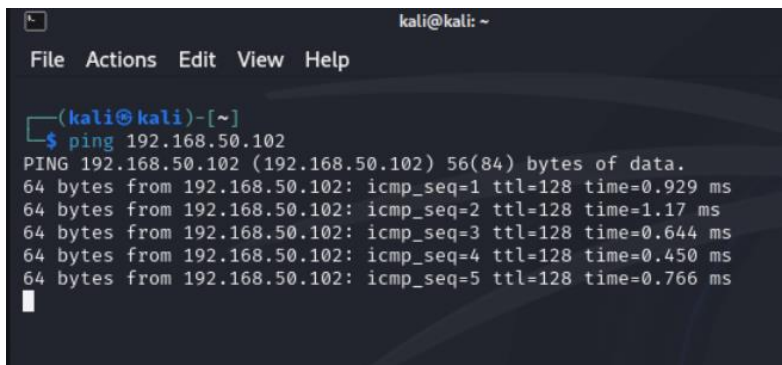


## Abilitazione Firewall e abilitazione policy per ping win 10



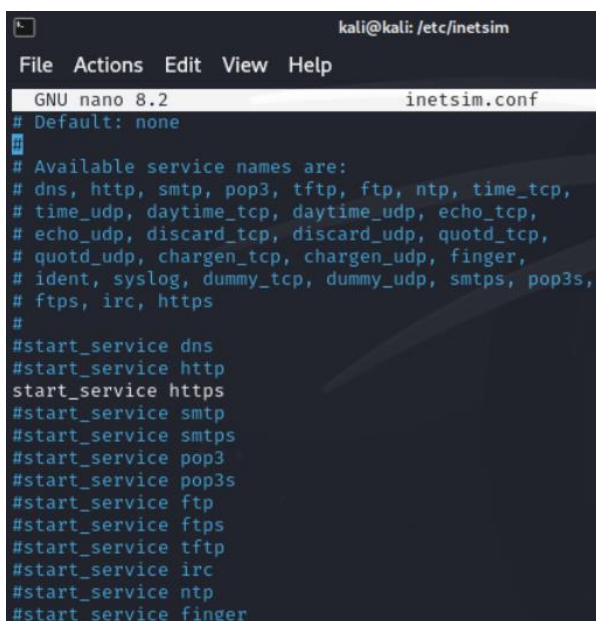
Nome	Gruppo	Profilo	Abilitata
ping		Tutti	Si

## Test del ping da Kali verso win 10



```
kali@kali: ~  
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=0.929 ms  
64 bytes from 192.168.50.102: icmp_seq=2 ttl=128 time=1.17 ms  
64 bytes from 192.168.50.102: icmp_seq=3 ttl=128 time=0.644 ms  
64 bytes from 192.168.50.102: icmp_seq=4 ttl=128 time=0.450 ms  
64 bytes from 192.168.50.102: icmp_seq=5 ttl=128 time=0.766 ms
```

## Configurazione inetsim



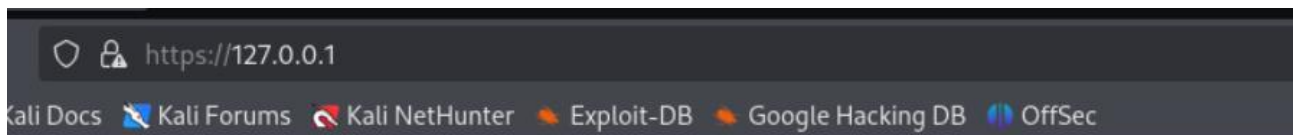
```
kali@kali: /etc/inetsim  
File Actions Edit View Help  
GNU nano 8.2 inetsim.conf  
# Default: none  
#  
# Available service names are:  
# dns, http, smtp, pop3, tftp, ftp, ntp, time_tcp,  
# time_udp, daytime_tcp, daytime_udp, echo_tcp,  
# echo_udp, discard_tcp, discard_udp, quotd_tcp,  
# quotd_udp, 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
```

## Attivazione servizio inetsim

```
kali@kali: /etc/inetsim
File Actions Edit View Help

(kali@kali)-[/etc/inetsim]
$ sudo inetsim
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 6979) ==
Session ID: 6979
Listening on: 127.0.0.1
Real Date/Time: 2024-11-25 12:41:25
Fake Date/Time: 2024-11-25 12:41:25 (Delta: 0 seconds)
Forking services ...
* https_443_tcp - started (PID 6989)
done.
Simulation running.
```

## Test del servizio fittizio in https



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

This file is an HTML document.

