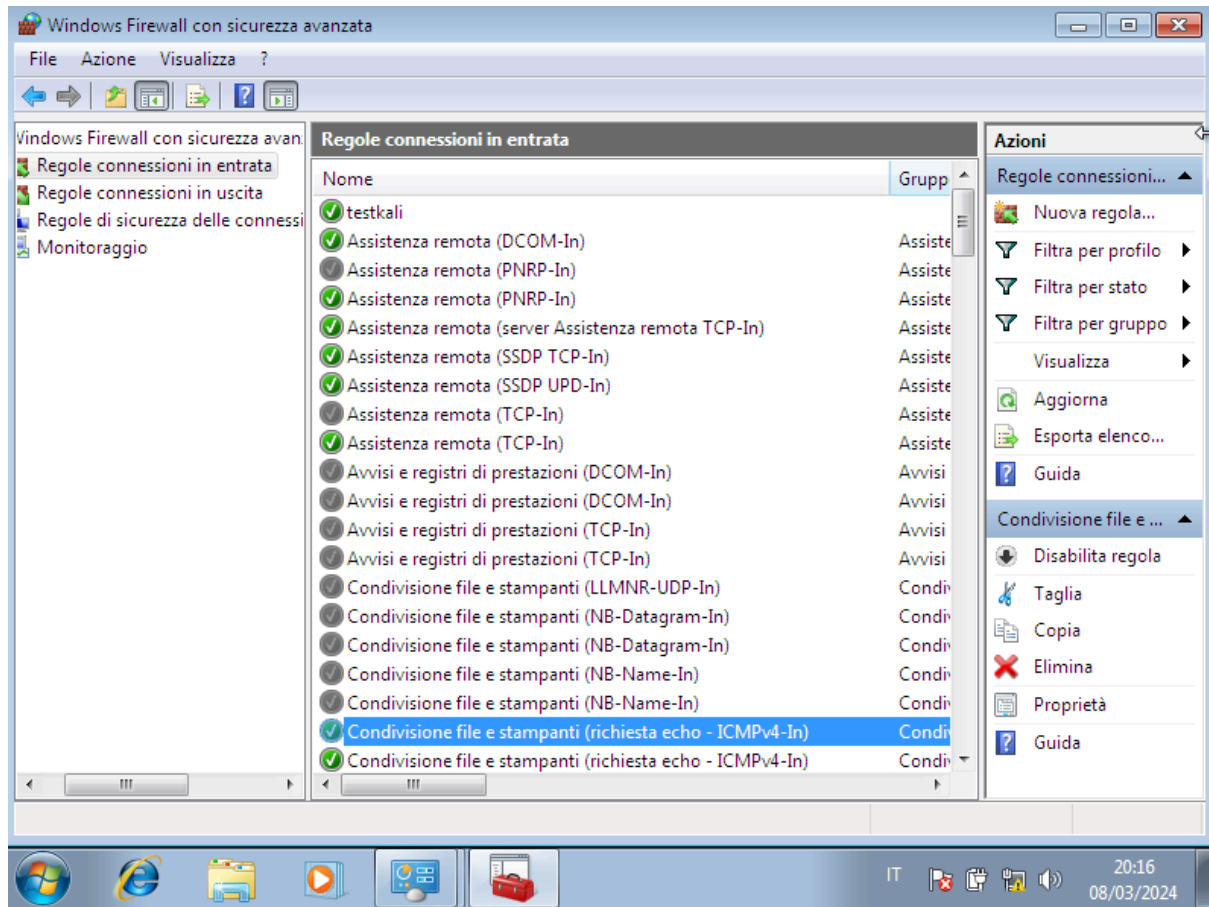


ES1: Configurare policy per permettere il ping da macchine Linux a macchina Windows 7 nel nostro laboratorio (Windows Firewall)



```
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=3.53 ms  
64 bytes from 192.168.50.102: icmp_seq=2 ttl=128 time=0.699 ms  
64 bytes from 192.168.50.102: icmp_seq=3 ttl=128 time=0.567 ms  
64 bytes from 192.168.50.102: icmp_seq=4 ttl=128 time=0.876 ms  
64 bytes from 192.168.50.102: icmp_seq=5 ttl=128 time=2.05 ms  
64 bytes from 192.168.50.102: icmp_seq=6 ttl=128 time=1.34 ms  
64 bytes from 192.168.50.102: icmp_seq=7 ttl=128 time=0.909 ms  
64 bytes from 192.168.50.102: icmp_seq=8 ttl=128 time=1.02 ms  
^C  
— 192.168.50.102 ping statistics —  
8 packets transmitted, 8 received, 0% packet loss, time 7052ms  
rtt min/avg/max/mdev = 0.567/1.373/3.525/0.920 ms  
(kali@kali)-[~]  
$
```

ES:

Utilizzo dell'utility InetSim per l'emulazione di servizi Internet

```
root@kali: ~  
File Actions Edit View Help  
(root@kali)-[~]  
# 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 21161) ==  
Session ID: 21161  
Listening on: 127.0.0.1  
Real Date/Time: 2024-03-08 14:37:42  
Fake Date/Time: 2024-03-08 14:37:42 (Delta: 0 seconds)  
Forking services ...  
* dns_53_tcp_udp - started (PID 21163)  
print() on closed filehandle MLOG at /usr/share/perl5/Net/DNS/Nameserver.pm line 399.  
print() on closed filehandle MLOG at /usr/share/perl5/Net/DNS/Nameserver.pm line 399.  
* https_443_tcp - started (PID 21165)  
* tftp_69_udp - started (PID 21174)  
* ident_113_tcp - started (PID 21182)  
* syslog_514_udp - started (PID 21187)  
* daytime_13_udp - started (PID 21191)  
* time_37_udp - started (PID 21189)  
* ftps_990_tcp - started (PID 21173)
```

Cattura di pacchetti con Wireshark

