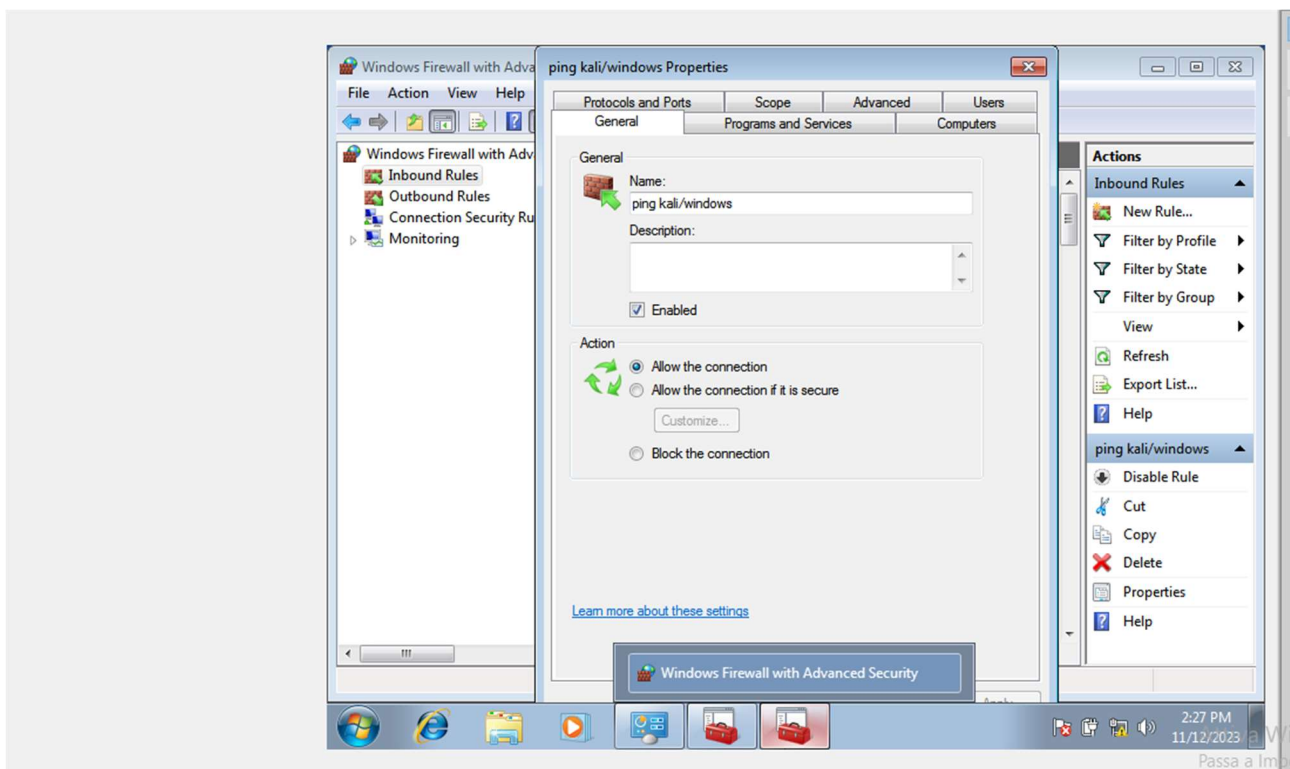
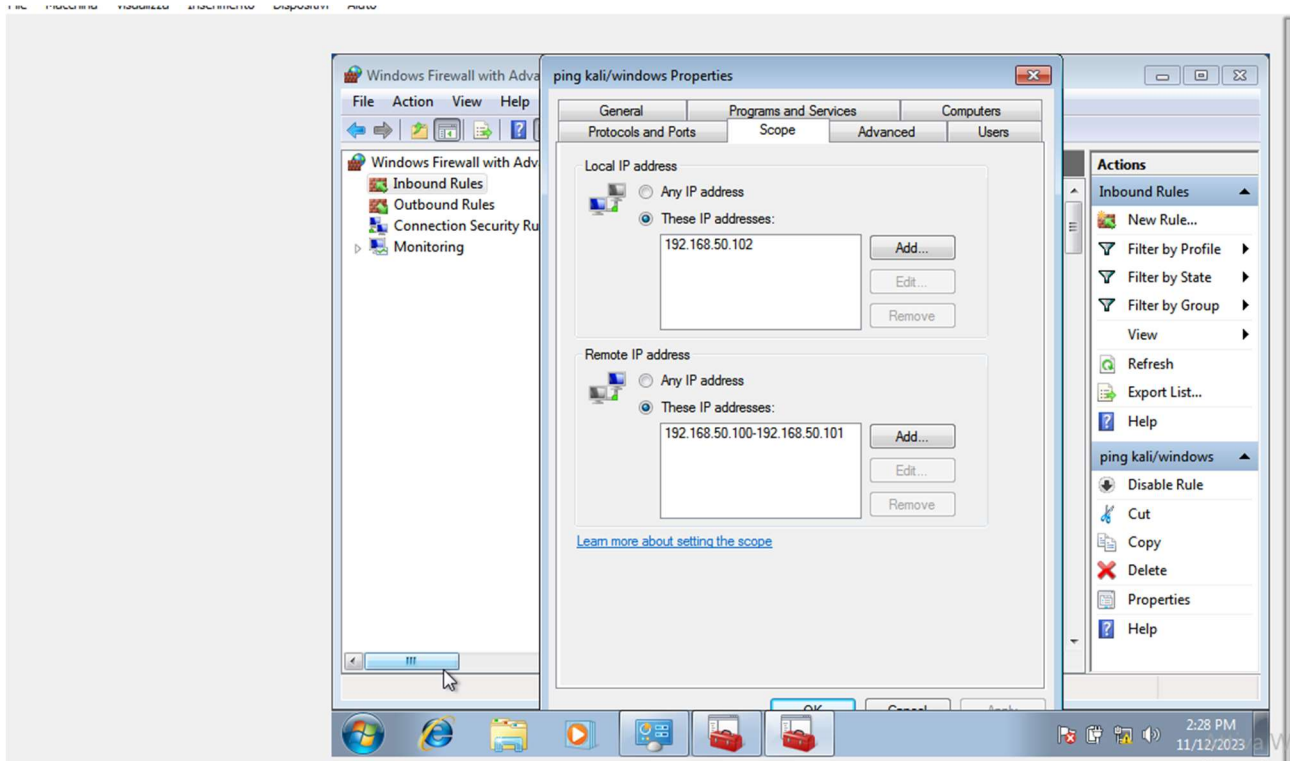
