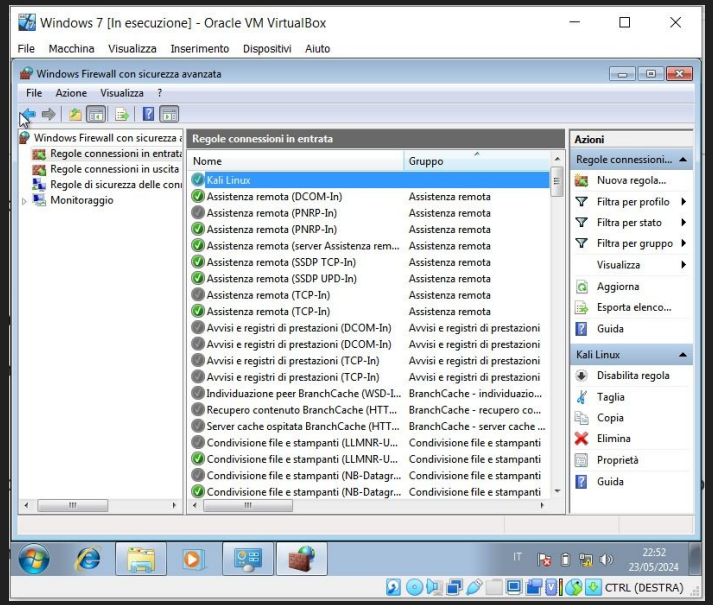
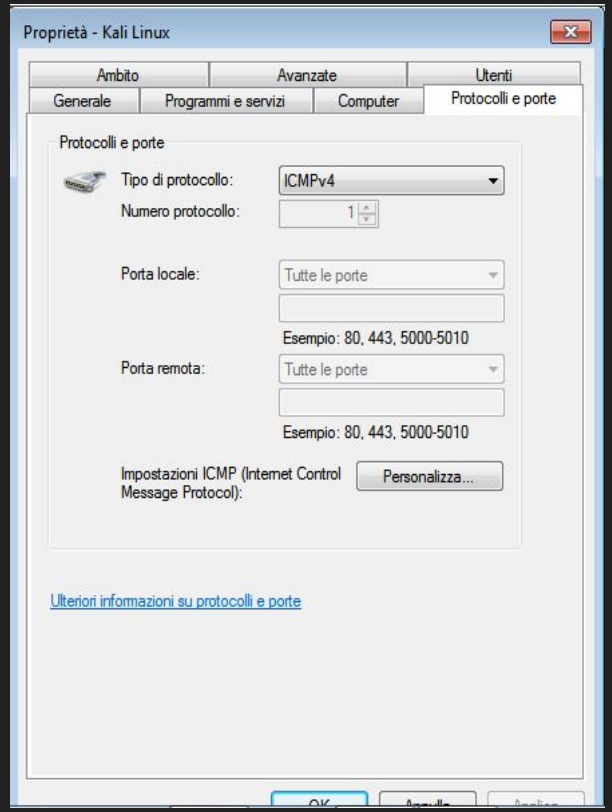
# W3D4 - Pratica

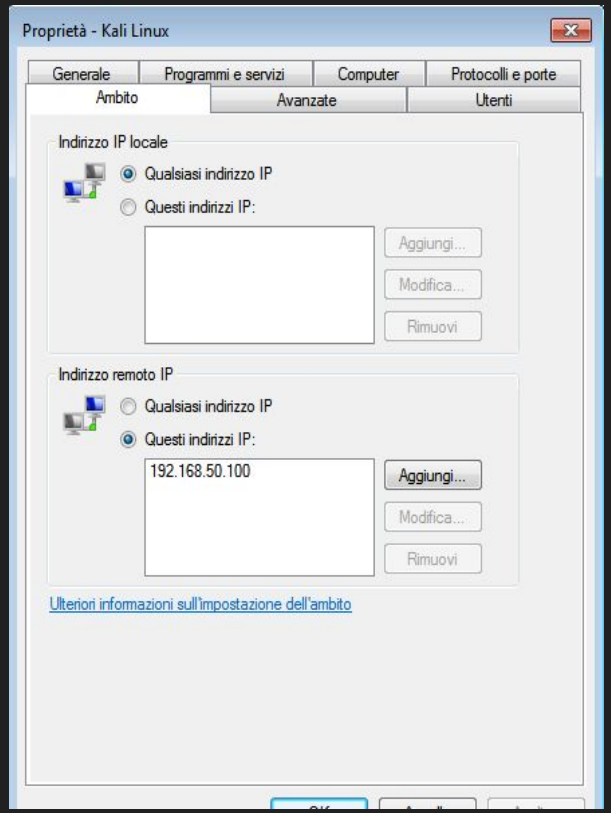
Configurazione regola Windows Firewall
Utilizzo InetSim
Cattura pacchetti con Wireshark

