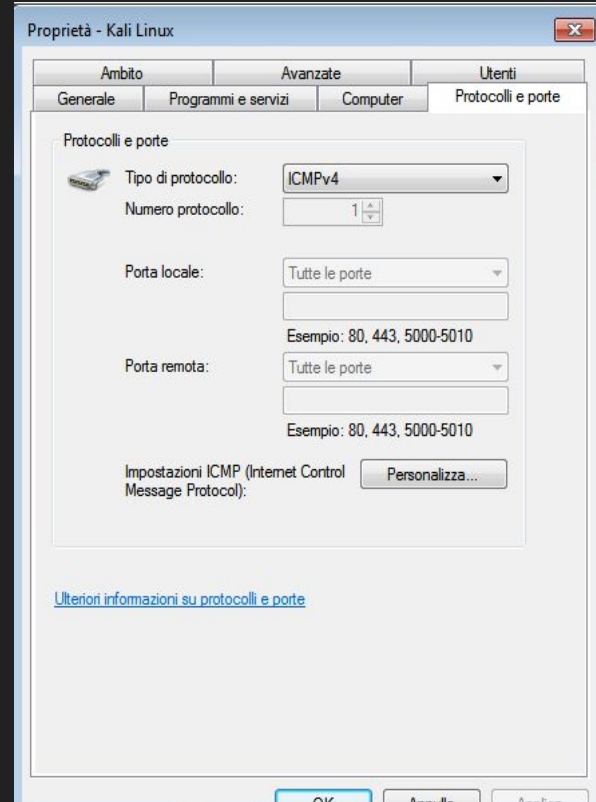
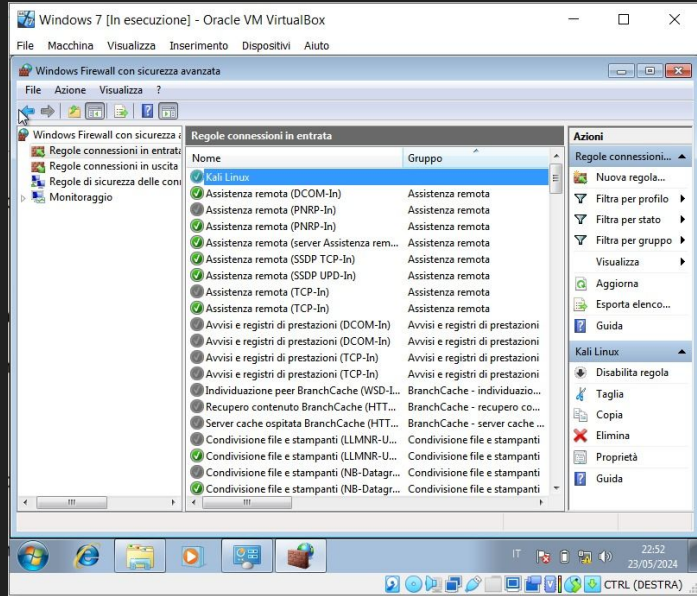


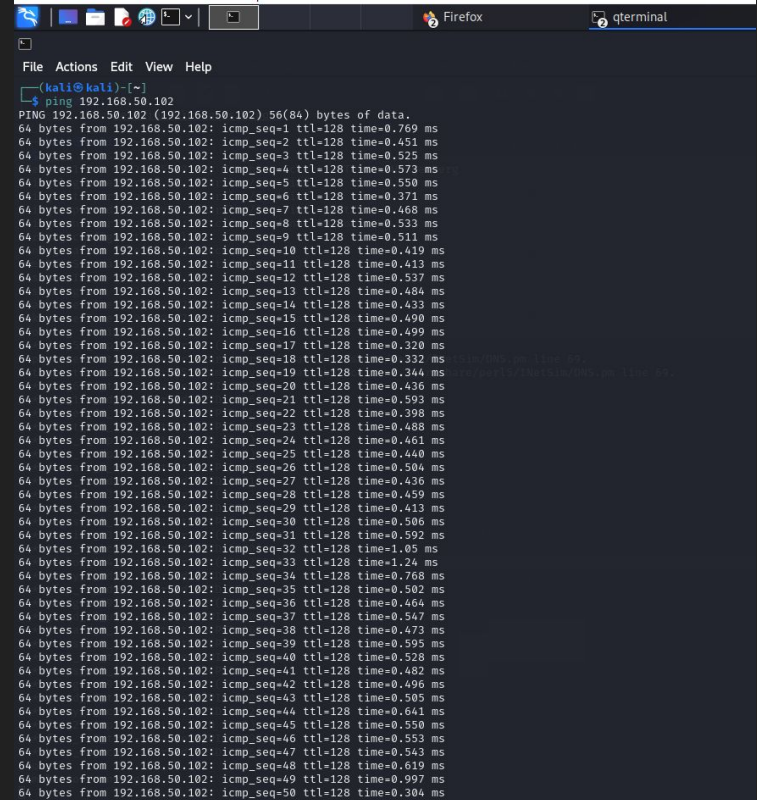
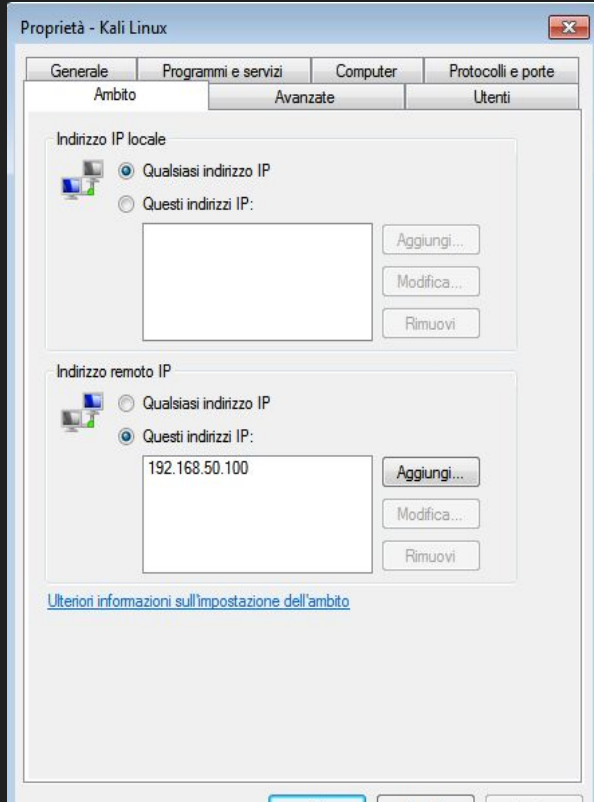
# W3D4 - Pratica

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 2501)
* daytime_13_tcp - started (PID 2602)
* time_37_tcp - started (PID 2600)
* syslog_514_udp - started (PID 2590)
* 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_udp - 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_tcp - 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

The screenshot shows a Kali Linux desktop environment. In the background, a Firefox browser window displays the "InetSim default HTML page" with a list of links: Kali Linux, Kali Tools, Kali Forums, Kali Docs, NetHunter, Offensive Security, MSFU, Exploit-DB, and GHDB. In the foreground, Wireshark is capturing network traffic on the eth0 interface. The packet list shows a series of ICMP Echo (ping) requests and responses between 192.168.50.100 and 192.168.50.102. The packet details pane shows the structure of an ICMP Echo request, including the type, code, identifier, and sequence number. The packet bytes pane shows the raw data of the packet.

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

This file is an HTML document.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.50.100	192.168.50.102	ICMP	98	Echo (ping) request id=0x0dfc, seq=1/250, ttl=64 (reply in 4)
2	0.000572822	08:00:27:ec:9f:f3	Broadcast	ARP	60	Who has 192.168.50.100? Tell 192.168.50.102
3	0.000597618	08:00:27:43:73:bc	08:00:27:ec:9f:f3	ARP	42	192.168.50.100 is at 08:00:27:43:73:bc
4	0.000925941	192.168.50.102	192.168.50.100	ICMP	98	Echo (ping) reply id=0x0dfc, seq=1/250, ttl=128 (request in 1)
5	1.000570010	192.168.50.100	192.168.50.102	ICMP	98	Echo (ping) request id=0x0dfc, seq=2/512, ttl=64 (reply in 6)
6	1.000906790	192.168.50.102	192.168.50.100	ICMP	98	Echo (ping) reply id=0x0dfc, seq=2/512, ttl=128 (request in 5)
7	2.014739047	192.168.50.100	192.168.50.102	ICMP	98	Echo (ping) request id=0x0dfc, seq=3/768, ttl=64 (reply in 8)