## Sniffer utilizzando il programma wireshark

The image shows a Wireshark network traffic capture window. The title bar indicates "Capturing from Loopback: lo". The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains various icons for file operations, capture control, and analysis. The display filter bar shows "Apply a display filter ... <Ctrl-/>".

The packet list pane displays the following packets:

No.	Time	Source	Destination	Protocol	Length	Info
214	20.999738121	127.0.0.1	127.0.0.1	TLSv1.3	321	Application Data
215	20.999748926	127.0.0.1	127.0.0.1	TCP	66	50846 → 443 [ACK] Seq=720
216	21.004160735	127.0.0.1	127.0.0.1	TCP	66	50856 → 443 [ACK] Seq=1221
217	21.008966019	127.0.0.1	127.0.0.1	TLSv1.3	239	Application Data
218	21.010600086	127.0.0.1	127.0.0.1	TCP	66	50856 → 443 [ACK] Seq=1221
219	21.010929406	127.0.0.1	127.0.0.1	TLSv1.3	346	Application Data
220	21.010938693	127.0.0.1	127.0.0.1	TCP	66	50856 → 443 [ACK] Seq=1221
221	21.011136364	127.0.0.1	127.0.0.1	TLSv1.3	90	Application Data
222	21.011148976	127.0.0.1	127.0.0.1	TCP	66	50856 → 443 [FIN, ACK] Seq=
223	21.015948525	127.0.0.1	127.0.0.1	TCP	66	[TCP Retransmission] 50856
224	21.016354348	127.0.0.1	127.0.0.1	TCP	78	443 → 50856 [ACK] Seq=2385
225	21.025313384	127.0.0.1	127.0.0.1	TLSv1.3	90	Application Data
226	21.025324517	127.0.0.1	127.0.0.1	TCP	54	50856 → 443 [RST] Seq=1246
227	25.943647728	127.0.0.1	127.0.0.1	TLSv1.3	90	Application Data
228	25.943747903	127.0.0.1	127.0.0.1	TCP	66	50846 → 443 [FIN, ACK] Seq=
229	25.948096517	127.0.0.1	127.0.0.1	TLSv1.3	90	Application Data
230	25.948116627	127.0.0.1	127.0.0.1	TCP	54	50846 → 443 [RST] Seq=745

The packet details pane for packet 226 shows the following information:

- [Conversation completeness: Complete, WITH\_DATA]
- [TCP Segment Len: 0]
- Sequence Number: 1221 (relative sequence num)
- Sequence Number (raw): 1769132051
- [Next Sequence Number: 1221 (relative sequen
- Acknowledgment Number: 2385 (relative ack nu
- Acknowledgment number (raw): 525942092
- 1000 .... = Header Length: 32 bytes (8)
- Flags: 0x010 (ACK)
- Window: 623
- [Calculated window size: 79744]
- [Window size scaling factor: 128]
- Checksum: 0xfe28 [unverified]
- [Checksum Status: Unverified]
- Urgent Pointer: 0
- Options: (12 bytes), No-Operation (NOP), No-Ope
- [Timestamps]
- [SEQ/ACK analysis]

The packet bytes pane shows the raw data of the TCP segment:

```
0000 00 00 00 00 00 00 00 00 00 00 00 08 00 45
0010 00 34 59 f3 40 00 40 06 e2 ce 7f 00 00 01 7f
0020 00 01 c6 a8 01 bb 69 72 d0 13 1f 59 3d 4c 80
0030 02 6f fe 28 00 00 01 01 08 0a e0 04 e3 9d e0
0040 e3 9d
```