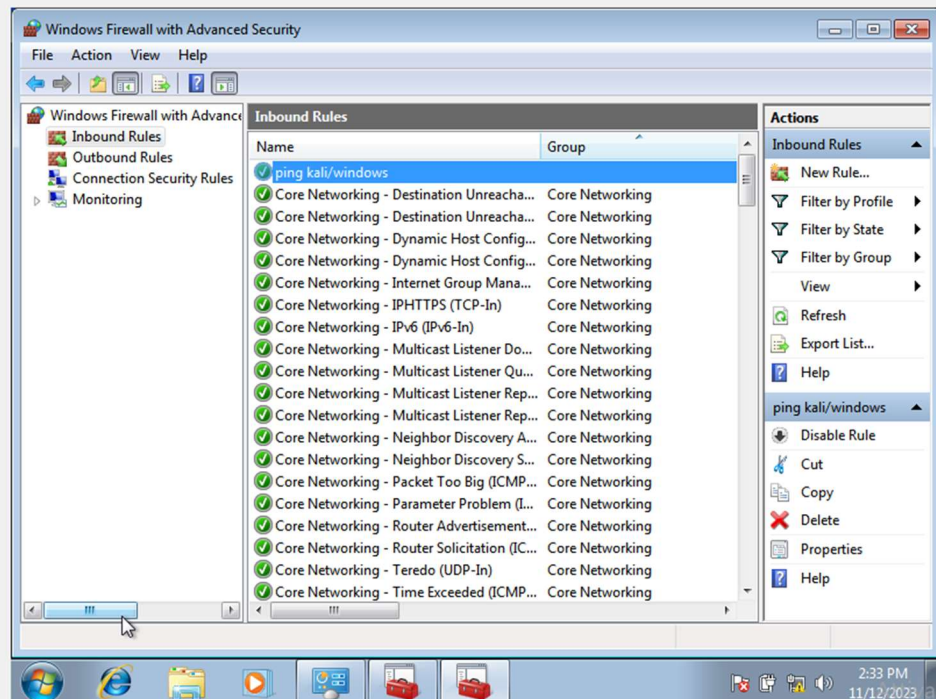


