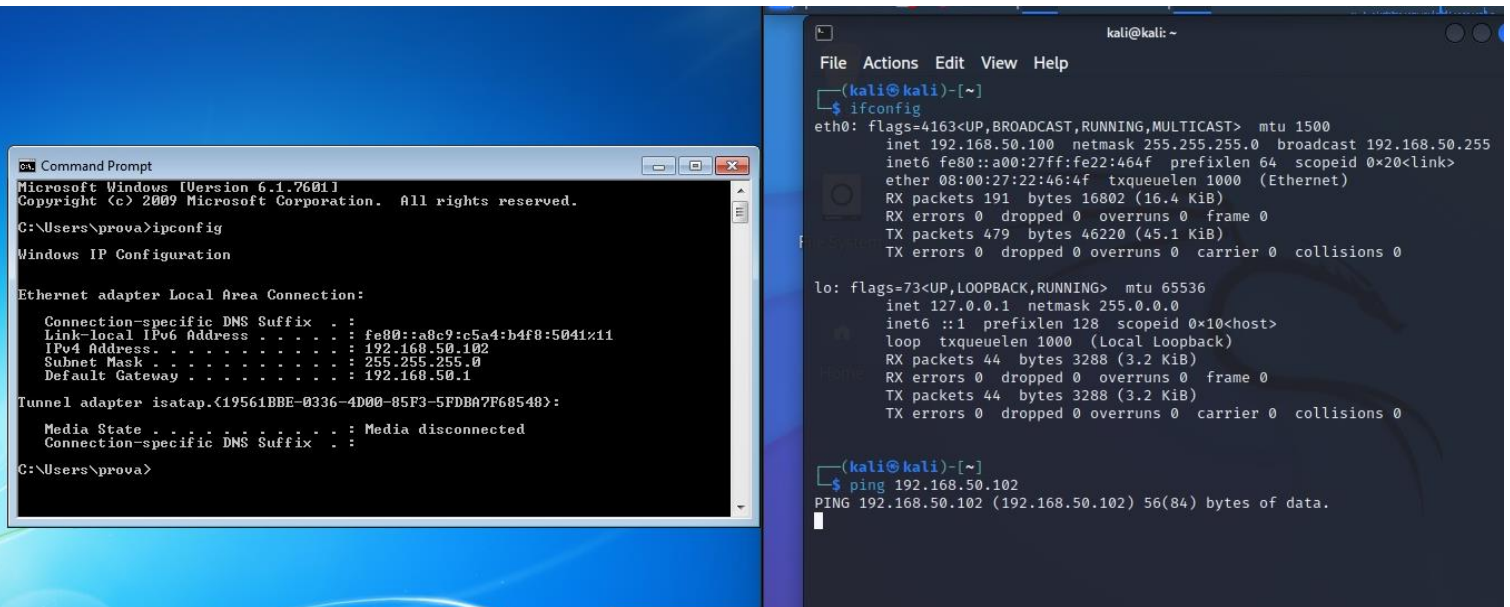
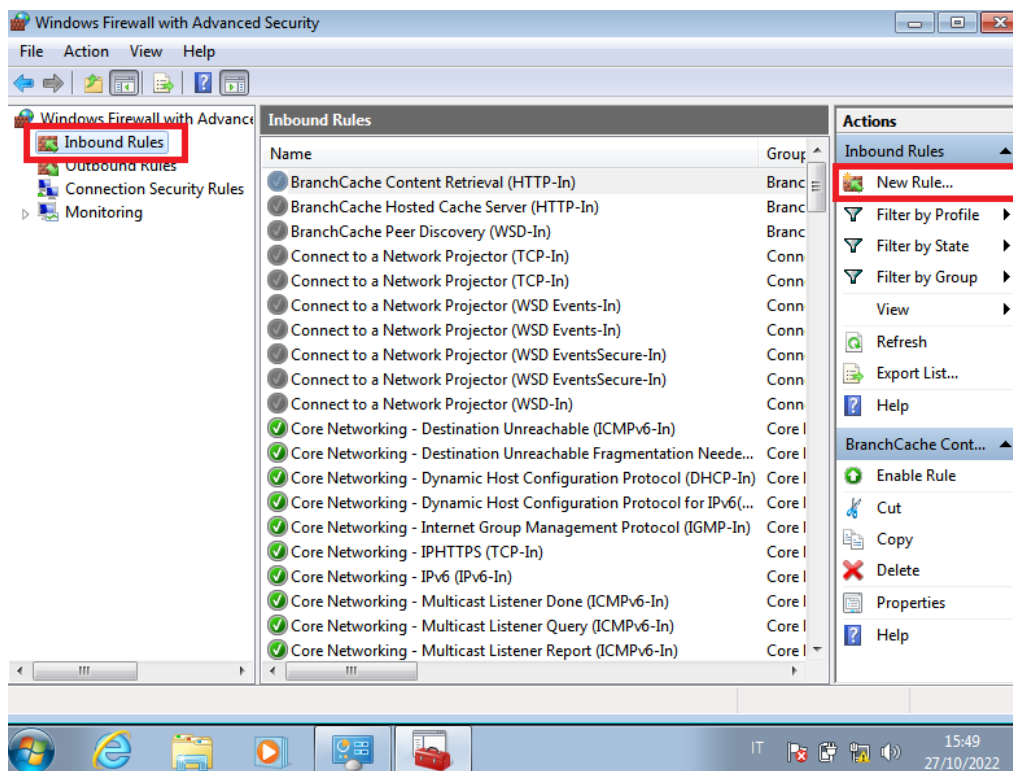


