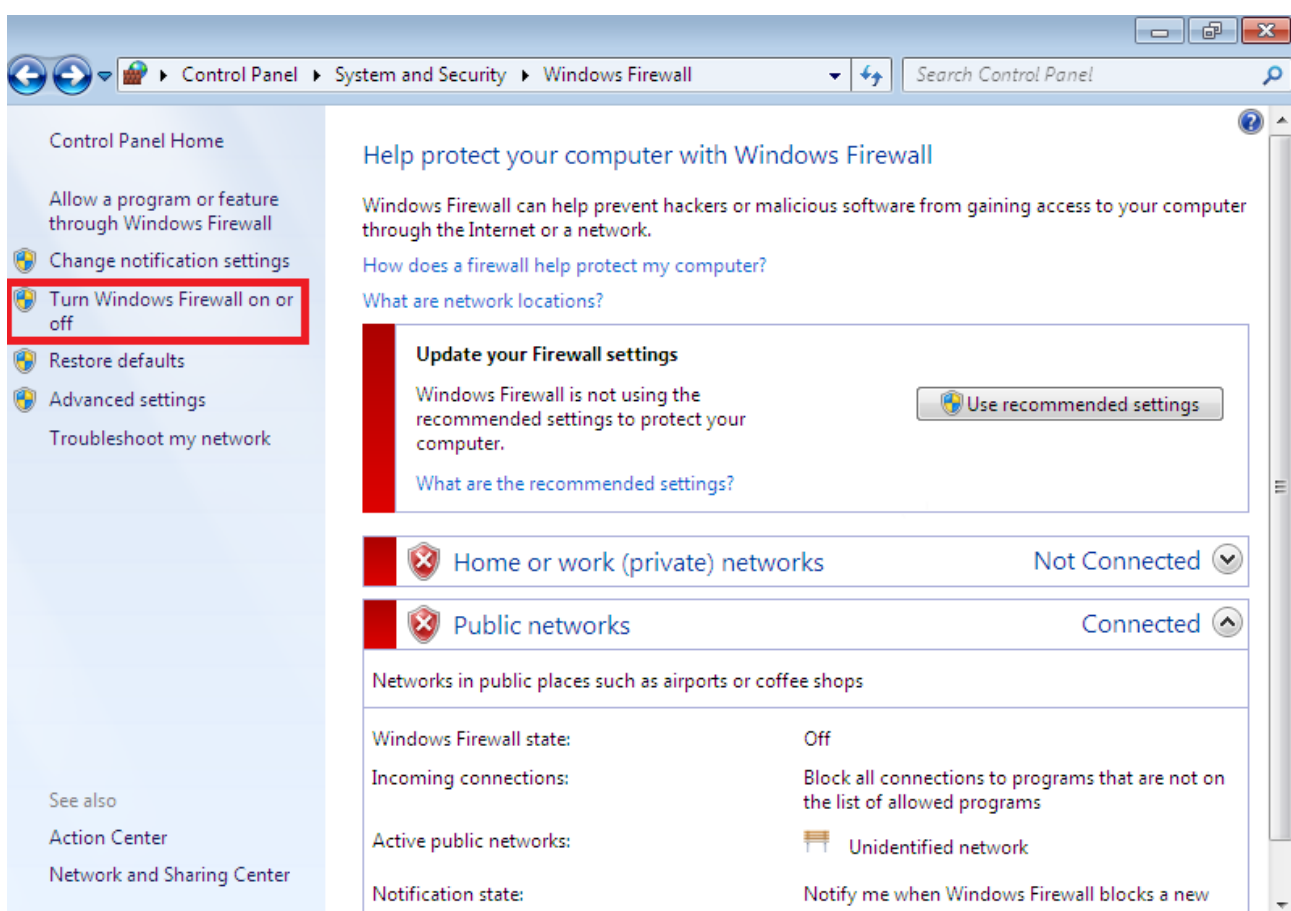


1. CONFIGURAZIONE DI UNA POLICY SU FIREWALL IN WINDOWS 7
2. SIMULAZIONE DI SERVIZI DI RETE CON INETSIM
3. CATTURA DI PACCHETTI CON WIRESHARK

## 1. Configurazione di una policy su firewall in Windows 7

### 1.1 Attivazione di Windows Firewall



### Customize settings for each type of network

You can modify the firewall settings for each type of network location that you use.

What are network locations?