8	2.015096852	192.168.50.102	192.168.50.100	ICMP	98	Echo (ping) reply id=0x0dfc, seq=3/768, ttl=128 (request in 7)
9	3.038726774	192.168.50.100	192.168.50.102	ICMP	98	Echo (ping) request id=0x0dfc, seq=4/1024, ttl=64 (reply in 10)
10	3.039129862	192.168.50.102	192.168.50.100	ICMP	98	Echo (ping) reply id=0x0dfc, seq=4/1024, ttl=128 (request in 9)
11	4.063406763	192.168.50.100	192.168.50.102	ICMP	98	Echo (ping) request id=0x0dfc, seq=5/1280, ttl=64 (reply in 12)
12	4.063920161	192.168.50.102	192.168.50.100	ICMP	98	Echo (ping) reply id=0x0dfc, seq=5/1280, ttl=128 (request in 11)
13	5.080710500	192.168.50.100	192.168.50.102	ICMP	98	Echo (ping) request id=0x0dfc, seq=6/1536, ttl=64 (reply in 14)
14	5.081746543	192.168.50.102	192.168.50.100	ICMP	98	Echo (ping) reply id=0x0dfc, seq=6/1536, ttl=128 (request in 13)
15	5.183256730	08:00:27:43:73:bc	08:00:27:ec:9f:f3	ARP	42	Who has 192.168.50.102? Tell 192.168.50.100
16	5.183746542	08:00:27:ec:9f:f3	08:00:27:43:73:bc	ARP	60	192.168.50.102 is at 08:00:27:ec:9f:f3
17	6.111359283	192.168.50.100	192.168.50.102	ICMP	98	Echo (ping) request id=0x0dfc, seq=7/1792, ttl=64 (reply in 18)
18	6.111812267	192.168.50.102	192.168.50.100	ICMP	98	Echo (ping) reply id=0x0dfc, seq=7/1792, ttl=128 (request in 17)
19	7.135259402	192.168.50.100	192.168.50.102	ICMP	98	Echo (ping) request id=0x0dfc, seq=8/2048, ttl=64 (reply in 20)
20	7.135717918	192.168.50.102	192.168.50.100	ICMP	98	Echo (ping) reply id=0x0dfc, seq=8/2048, ttl=128 (request in 19)
21	8.159029685	192.168.50.100	192.168.50.102	ICMP	98	Echo (ping) request id=0x0dfc, seq=9/2304, ttl=64 (reply in 22)
22	8.159316719	192.168.50.102	192.168.50.100	ICMP	98	Echo (ping) reply id=0x0dfc, seq=9/2304, ttl=128 (request in 21)
23	9.183408987	192.168.50.100	192.168.50.102	ICMP	98	Echo (ping) request id=0x0dfc, seq=10/2560, ttl=64 (reply in 24)
24	9.183892938	192.168.50.102	192.168.50.100	ICMP	98	Echo (ping) reply id=0x0dfc, seq=10/2560, ttl=128 (request in 23)
25	10.207497636	192.168.50.100	192.168.50.102	ICMP	98	Echo (ping) request id=0x0dfc, seq=11/2816, ttl=64 (reply in 26)
26	10.207866660	192.168.50.102	192.168.50.100	ICMP	98	Echo (ping) reply id=0x0dfc, seq=11/2816, ttl=128 (request in 25)