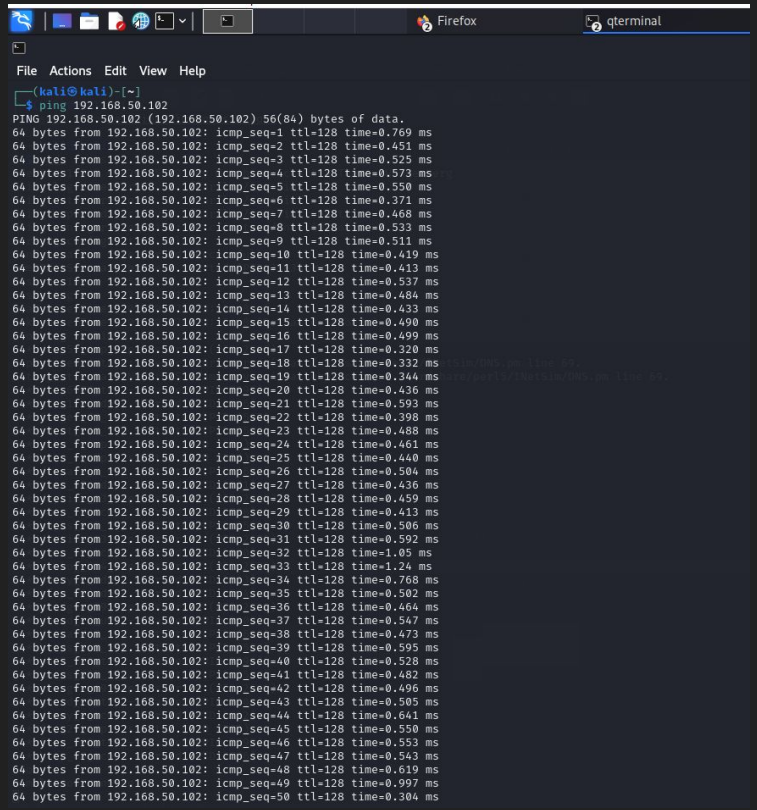
# Configurazione policy firewall - allow ping da Kali