## PUNTO 1:

- Creazione nuova policy firewall per permettere il ping tra kali e windows 7.

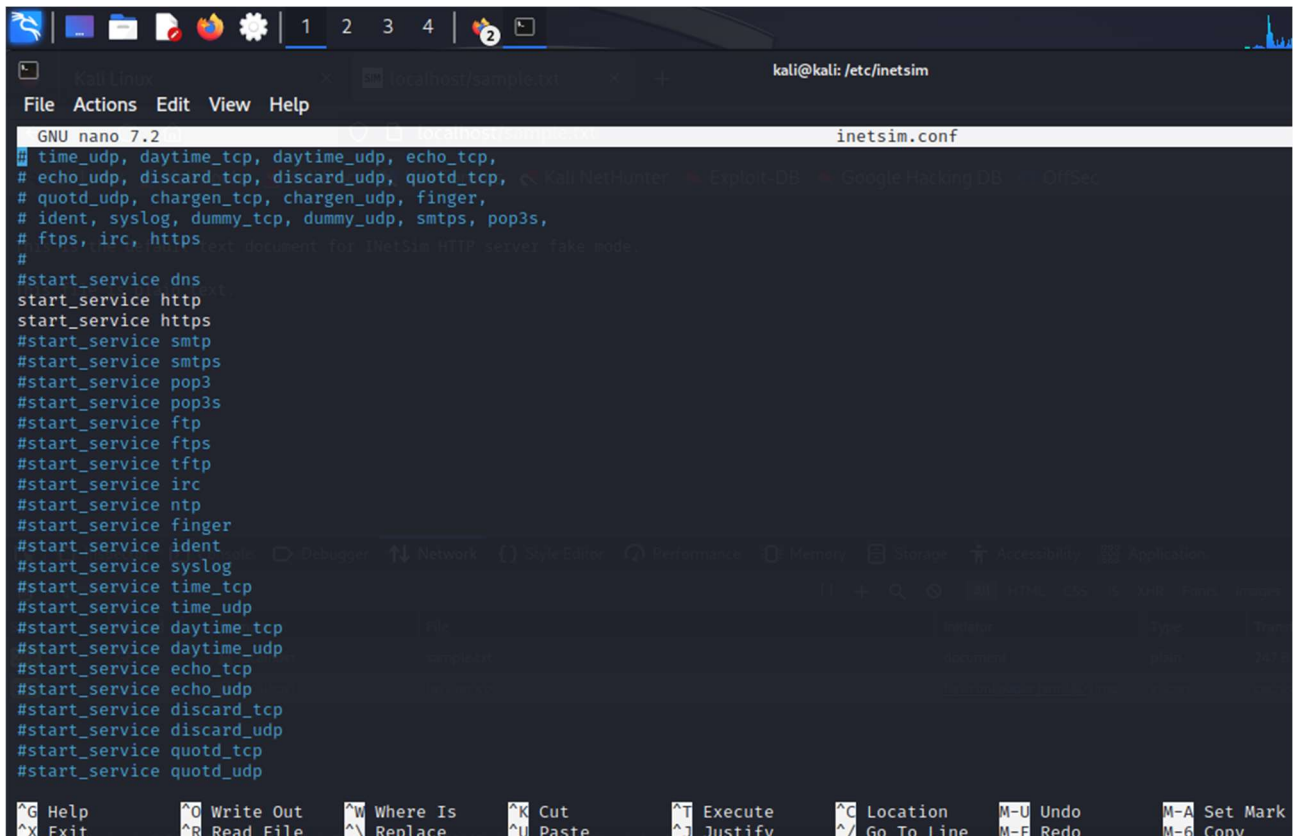




```
File Actions Edit View Help
(kali@kali)-[~]
$ ping 192.168.50.102
PING 192.168.50.102 (192.168.50.102) 56(84) bytes of data.
64 bytes from 192.168.50.102: icmp_seq=1 ttl=128 time=1.80 ms
64 bytes from 192.168.50.102: icmp_seq=2 ttl=128 time=0.478 ms
64 bytes from 192.168.50.102: icmp_seq=3 ttl=128 time=0.481 ms
64 bytes from 192.168.50.102: icmp_seq=4 ttl=128 time=0.748 ms
64 bytes from 192.168.50.102: icmp_seq=5 ttl=128 time=0.455 ms
64 bytes from 192.168.50.102: icmp_seq=6 ttl=128 time=0.840 ms
64 bytes from 192.168.50.102: icmp_seq=7 ttl=128 time=0.796 ms
64 bytes from 192.168.50.102: icmp_seq=8 ttl=128 time=0.478 ms
64 bytes from 192.168.50.102: icmp_seq=9 ttl=128 time=0.668 ms
64 bytes from 192.168.50.102: icmp_seq=10 ttl=128 time=0.929 ms
^C
— 192.168.50.102 ping statistics —
10 packets transmitted, 10 received, 0% packet loss, time 9187ms
rtt min/avg/max/mdev = 0.455/0.767/1.802/0.382 ms
(kali@kali)-[~]
$
```

