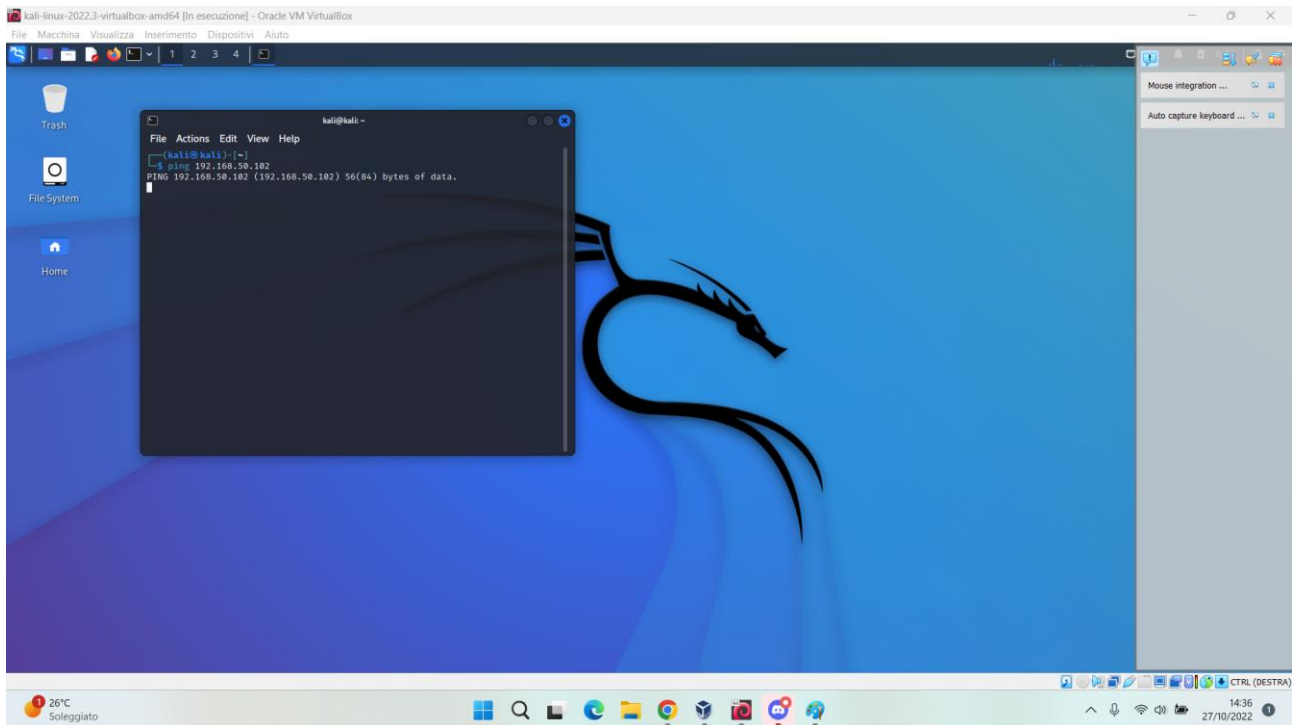
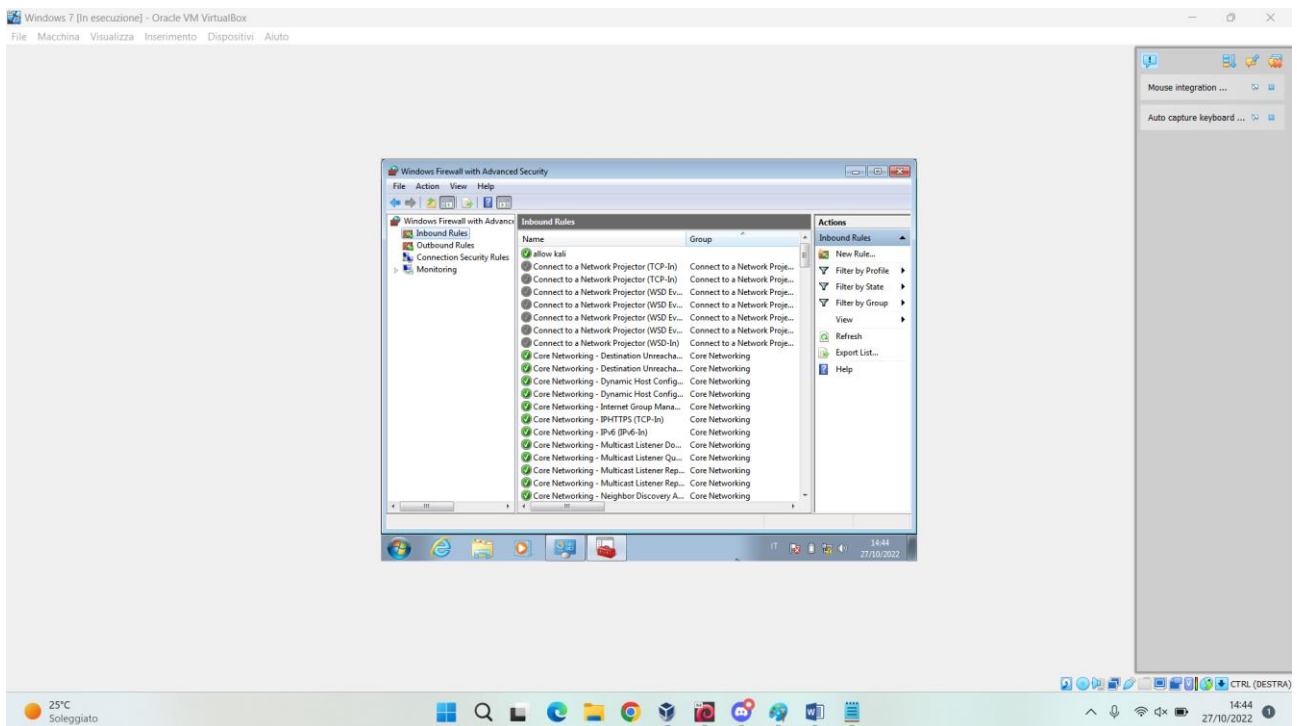


