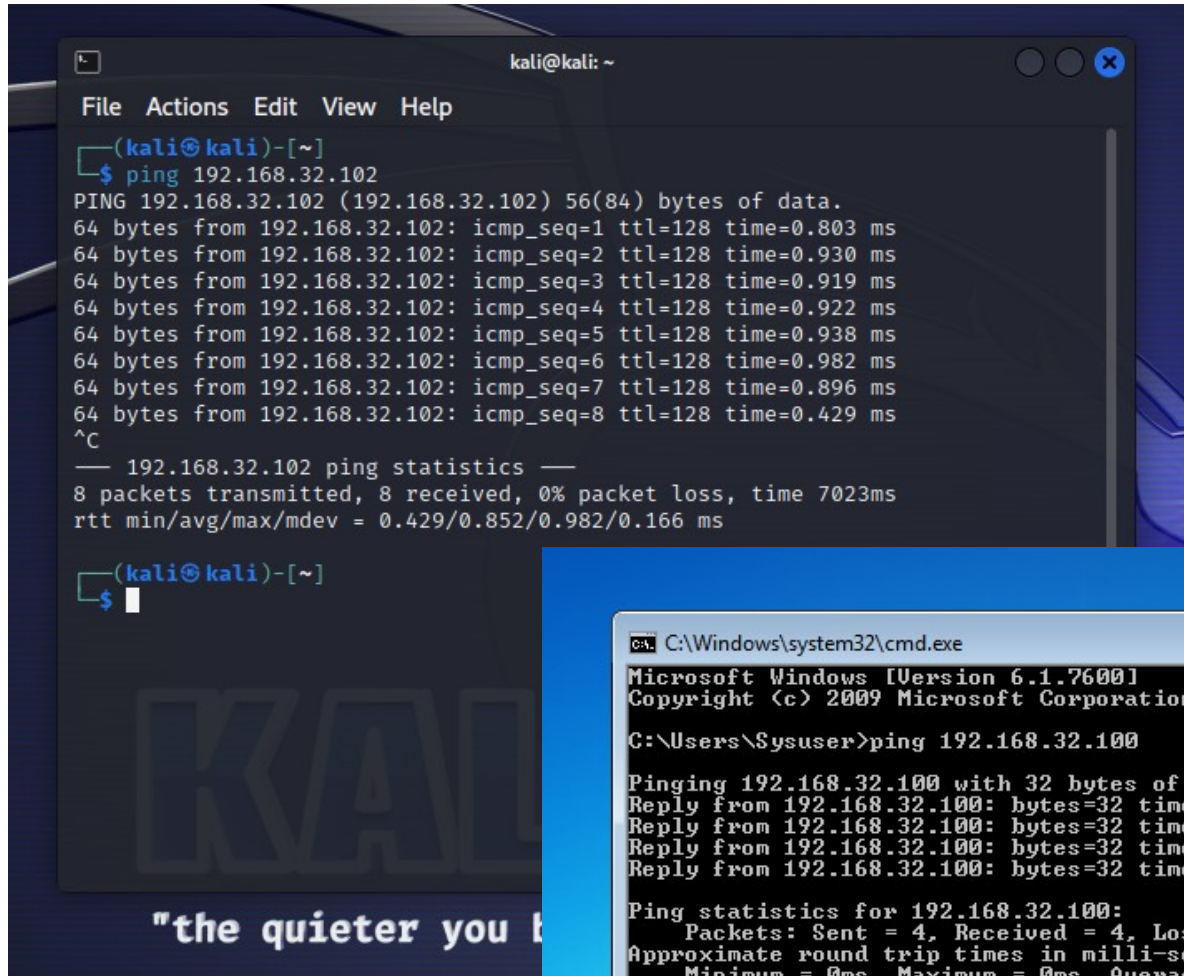


Accedo al sotto menu delle regole in entrata dove creerò una nuova regola da mettere in cima