## PUNTO 2:

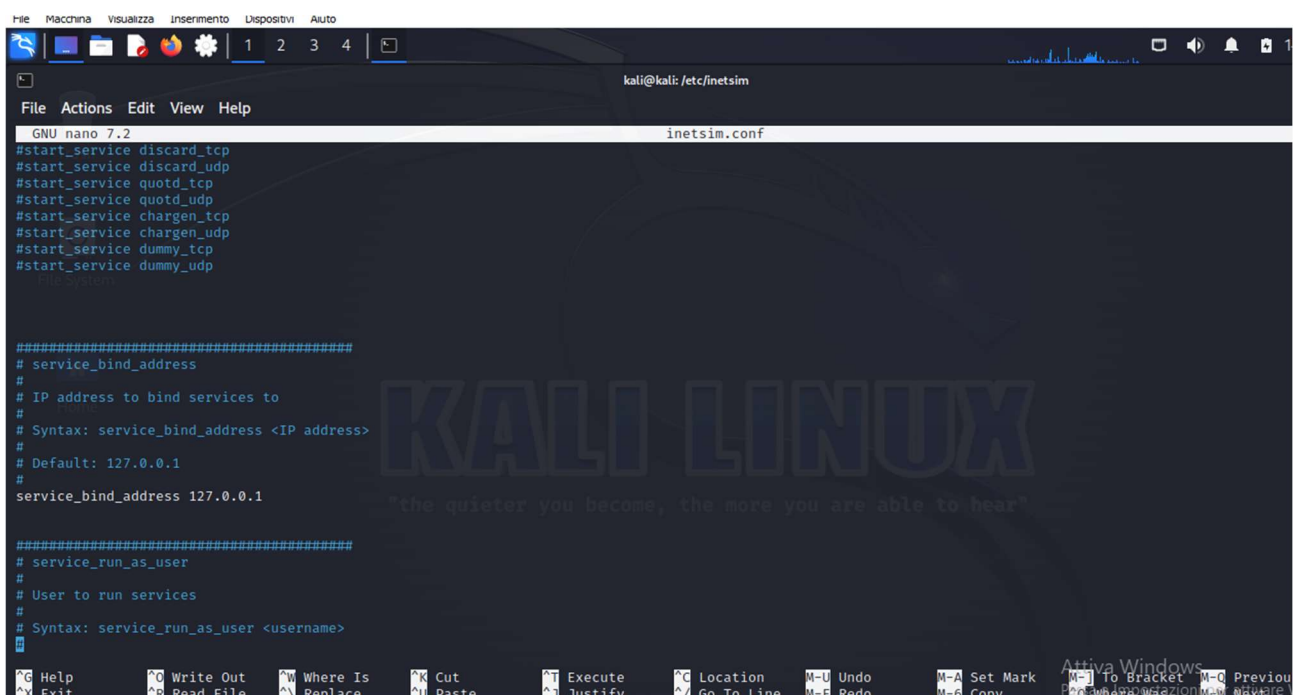
- Configurazione inetsim su kali
- Avvio simulazione inetsim
- Local host web e sample txt visibili