#### Home or work (private) network location settings

- ☒ Turn on Windows Firewall
  - ☐ Block all incoming connections, including those in the list of allowed programs
  - ☒ Notify me when Windows Firewall blocks a new program

☐ Turn off Windows Firewall (not recommended)

#### Public network location settings

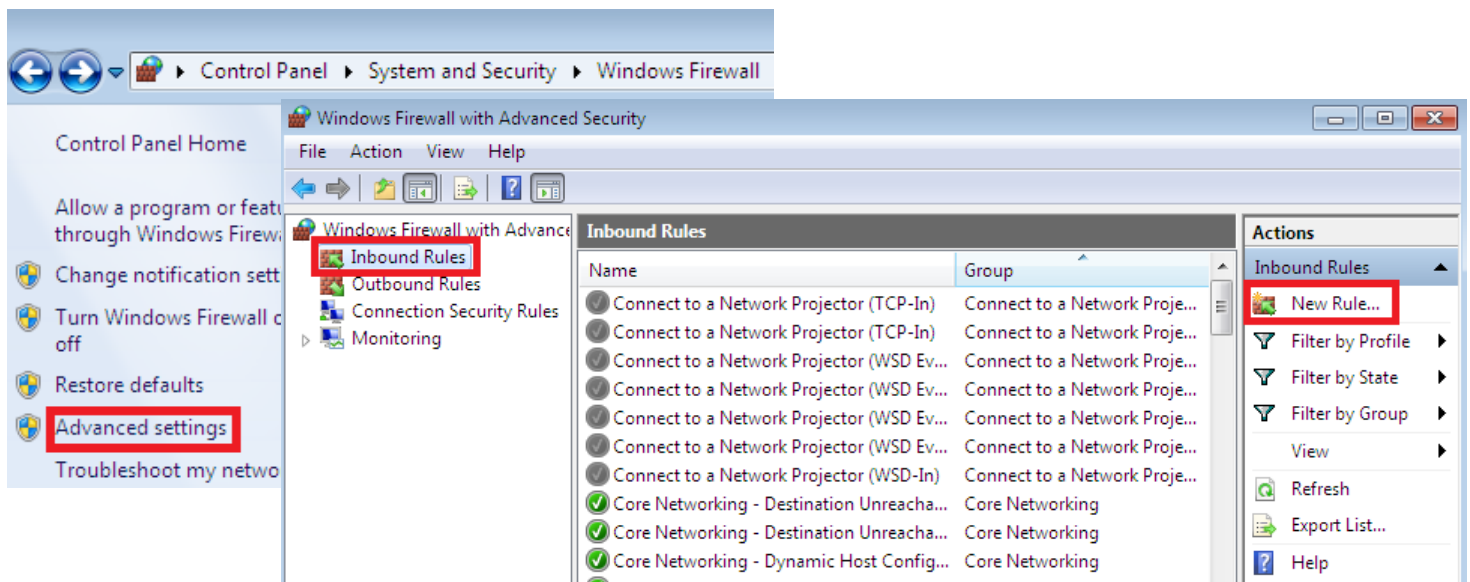
- ☒ Turn on Windows Firewall
  - ☐ Block all incoming connections, including those in the list of allowed programs
  - ☒ Notify me when Windows Firewall blocks a new program

☐ Turn off Windows Firewall (not recommended)

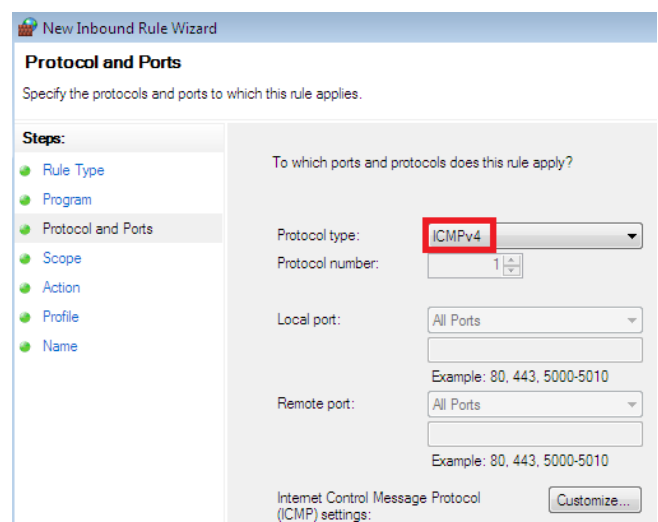
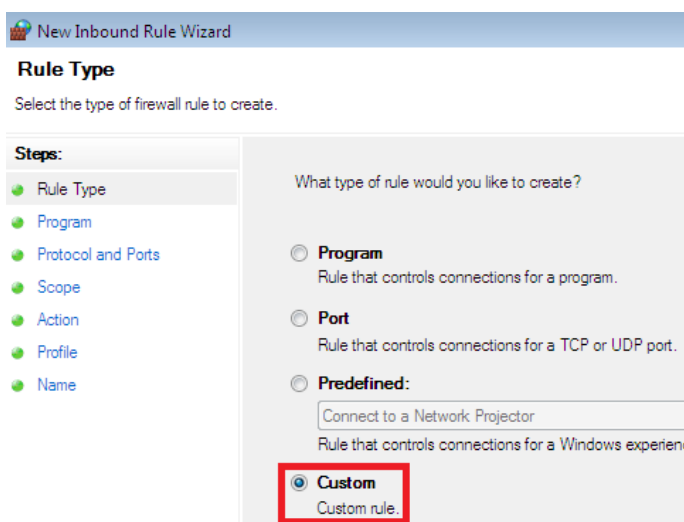
A questo punto si rende **necessaria** la configurazione di una policy per permettere la comunicazione tra Kali Linux e Windows 7, in quanto in questa fase la comunicazione tra le due macchine non può ancora avvenire (come mostrato in figura):