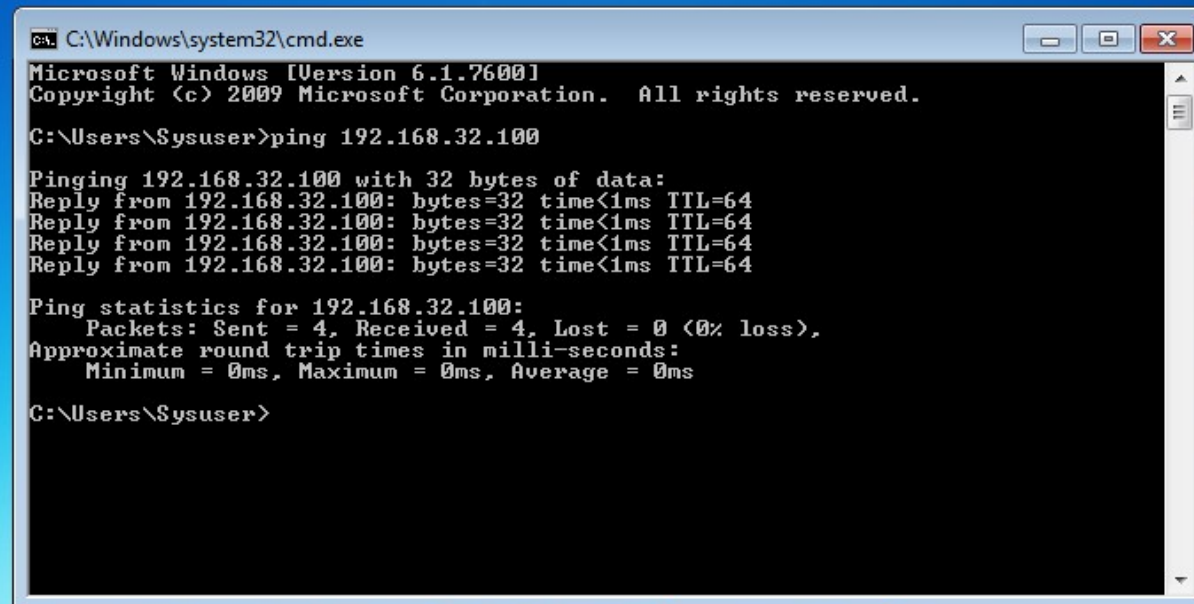


Questa nuova regola permetterà qualsiasi accesso da parte di Kali

Controllo che le due macchine comunichino con il comando PING



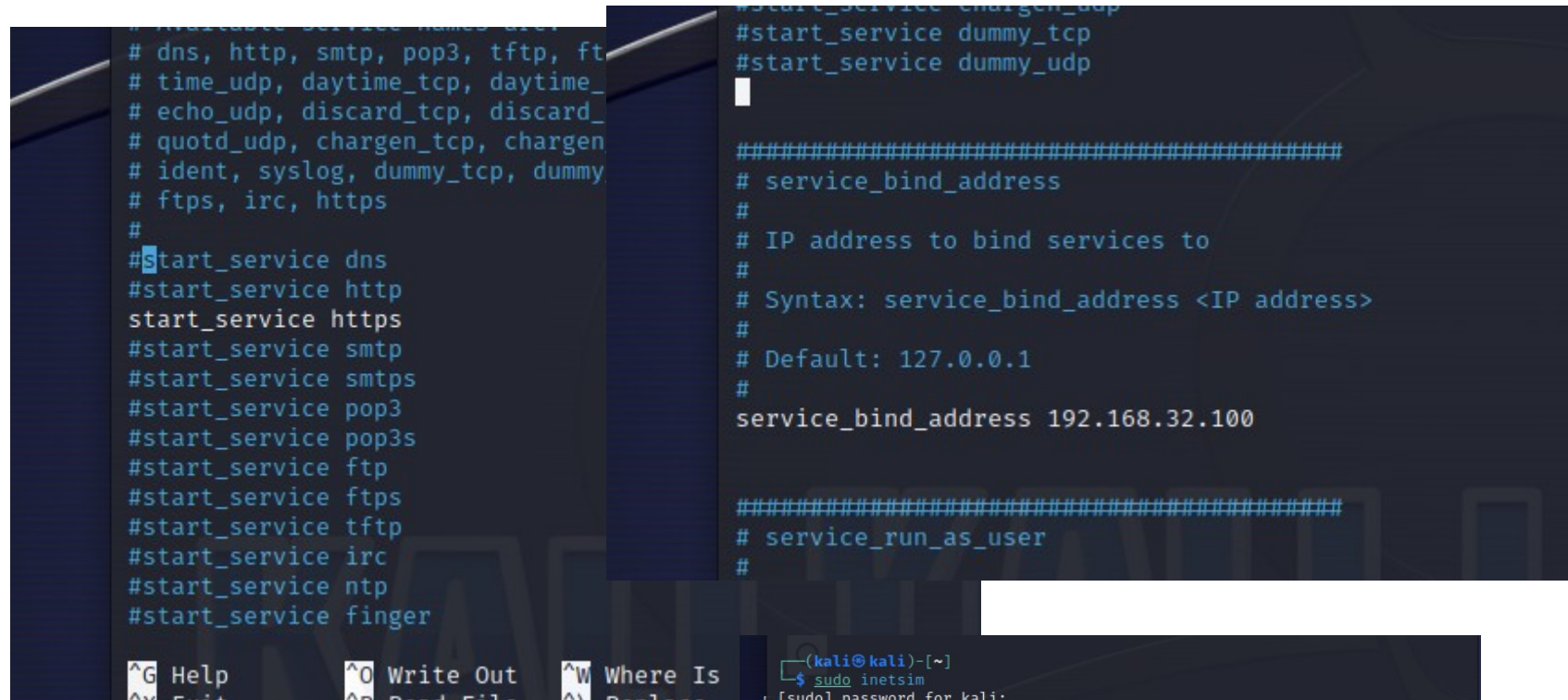
```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ ping 192.168.32.102  
PING 192.168.32.102 (192.168.32.102) 56(84) bytes of data.  
64 bytes from 192.168.32.102: icmp_seq=1 ttl=128 time=0.803 ms  
64 bytes from 192.168.32.102: icmp_seq=2 ttl=128 time=0.930 ms  
64 bytes from 192.168.32.102: icmp_seq=3 ttl=128 time=0.919 ms  
64 bytes from 192.168.32.102: icmp_seq=4 ttl=128 time=0.922 ms  
64 bytes from 192.168.32.102: icmp_seq=5 ttl=128 time=0.938 ms  
64 bytes from 192.168.32.102: icmp_seq=6 ttl=128 time=0.982 ms  
64 bytes from 192.168.32.102: icmp_seq=7 ttl=128 time=0.896 ms  
64 bytes from 192.168.32.102: icmp_seq=8 ttl=128 time=0.429 ms  
^C  
— 192.168.32.102 ping statistics —  
8 packets transmitted, 8 received, 0% packet loss, time 7023ms  
rtt min/avg/max/mdev = 0.429/0.852/0.982/0.166 ms  
  
(kali@kali)-[~]  
$
```



```
C:\Windows\system32\cmd.exe  
Microsoft Windows [Version 6.1.7600]  
Copyright (c) 2009 Microsoft Corporation. All rights reserved.  
  
C:\Users\Sysuser>ping 192.168.32.100  
  
Pinging 192.168.32.100 with 32 bytes of data:  
Reply from 192.168.32.100: bytes=32 time<1ms TTL=64  
Reply from 192.168.32.100: bytes=32 time<1ms TTL=64  
Reply from 192.168.32.100: bytes=32 time<1ms TTL=64  
Reply from 192.168.32.100: bytes=32 time<1ms TTL=64  
  
Ping statistics for 192.168.32.100:  
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 0ms, Maximum = 0ms, Average = 0ms  
  
C:\Users\Sysuser>
```

- CONFIGURAZIONE INETSIM SU KALI:

Lancio l'editor di testo e configuro le impostazioni di inetsim “sudo nano /etc/inetsim/inetsim.conf”