The screenshot shows a Kali Linux terminal window with the nano text editor open to the file `/etc/inetsim/inetsim.conf`. The terminal title bar indicates the user is `kali@kali` in the directory `/etc/inetsim`. The nano editor's status bar shows "GNU nano 7.2". The configuration file content is as follows:

```
#time_udp, daytime_tcp, daytime_udp, echo_tcp,
# echo_udp, discard_tcp, discard_udp, quotd_tcp,
# quotd_udp, chargen_tcp, chargen_udp, finger,
# ident, syslog, dummy_tcp, dummy_udp, smtps, pop3s,
# 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
#start_service ident
#start_service syslog
#start_service time_tcp
#start_service time_udp
#start_service daytime_tcp
#start_service daytime_udp
#start_service echo_tcp
#start_service echo_udp
#start_service discard_tcp
#start_service discard_udp
#start_service quotd_tcp
#start_service quotd_udp
```

The bottom of the terminal shows the nano editor's command shortcuts: `^G Help`, `^O Write Out`, `^W Where Is`, `^K Cut`, `^T Execute`, `^C Location`, `M-U Undo`, `M-A Set Mark`, `^X Exit`, `^R Read File`, `^N Replace`, `^U Paste`, `^J Justify`, `^_ Go To Line`, `M-E Redo`, `M-6 Copy`.



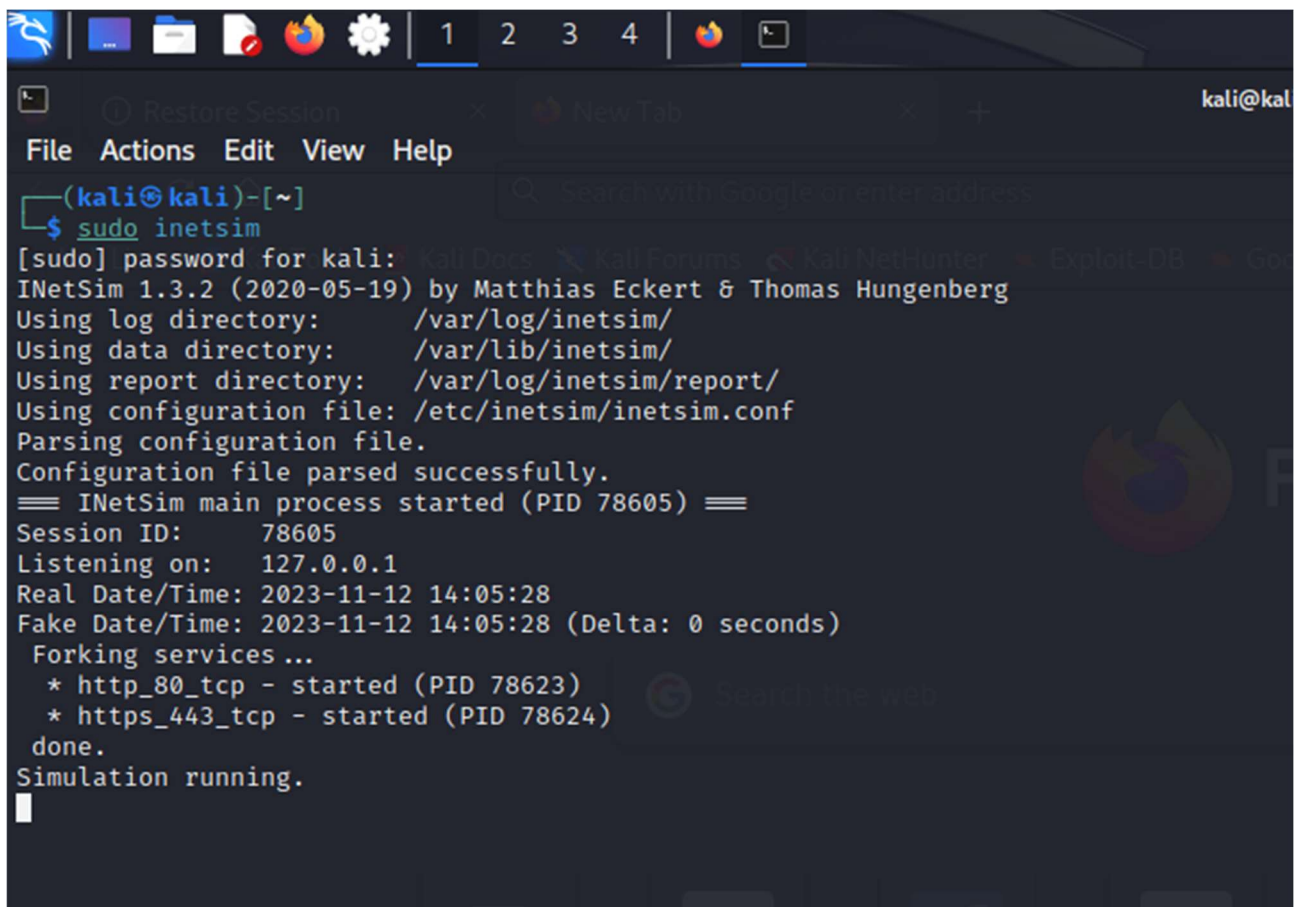
The screenshot shows the same Kali Linux terminal window with the nano text editor open to `/etc/inetsim/inetsim.conf`. The terminal title bar shows `kali@kali: /etc/inetsim`. The nano editor's status bar shows "GNU nano 7.2". The configuration file content is as follows:

```
#start_service discard_tcp
#start_service discard_udp
#start_service quotd_tcp
#start_service quotd_udp
#start_service chargen_tcp
#start_service chargen_udp
#start_service dummy_tcp
#start_service dummy_udp

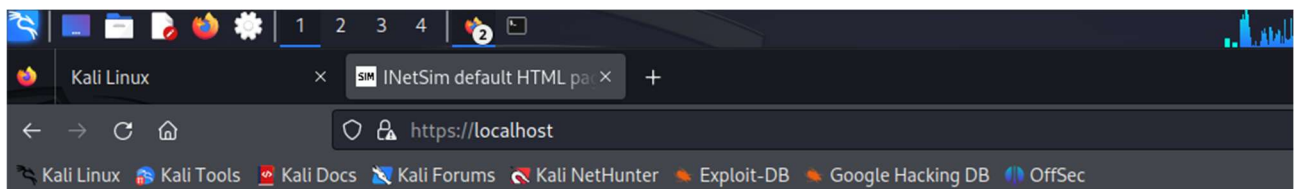
#####
# service_bind_address
#
# IP address to bind services to
# Syntax: service_bind_address <IP address>
#
# Default: 127.0.0.1
service_bind_address 127.0.0.1

#####
# service_run_as_user
#
# User to run services
# Syntax: service_run_as_user <username>
```