# Configurazione policy firewall - allow ping da Kali



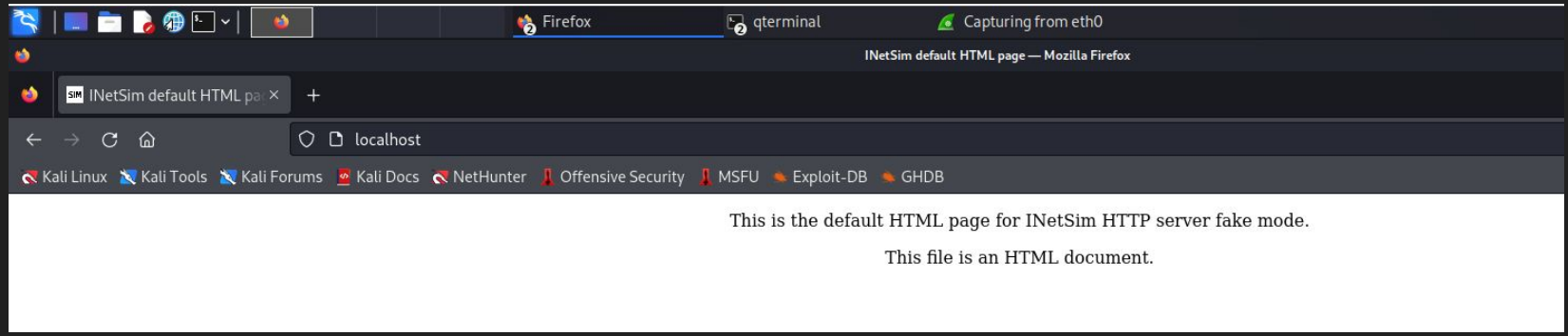



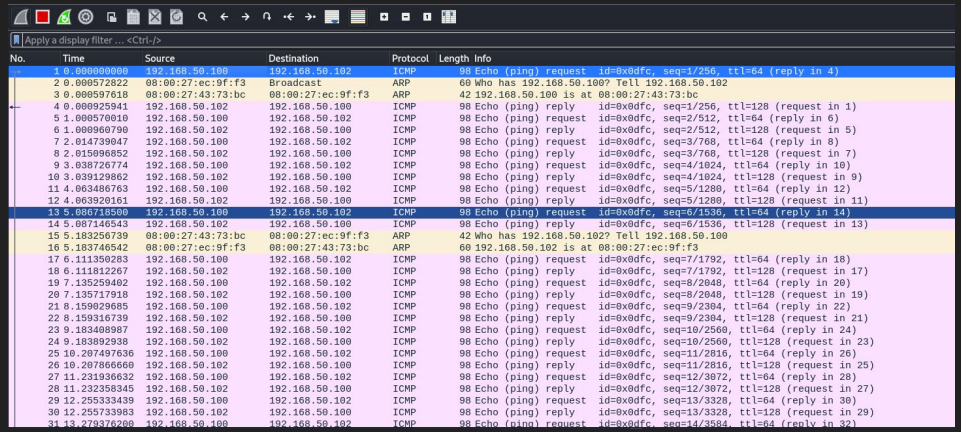
# Utilizzo InetSim

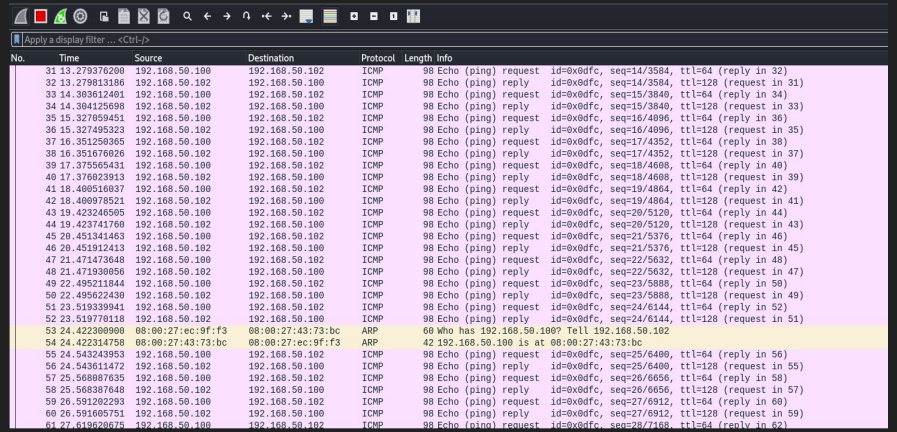
```
┌──(kali㉿kali)-[~]
└─$ sudo inetsim
INetSim 1.3.2 (2020-05-19) by Matthias Eckert & Thomas Hungenberg
Using log directory:      /var/log/inetsim/
Using data directory:     /var/lib/inetsim/
Using report directory:   /var/log/inetsim/report/
Using configuration file: /etc/inetsim/inetsim.conf
Parsing configuration file.
Configuration file parsed successfully.
=== INetSim main process started (PID 2583) ===
Session ID:     2583
Listening on:   127.0.0.1
Real Date/Time: 2024-05-24 13:26:48
Fake Date/Time: 2024-05-24 13:26:48 (Delta: 0 seconds)
 Forking services...
  * dns_53_tcp_udp - started (PID 2585)
deprecated method; prefer start_server() at /usr/share/perl5/INetSim/DNS.pm line 69.
Attempt to start Net::DNS::Nameserver in a subprocess at /usr/share/perl5/INetSim/DNS.pm line 69.
  * irc_6667_tcp - started (PID 2595)
  * ntp_123_udp - started (PID 2596)
  * finger_79_tcp - started (PID 2597)
  * ident_113_tcp - started (PID 2598)
  * echo_7_tcp - started (PID 2604)
  * echo_7_udp - started (PID 2605)
  * discard_9_udp - started (PID 2607)
  * time_37_udp - started (PID 2601)
  * daytime_13_udp - started (PID 2603)
  * smtp_25_tcp - started (PID 2588)
  * pop3s_995_tcp - started (PID 2591)
  * daytime_13_tcp - started (PID 2602)
  * time_37_tcp - started (PID 2600)
  * syslog_514_udp - started (PID 2599)
  * dummy_1_udp - started (PID 2613)
  * tftp_69_udp - started (PID 2594)
  * chargen_19_tcp - started (PID 2610)
  * quotd_17_udp - started (PID 2609)
  * discard_9_tcp - started (PID 2606)
  * https_443_tcp - started (PID 2587)
  * pop3_110_tcp - started (PID 2590)
  * smtps_465_tcp - started (PID 2589)
  * chargen_19_udp - started (PID 2611)