27	11.231936632	192.168.50.100	192.168.50.102	ICMP	98	Echo (ping) request id=0x0dfc, seq=12/3072, ttl=64 (reply in 28)
28	11.232358345	192.168.50.102	192.168.50.100	ICMP	98	Echo (ping) reply id=0x0dfc, seq=12/3072, ttl=128 (request in 27)
29	12.255333439	192.168.50.100	192.168.50.102	ICMP	98	Echo (ping) request id=0x0dfc, seq=13/3328, ttl=64 (reply in 30)
30	12.255733983	192.168.50.102	192.168.50.100	ICMP	98	Echo (ping) reply id=0x0dfc, seq=13/3328, ttl=128 (request in 29)
31	13.279376280	192.168.50.100	192.168.50.102	ICMP	98	Echo (ping) request id=0x0dfc, seq=14/3584, ttl=64 (reply in 32)
32	13.279813186	192.168.50.102	192.168.50.100	ICMP	98	Echo (ping) reply id=0x0dfc, seq=14/3584, ttl=128 (request in 31)
33	14.303051201	192.168.50.100	192.168.50.102	ICMP	98	Echo (ping) request id=0x0dfc, seq=15/3840, ttl=64 (reply in 34)
34	14.304125698	192.168.50.102	192.168.50.100	ICMP	98	Echo (ping) reply id=0x0dfc, seq=15/3840, ttl=128 (request in 33)
35	15.327059451	192.168.50.100	192.168.50.102	ICMP	98	Echo (ping) request id=0x0dfc, seq=16/4096, ttl=64 (reply in 36)
36	15.327495323	192.168.50.102	192.168.50.100	ICMP	98	Echo (ping) reply id=0x0dfc, seq=16/4096, ttl=128 (request in 35)
37	16.351250305	192.168.50.100	192.168.50.102	ICMP	98	Echo (ping) request id=0x0dfc, seq=17/4352, ttl=64 (reply in 38)
38	16.351676826	192.168.50.102	192.168.50.100	ICMP	98	Echo (ping) reply id=0x0dfc, seq=17/4352, ttl=128 (request in 37)
39	17.375565431	192.168.50.100	192.168.50.102	ICMP	98	Echo (ping) request id=0x0dfc, seq=18/4608, ttl=64 (reply in 40)
40	17.376820913	192.168.50.102	192.168.50.100	ICMP	98	Echo (ping) reply id=0x0dfc, seq=18/4608, ttl=128 (request in 39)
41	18.408510837	192.168.50.100	192.168.50.102	ICMP	98	Echo (ping) request id=0x0dfc, seq=19/4864, ttl=64 (reply in 42)
42	18.408978521	192.168.50.102	192.168.50.100	ICMP	98	Echo (ping) reply id=0x0dfc, seq=19/4864, ttl=128 (request in 41)
43	19.423246595	192.168.50.100	192.168.50.102	ICMP	98	Echo (ping) request id=0x0dfc, seq=20/5120, ttl=64 (reply in 44)