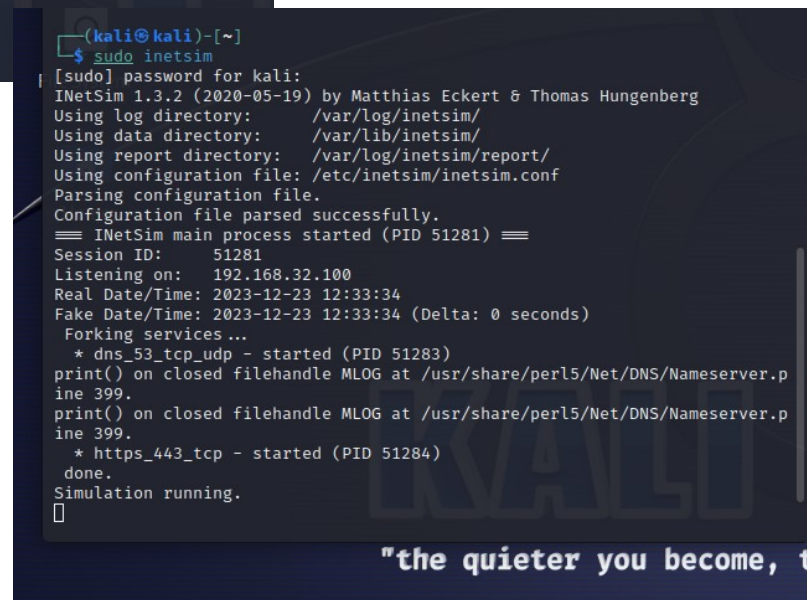


```
# dns, http, smtp, pop3, tftp, ft
# time_udp, daytime_tcp, daytime_
# echo_udp, discard_tcp, discard_
# quotd_udp, chargen_tcp, chargen
# ident, syslog, dummy_tcp, dummy
# ftps, irc, https
#
#start_service dns
#start_service http
start_service https
#start_service smtp
#start_service smtps
#start_service pop3
#start_service pop3s
#start_service ftp
#start_service ftps
#start_service tftp
#start_service irc
#start_service ntp
#start_service finger

#####
# service_bind_address
#
# IP address to bind services to
#
# Syntax: service_bind_address <IP address>
#
# Default: 127.0.0.1
#
service_bind_address 192.168.32.100

#####
# service_run_as_user
#
```

Poi lancio inetsim da terminale “sudo inetsim”