# Configurazione Firewall di Windows, Packet capture con Wireshark e InetSim

## Configurazione Firewall Windows:



Qui possiamo notare come non ci sia risposta da parte di Kali alla richiesta del ping da parte di Windows, per ovviare a questo problema bisogna entrare in **Windows Firewall -> Advanced Settings**, qui ci troveremo nell'immagine sottostante: **Inbound Rules -> New Rules**



Per proseguire con **Custom -> All Programs ->** in **Protocol Type** selezioneremo **ICMPv4** -> Inserendo nella schermata successiva l' Ip di Windows e di Kali

New Inbound Rule Wizard

**Protocol and Ports**  
Specify the protocols and ports to which this rule applies.

**Steps:**

- Rule Type
- Program
- Protocol and Ports
- Scope
- Action
- Profile
- Name

To which ports and protocols does this rule apply?

Protocol type: ICMPv4  
Protocol number: 1  
Local port: All Ports  
Remote port: All Ports  
Example: 80, 443, 5000-5010  
Internet Control Message Protocol (ICMP) settings: Customize...

[Learn more about protocol and ports](#)

< Back Next > Cancel

**Which local IP addresses does this rule apply to?**

☐ Any IP address  
☒ These IP addresses:

192.168.50.102  
192.168.50.100

Add... Edit... Remove

Customize the interface types to which this rule applies: Customize...

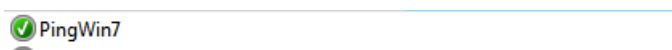
**Which remote IP addresses does this rule apply to?**

☐ Any IP address  
☒ These IP addresses:

192.168.50.102  
192.168.50.100

Add... Edit... Remove

Proseguendo fino alla fine scegliendo poi il nome della regola



Effettuata la modifica, riprovando la richiesta di Ping, ci sarà la risposta da parte di Windows

```
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=1.10 ms  
64 bytes from 192.168.50.102: icmp_seq=2 ttl=128 time=0.496 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=0.797 ms  
64 bytes from 192.168.50.102: icmp_seq=5 ttl=128 time=0.813 ms  
^Z  
zsh: suspended ping 192.168.50.102  
  
(kali@kali)-[~]  
$
```

Ora passeremo alla creazione di InetSim, dove ci basterà aprire la console di Kali con **Sudo Inetsim**

```
kali@kali: ~  
File Actions Edit View Help  
--(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 11545) ==  
Session ID: 11545  
Listening on: 127.0.0.1  
Real Date/Time: 2022-10-27 08:51:01  
Fake Date/Time: 2022-10-27 08:51:01 (Delta: 0 seconds)  
Forking services ...  
* dns_53_tcp_udp - started (PID 11547)  
* pop3_110_tcp - started (PID 11552)  
* ftp_21_tcp - started (PID 11554)  
* pop3s_995_tcp - started (PID 11553)  
* irc_6667_tcp - started (PID 11557)  
* ntp_123_udp - started (PID 11558)  
* finger_79_tcp - started (PID 11559)  
* time_37_tcp - started (PID 11562)  
* syslog_514_udp - started (PID 11561)  
* daytime_13_tcp - started (PID 11564)  
* echo_7_tcp - started (PID 11566)  
* smtps_465_tcp - started (PID 11551)  
* discard_9_tcp - started (PID 11568)  
* time_37_udp - started (PID 11563)  
* quotd_17_tcp - started (PID 11570)  
* tftp_69_udp - started (PID 11556)  
* chargen_19_udp - started (PID 11573)  
* daytime_13_udp - started (PID 11565)  
* dummy_1_udp - started (PID 11575)  
* echo_7_udp - started (PID 11567)  
* discard_9_udp - started (PID 11569)  
* http_80_tcp - started (PID 11548)  
* quotd_17_udp - started (PID 11571)  
* chargen_19_tcp - started (PID 11572)  
* dummy_1_tcp - started (PID 11574)  
* https_443_tcp - started (PID 11549)  
* ident_113_tcp - started (PID 11560)  
* ftps_990_tcp - started (PID 11555)  
* smtp_25_tcp - started (PID 11550)  
done.  
Simulation running.
```

Dove verrà creata la nostra Simulazione dei servizi Internet ( 127.0.0.1 ) e aprendo **Wireshark**, avviandolo, si potranno vedere i “Packet Sniffet”, ovvero la possibilità di analizzare i vari dati catturati nella rete.

The image shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for file operations, capture control, and analysis. The main display area is divided into three panes:

- Packet List Pane:** Displays a list of captured packets with columns for No., Time, Source, Destination, Protocol, and Length. The first few packets are ICMP 'Destination unreachable' messages. A packet at time 34.9.221157576 is selected, showing a source of 192.168.50.100 and destination of 127.0.0.1.
- Packet Details Pane:** Provides a hierarchical view of the selected packet's structure. For the selected ARP packet, it shows 'Ethernet II', 'Internet Protocol Version 4', and 'Address Resolution Protocol (request)'. The selected packet is an ARP request from 192.168.50.100 to 127.0.0.1.
- Packet Bytes Pane:** Shows the raw data of the selected packet in hexadecimal and ASCII. The first few bytes are '0000 00 04 00 01 00 06 00 00', which correspond to the Ethernet II header.