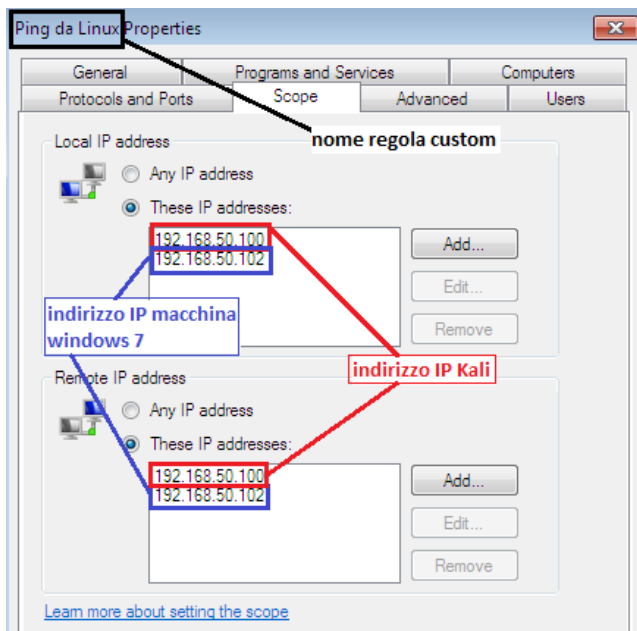
```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ ping 192.168.50.102  
PING 192.168.50.102 (192.168.50.102) 56(84) bytes of data.  
[...]
```

## 1.2 Creazione di una policy su Windows Firewall per consentire il ping da Kali Linux



Definizione di una regola custom per abilitare il protocollo ICMPv4 e permettere, quindi, la comunicazione tra Kali Linux (IP 192.168.50.100) e Windows 7 (IP 192.168.50.102).





Test ping positivo da Kali Linux:

```
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=5.69 ms
64 bytes from 192.168.50.102: icmp_seq=2 ttl=128 time=0.556 ms
64 bytes from 192.168.50.102: icmp_seq=3 ttl=128 time=0.484 ms
64 bytes from 192.168.50.102: icmp_seq=4 ttl=128 time=0.740 ms
64 bytes from 192.168.50.102: icmp_seq=5 ttl=128 time=0.510 ms
^Z
zsh: suspended ping 192.168.50.102
(kali@kali)-[~]
$
```

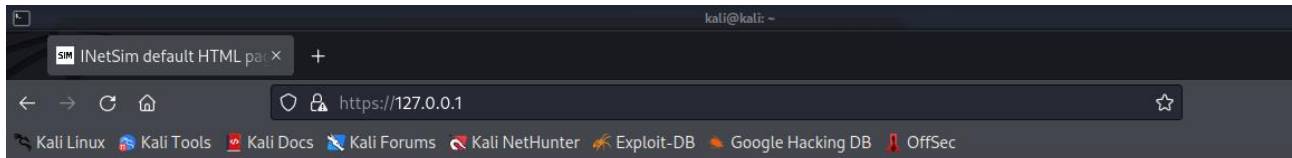
## 2. Simulazione di servizi di rete con InetSim

Avviamo il servizio INetSim su Kali e individuiamo l'indirizzo IP del server di rete:

```
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
Main logfile '/var/log/inetsim/main.log' does not exist. Trying to create it.
..
Main logfile '/var/log/inetsim/main.log' successfully created.
Sub logfile '/var/log/inetsim/service.log' does not exist. Trying to create i
t...
Sub logfile '/var/log/inetsim/service.log' successfully created.
Debug logfile '/var/log/inetsim/debug.log' does not exist. Trying to create i
t...
Debug logfile '/var/log/inetsim/debug.log' successfully created.
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 3271) ==
Session ID: 3271
Listening on: 127.0.0.1
Real Date/Time: 2022-10-27 13:39:11
Fake Date/Time: 2022-10-27 13:39:11 (Delta: 0 seconds)
Forking services...
* dns_53_tcp_udp - started (PID 3281)
* time_37_tcp - started (PID 3296)
* irc_6667_tcp - started (PID 3291)
* ntp_123_udp - started (PID 3292)
* ident_113_tcp - started (PID 3294)
* syslog_514_udp - started (PID 3295)
* daytime_13_udp - started (PID 3299)
* daytime_13_tcp - started (PID 3298)
```

### 3. Cattura di pacchetti con Wireshark

A questo punto avviamo la cattura dei pacchetti con Wireshark, visitando da browser l'indirizzo IP del server INetSim 127.0.0.1



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

This file is an HTML document.