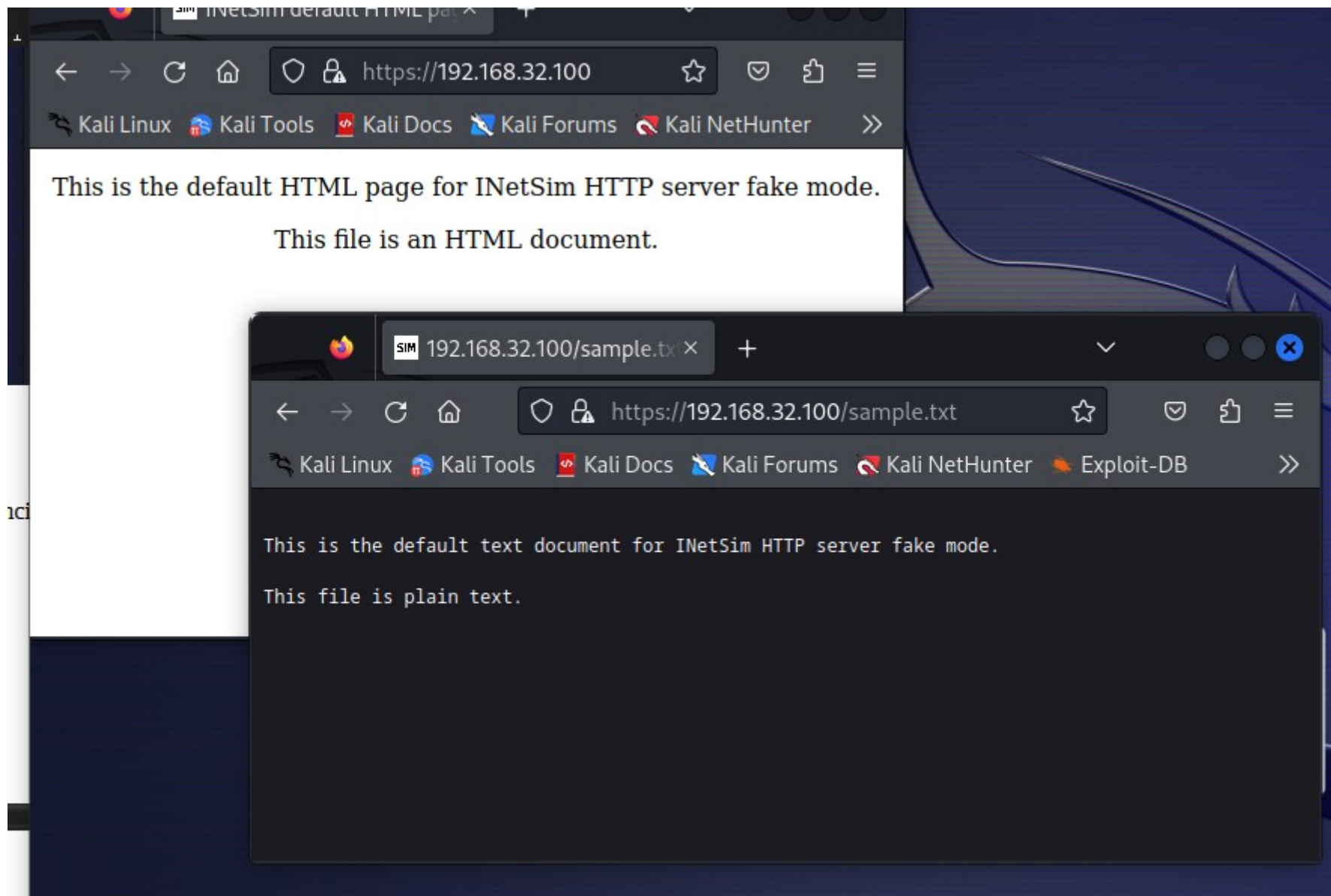


```
(kali@kali)-[~]
$ sudo inetsim
[sudo] password for kali:
InetSim 1.3.2 (2020-05-19) by Matthias Eckert & Thomas Hungenberg
Using log directory: /var/log/inetsim/
Using data directory: /var/lib/inetsim/
Using report directory: /var/log/inetsim/report/
Using configuration file: /etc/inetsim/inetsim.conf
Parsing configuration file.
Configuration file parsed successfully.
== InetSim main process started (PID 51281) ==
Session ID: 51281
Listening on: 192.168.32.100
Real Date/Time: 2023-12-23 12:33:34
Fake Date/Time: 2023-12-23 12:33:34 (Delta: 0 seconds)
Forking services...
* dns_53_tcp_udp - started (PID 51283)
print() on closed filehandle MLOG at /usr/share/perl5/Net/DNS/Nameserver.p
ine 399.
print() on closed filehandle MLOG at /usr/share/perl5/Net/DNS/Nameserver.p
ine 399.
* https_443_tcp - started (PID 51284)
done.
Simulation running.
█
```