44	19.423741760	192.168.50.102	192.168.50.100	ICMP	98	Echo (ping) reply id=0x0dfc, seq=20/5120, ttl=128 (request in 43)
45	19.451341463	192.168.50.100	192.168.50.102	ICMP	98	Echo (ping) request id=0x0dfc, seq=21/5376, ttl=64 (reply in 46)
46	19.451912413	192.168.50.102	192.168.50.100	ICMP	98	Echo (ping) reply id=0x0dfc, seq=21/5376, ttl=128 (request in 45)
47	21.471473848	192.168.50.100	192.168.50.102	ICMP	98	Echo (ping) request id=0x0dfc, seq=22/5632, ttl=64 (reply in 48)
48	21.471938056	192.168.50.102	192.168.50.100	ICMP	98	Echo (ping) reply id=0x0dfc, seq=22/5632, ttl=128 (request in 47)
49	22.495211344	192.168.50.100	192.168.50.102	ICMP	98	Echo (ping) request id=0x0dfc, seq=23/5888, ttl=64 (reply in 50)
50	22.495622430	192.168.50.102	192.168.50.100	ICMP	98	Echo (ping) reply id=0x0dfc, seq=23/5888, ttl=128 (request in 49)
51	23.519339941	192.168.50.100	192.168.50.102	ICMP	98	Echo (ping) request id=0x0dfc, seq=24/6144, ttl=64 (reply in 52)
52	23.519770116	192.168.50.102	192.168.50.100	ICMP	98	Echo (ping) reply id=0x0dfc, seq=24/6144, ttl=128 (request in 51)
53	24.422300900	08:00:27:ec:9f:f3	08:00:27:43:73:bc	ARP	60	Who has 192.168.50.100? Tell 192.168.50.102
54	24.422314758	08:00:27:43:73:bc	08:00:27:ec:9f:f3	ARP	42	192.168.50.100 is at 08:00:27:ec:9f:f3
55	24.543243953	192.168.50.100	192.168.50.102	ICMP	98	Echo (ping) request id=0x0dfc, seq=25/6400, ttl=64 (reply in 56)
56	24.543611472	192.168.50.102	192.168.50.100	ICMP	98	Echo (ping) reply id=0x0dfc, seq=25/6400, ttl=128 (request in 55)
57	25.568807635	192.168.50.100	192.168.50.102	ICMP	98	Echo (ping) request id=0x0dfc, seq=26/6656, ttl=64 (reply in 58)
58	25.568387648	192.168.50.102	192.168.50.100	ICMP	98	Echo (ping) reply id=0x0dfc, seq=26/6656, ttl=128 (request in 57)
59	26.591202293	192.168.50.100	192.168.50.102	ICMP	98	Echo (ping) request id=0x0dfc, seq=27/6912, ttl=64 (reply in 60)
60	26.591608751	192.168.50.102	192.168.50.100	ICMP	98	Echo (ping) reply id=0x0dfc, seq=27/6912, ttl=128 (request in 59)
61	27.619208075	192.168.50.100	192.168.50.102	ICMP	98	Echo (ping) request id=0x0dfc, seq=28/7168, ttl=64 (reply in 62)



# InetSim da Windows 7