The bottom of the terminal shows the nano editor's command shortcuts: `^G Help`, `^O Write Out`, `^W Where Is`, `^K Cut`, `^T Execute`, `^C Location`, `M-U Undo`, `M-A Set Mark`, `^X Exit`, `^R Read File`, `^N Replace`, `^U Paste`, `^J Justify`, `^_ Go To Line`, `M-E Redo`, `M-6 Copy`. A faint "KALI LINUX" watermark is visible in the background.

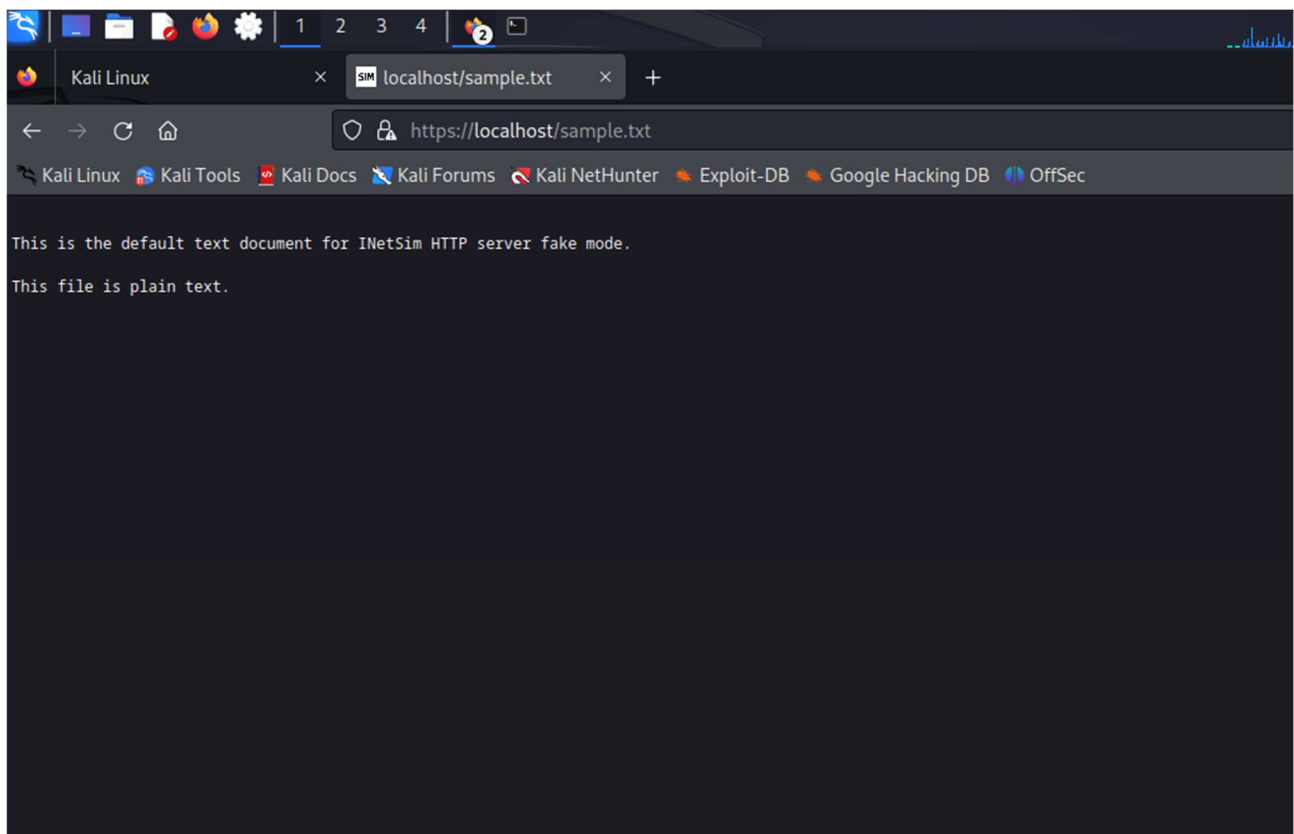


```
(kali@kali)-[~]
$ sudo inetsim
[sudo] password for kali:
INetSim 1.3.2 (2020-05-19) by Matthias Eckert & Thomas Hungenberg
Using log directory: /var/log/inetsim/
Using data directory: /var/lib/inetsim/
Using report directory: /var/log/inetsim/report/
Using configuration file: /etc/inetsim/inetsim.conf
Parsing configuration file.
Configuration file parsed successfully.
== INetSim main process started (PID 78605) ==
Session ID: 78605
Listening on: 127.0.0.1
Real Date/Time: 2023-11-12 14:05:28
Fake Date/Time: 2023-11-12 14:05:28 (Delta: 0 seconds)
Forking services ...
* http_80_tcp - started (PID 78623)
* https_443_tcp - started (PID 78624)
done.
Simulation running.
```



This is the default HTML page for INetSim HTTP server fake mode.

This file is an HTML document.



### PUNTO 3:

- Utilizzo Wireshark per intercettare il traffico di rete (Loopback)
- Prova con protocollo http: non cifrato, testo visibile
- Prova con protocollo https: cifrato, testo non visibile