  * quotd_17_tcp - started (PID 2608)
  * dummy_1_tcp - started (PID 2612)
  * ftp_21_tcp - started (PID 2592)
  * ftps_990_tcp - started (PID 2593)
  * http_80_tcp - started (PID 2586)
 done.
Simulation running.
```

```
┌──(kali㉿kali)-[~]
└─$ sudo inetsim --bind-address 192.168.50.100
[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 3183) ===
Session ID:     3183
Listening on:   192.168.50.100
Real Date/Time: 2024-05-24 13:54:19
Fake Date/Time: 2024-05-24 13:54:19 (Delta: 0 seconds)
 Forking services...
  * dns_53_tcp_udp - started (PID 3185)
deprecated method; prefer start_server() at /usr/share/perl5/INetSim/DNS.pm line 69.
Attempt to start Net::DNS::Nameserver in a subprocess at /usr/share/perl5/INetSim/DNS.pm line 69.
  * irc_6667_tcp - started (PID 3195)
  * ident_113_tcp - started (PID 3198)
  * finger_79_tcp - started (PID 3197)
  * discard_9_udp - started (PID 3207)
  * time_37_tcp - started (PID 3200)
  * echo_7_tcp - started (PID 3204)
  * ntp_123_udp - started (PID 3196)
  * time_37_udp - started (PID 3201)
  * echo_7_udp - started (PID 3205)
  * discard_9_tcp - started (PID 3206)
  * chargen_19_udp - started (PID 3211)
  * syslog_514_udp - started (PID 3199)
  * ftp_21_tcp - started (PID 3192)
  * daytime_13_tcp - started (PID 3202)
  * smtps_465_tcp - started (PID 3189)
  * tftp_69_udp - started (PID 3194)
  * http_80_tcp - started (PID 3186)
  * dummy_1_tcp - started (PID 3212)
  * smtp_25_tcp - started (PID 3188)
  * daytime_13_udp - started (PID 3203)
  * https_443_tcp - started (PID 3187)
  * pop3_110_tcp - started (PID 3190)
  * dummy_1_udp - started (PID 3213)
  * chargen_19_tcp - started (PID 3210)
  * quotd_17_udp - started (PID 3209)
  * ftps_990_tcp - started (PID 3193)
  * quotd_17_tcp - started (PID 3208)
  * pop3s_995_tcp - started (PID 3191)
 done.
Simulation running.
```

# Utilizzo InetSim e cattura pacchetti con Wireshark



# InetSim da Windows 7