"the quieter you become, t

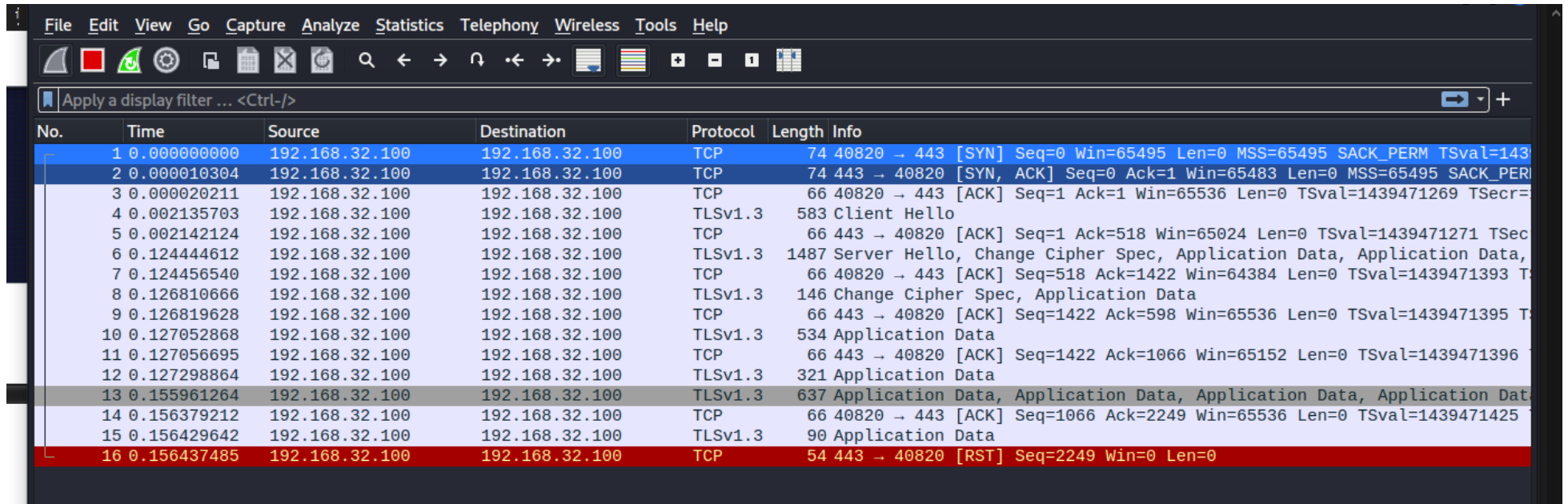


Controllo che il servizio di simulazione sia attivo con un browser



- **CATTURA PACCHETTI CON WIRESHARK:**

Avvio il programma Wireshark da menu o da terminale, selezionando il filtro loopback



The screenshot shows the Wireshark interface with the following components:

- Menu Bar:** File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help.
- Toolbar:** Contains icons for file operations, capture, analysis, and display.
- Filter Bar:** Displays "Apply a display filter ... <Ctrl-/>" with a button to open the filter dialog.
- Packets List:** A table showing 16 captured packets. The first 15 packets are from 192.168.32.100 to 192.168.32.100, and the 16th packet is a RST from 192.168.32.100 to 192.168.32.100.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.32.100	192.168.32.100	TCP	74	40820 → 443 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM TSval=143
2	0.000010304	192.168.32.100	192.168.32.100	TCP	74	443 → 40820 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=65495 SACK_PER
3	0.000020211	192.168.32.100	192.168.32.100	TCP	66	40820 → 443 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=1439471269 TSecr=
4	0.002135703	192.168.32.100	192.168.32.100	TLSv1.3	583	Client Hello
5	0.002142124	192.168.32.100	192.168.32.100	TCP	66	443 → 40820 [ACK] Seq=1 Ack=518 Win=65024 Len=0 TSval=1439471271 TSec
6	0.124444612	192.168.32.100	192.168.32.100	TLSv1.3	1487	Server Hello, Change Cipher Spec, Application Data, Application Data,
7	0.124456540	192.168.32.100	192.168.32.100	TCP	66	40820 → 443 [ACK] Seq=518 Ack=1422 Win=64384 Len=0 TSval=1439471393 T
8	0.126810666	192.168.32.100	192.168.32.100	TLSv1.3	146	Change Cipher Spec, Application Data
9	0.126819628	192.168.32.100	192.168.32.100	TCP	66	443 → 40820 [ACK] Seq=1422 Ack=598 Win=65536 Len=0 TSval=1439471395 T
10	0.127052868	192.168.32.100	192.168.32.100	TLSv1.3	534	Application Data
11	0.127056695	192.168.32.100	192.168.32.100	TCP	66	443 → 40820 [ACK] Seq=1422 Ack=1066 Win=65152 Len=0 TSval=1439471396
12	0.127298864	192.168.32.100	192.168.32.100	TLSv1.3	321	Application Data
13	0.155961264	192.168.32.100	192.168.32.100	TLSv1.3	637	Application Data, Application Data, Application Data, Application Dat
14	0.156379212	192.168.32.100	192.168.32.100	TCP	66	40820 → 443 [ACK] Seq=1066 Ack=2249 Win=65536 Len=0 TSval=1439471425
15	0.156429642	192.168.32.100	192.168.32.100	TLSv1.3	90	Application Data
16	0.156437485	192.168.32.100	192.168.32.100	TCP	54	443 → 40820 [RST] Seq=2249 Win=0 Len=0