Wireshark interface showing a packet capture on the interface 'Loopback: lo'. The filter is 'ip.addr == 127.0.0.1'. The packet list shows a sequence of packets including TCP SYN, ACK, and HTTP GET requests. The selected packet (No. 8) is an HTTP GET request for '/sample.txt'. The packet details pane shows the structure of the packet, including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	127.0.0.1	127.0.0.1	TCP	74	42262 → 80 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM TSval=240...
2	0.000014083	127.0.0.1	127.0.0.1	TCP	74	80 → 42262 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=65495 SACK_PER...
3	0.000028598	127.0.0.1	127.0.0.1	TCP	66	42262 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=24042916 TSecr=24...
4	1.257844180	127.0.0.1	127.0.0.1	HTTP	507	GET /sample.txt HTTP/1.1
5	1.257870400	127.0.0.1	127.0.0.1	TCP	66	80 → 42262 [ACK] Seq=1 Ack=442 Win=65152 Len=0 TSval=24044173 TSecr=...
6	1.477721310	127.0.0.1	127.0.0.1	TCP	216	80 → 42262 [PSH, ACK] Seq=1 Ack=442 Win=65536 Len=150 TSval=24044393...
7	1.477846853	127.0.0.1	127.0.0.1	TCP	66	42262 → 80 [ACK] Seq=442 Ack=151 Win=65408 Len=0 TSval=24044393 TSecr=...
8	1.477894621	127.0.0.1	127.0.0.1	HTTP	163	HTTP/1.1 200 OK (text/plain)
9	1.477905348	127.0.0.1	127.0.0.1	TCP	66	42262 → 80 [ACK] Seq=442 Ack=248 Win=65408 Len=0 TSval=24044393 TSecr=...
10	1.480177302	127.0.0.1	127.0.0.1	TCP	66	42262 → 80 [FIN, ACK] Seq=442 Ack=248 Win=65536 Len=0 TSval=24044390...
11	1.499478949	127.0.0.1	127.0.0.1	TCP	66	80 → 42262 [FIN, ACK] Seq=248 Ack=443 Win=65536 Len=0 TSval=24044415...