CREARE UNA REGOLA SUL FIREWALL E SNIFFARE TRAFFICO CON WIRESHARK

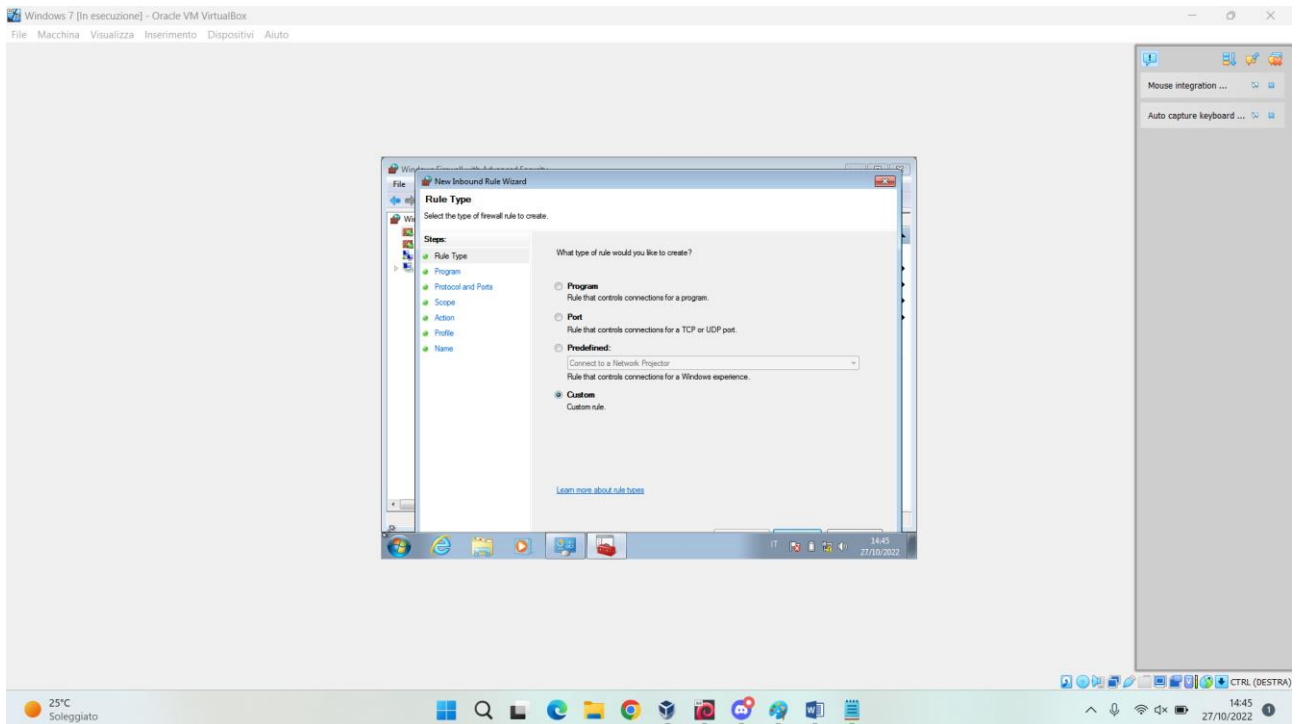
Possiamo vedere come, una volta riattivato il firewall, l'IP di Windows 7 non è più raggiungibile:



Per poter di nuovo raggiungere l'host, dobbiamo creare una regola andando su Windows 7, Control Panel, cliccheremo poi su Windows Firewall e dal menù a sinistra selezioneremo Advanced Settings ritrovandoci così in questa schermata:

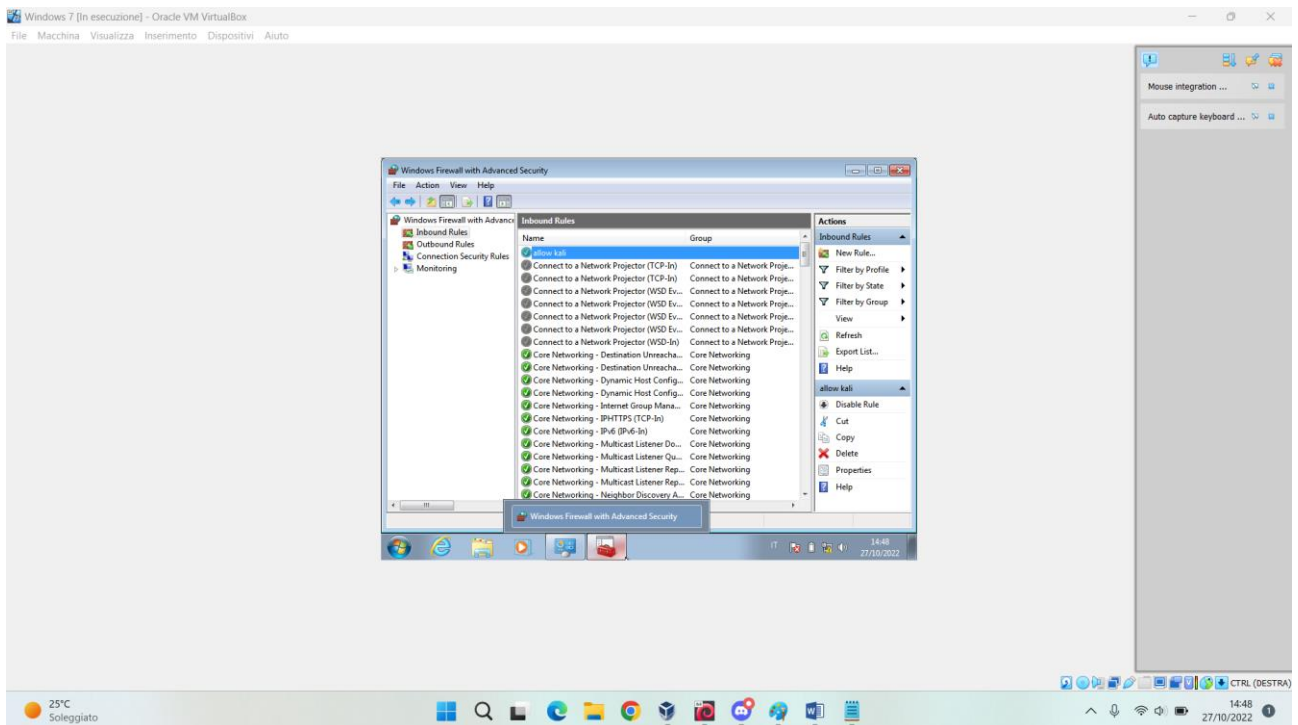


Selezioniamo Inbound Rules e successivamente New Rules; si aprirà così questa schermata:



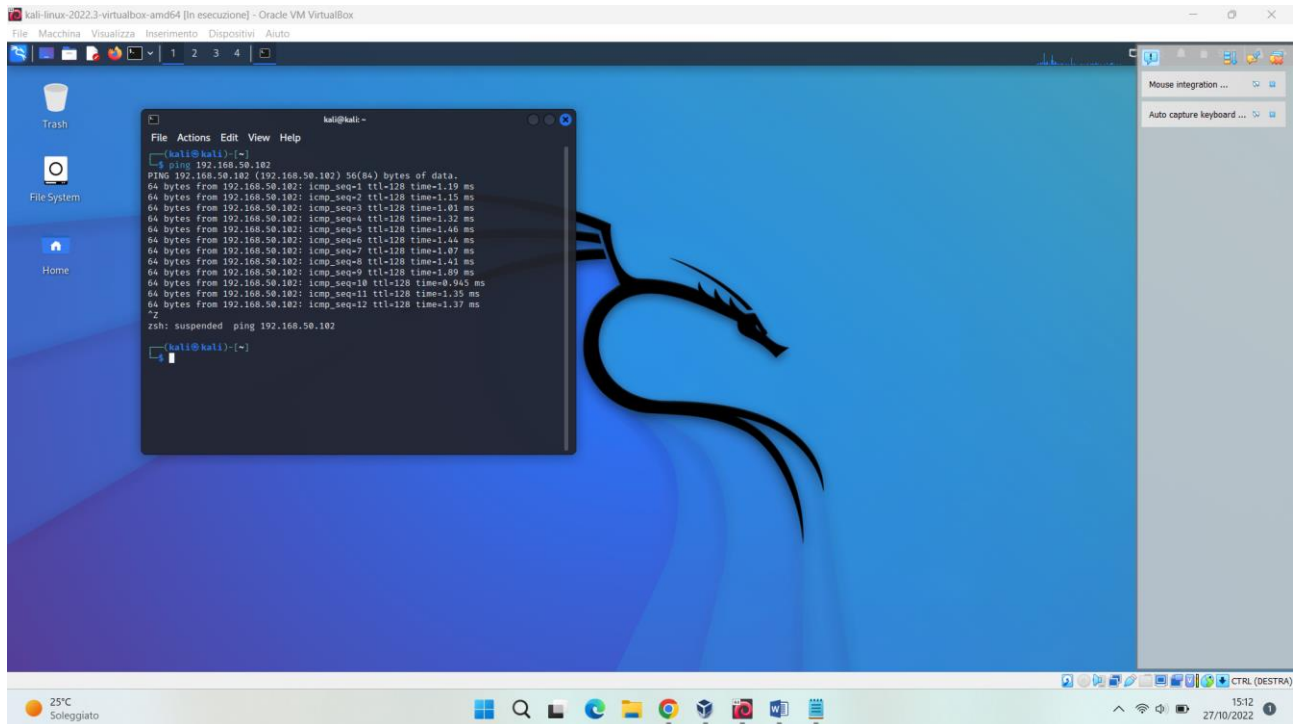
Procediamo quindi a creare la nuova regola modificando le seguenti voci:

- Rule Type: Custom
- Scope: Local IP Address quello di Windows 7 (192.168.50.102) – Remote IP Address quello di Kali (192.168.50.100)
- Action: Allow the connection
- Name: il nome della regola (in questo caso l’ho chiamata “allow kali” come si può vedere nell’immagine sotto)

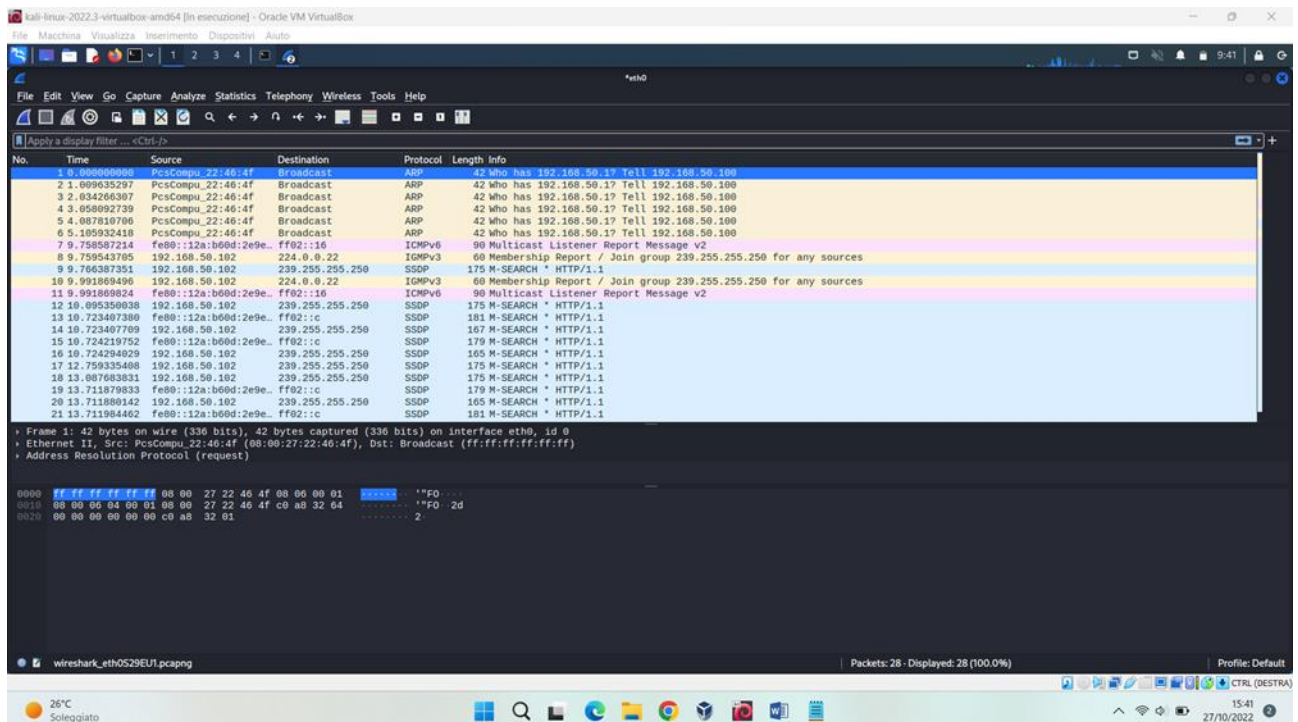


Riavviamo il sistema per rendere effettive le modifiche.