Frame 8: 163 bytes on wire (1304 bits), 163 bytes captured on interface 'Loopback: lo', 163 bytes from 127.0.0.1 to 127.0.0.1 on interface 'Loopback: lo'.  
Ethernet II, Src: 00:00:00:00:00:00 (00:00:00:00:00:00), Dst: 00:00:00:00:00:00 (00:00:00:00:00:00)  
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1  
Transmission Control Protocol, Src Port: 80, Dst Port: 42262  
[2 Reassembled TCP Segments (247 bytes): #6(150), #8(97)]  
Hypertext Transfer Protocol  
Line-based text data: text/plain (5 lines)  
This is the default text document for INetSim HTTP server fake mode. This file is plain text.

Wireshark interface showing a packet capture on the interface 'Loopback: lo'. The filter is 'ip.addr == 127.0.0.1'. The packet list shows a sequence of packets including TCP ACK, TLSv1.3 Client Hello, Change Cipher Spec, and Application Data. The selected packet (No. 6) is a TLSv1.3 Server Hello, Change Cipher Spec, Application Data, and Application Data. The packet details pane shows the structure of the packet, including Transmission Control Protocol, Transport Layer Security, and TLSv1.3 Record Layer. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
3	0.000039892	127.0.0.1	127.0.0.1	TCP	66	42636 → 443 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=25260291 TSecr=2...
4	0.0006686146	127.0.0.1	127.0.0.1	TLSv1	705	Client Hello
5	0.0006713532	127.0.0.1	127.0.0.1	TCP	66	443 → 42636 [ACK] Seq=1 Ack=640 Win=64896 Len=0 TSval=25260297 TSecr=...
6	0.433067388	127.0.0.1	127.0.0.1	TLSv1.3	1487	Server Hello, Change Cipher Spec, Application Data, Application Data...
7	0.433097641	127.0.0.1	127.0.0.1	TCP	66	42636 → 443 [ACK] Seq=640 Ack=1422 Win=64384 Len=0 TSval=25260724 TS...
8	0.448622308	127.0.0.1	127.0.0.1	TLSv1.3	146	Change Cipher Spec, Application Data
9	0.448652252	127.0.0.1	127.0.0.1	TCP	66	443 → 42636 [ACK] Seq=1422 Ack=720 Win=65536 Len=0 TSval=25260739 TS...
10	0.449032576	127.0.0.1	127.0.0.1	TLSv1.3	529	Application Data
11	0.449043407	127.0.0.1	127.0.0.1	TCP	66	443 → 42636 [ACK] Seq=1422 Ack=1183 Win=65152 Len=0 TSval=25260740 T...
12	0.449449292	127.0.0.1	127.0.0.1	TLSv1.3	321	Application Data
13	0.492623784	127.0.0.1	127.0.0.1	TCP	66	42636 → 443 [ACK] Seq=1183 Ack=1677 Win=65536 Len=0 TSval=25260783 T...

Transmission Control Protocol, Src Port: 443, Dst Port: 42636  
Transport Layer Security  
TLSv1.3 Record Layer: Handshake Protocol: Server Hello  
TLSv1.3 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec  
TLSv1.3 Record Layer: Application Data Protocol: Hypertext Transfer Protocol  
Version: TLS 1.2 (0x0303)  
Length: 23  
Encrypted Application Data: 8b769f5da520b9b4f441a6  
[Application Data Protocol: Hypertext Transfer Protocol]  
TLSv1.3 Record Layer: Application Data Protocol: Hypertext Transfer Protocol  
TLSv1.3 Record Layer: Application Data Protocol: Hypertext Transfer Protocol  
TLSv1.3 Record Layer: Application Data Protocol: Hypertext Transfer Protocol