Una volta creata la nuova regola sul firewall di Windows 7, andiamo su Kali e diamo il comando ping:



Qui sotto troviamo il traffico sniffato da Wireshark cercando Inetsim sul prompt:



Questo invece è il traffico sniffato da Wireshark facendo il ping all' IP appartenente a Windows 7:

The screenshot shows a Kali Linux virtual machine environment. The Wireshark network protocol analyzer is open, displaying a list of captured packets. The display filter is set to 'icmp'. The packet list shows 22 packets, all of which are ICMP Echo (ping) requests and replies. The source and destination IP addresses are 192.168.50.100 and 192.168.50.102. The packet details pane shows the selected packet (No. 1) as an ICMP Echo (ping) request. The packet bytes pane shows the raw data of the packet, including the ICMP header and the payload.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.50.100	192.168.50.102	ICMP	98	Echo (ping) request id=0x80e2, seq=1/256, ttl=64 (reply in 4)
2	0.000702217	PcsCompu_44:8f:fc	Broadcast	ARP	60	Who has 192.168.50.100? Tell 192.168.50.102
3	0.000714518	PcsCompu_22:46:4f	PcsCompu_44:8f:fc	ARP	42	192.168.50.100 is at 08:00:27:22:46:4f
4	0.001145849	192.168.50.102	192.168.50.100	ICMP	98	Echo (ping) reply id=0x80e2, seq=1/256, ttl=128 (request in 1)
5	1.005564485	192.168.50.100	192.168.50.102	ICMP	98	Echo (ping) request id=0x80e2, seq=2/512, ttl=64 (reply in 6)
6	1.006786680	192.168.50.102	192.168.50.100	ICMP	98	Echo (ping) reply id=0x80e2, seq=2/512, ttl=128 (request in 5)
7	2.014859130	192.168.50.100	192.168.50.102	ICMP	98	Echo (ping) request id=0x80e2, seq=3/768, ttl=64 (reply in 8)
8	2.015418767	192.168.50.102	192.168.50.100	ICMP	98	Echo (ping) reply id=0x80e2, seq=3/768, ttl=128 (request in 7)
9	3.026867935	192.168.50.100	192.168.50.102	ICMP	98	Echo (ping) request id=0x80e2, seq=4/1024, ttl=64 (reply in 10)
10	3.028190062	192.168.50.102	192.168.50.100	ICMP	98	Echo (ping) reply id=0x80e2, seq=4/1024, ttl=128 (request in 9)
11	4.037437691	192.168.50.100	192.168.50.102	ICMP	98	Echo (ping) request id=0x80e2, seq=5/1280, ttl=64 (reply in 12)
12	4.038581755	192.168.50.102	192.168.50.100	ICMP	98	Echo (ping) reply id=0x80e2, seq=5/1280, ttl=128 (request in 11)
13	5.043845203	192.168.50.100	192.168.50.102	ICMP	98	Echo (ping) request id=0x80e2, seq=6/1536, ttl=64 (reply in 14)
14	5.044933375	192.168.50.102	192.168.50.100	ICMP	98	Echo (ping) reply id=0x80e2, seq=6/1536, ttl=128 (request in 13)
15	5.115854235	PcsCompu_22:46:4f	PcsCompu_44:8f:fc	ARP	42	Who has 192.168.50.102? Tell 192.168.50.100
16	5.116798883	PcsCompu_44:8f:fc	PcsCompu_22:46:4f	ARP	60	192.168.50.102 is at 08:00:27:22:46:4f
17	6.048495762	192.168.50.100	192.168.50.102	ICMP	98	Echo (ping) request id=0x80e2, seq=7/1792, ttl=64 (reply in 18)
18	6.049577917	192.168.50.102	192.168.50.100	ICMP	98	Echo (ping) reply id=0x80e2, seq=7/1792, ttl=128 (request in 17)
19	7.067469856	192.168.50.100	192.168.50.102	ICMP	98	Echo (ping) request id=0x80e2, seq=8/2048, ttl=64 (reply in 20)
20	7.068382507	192.168.50.102	192.168.50.100	ICMP	98	Echo (ping) reply id=0x80e2, seq=8/2048, ttl=128 (request in 19)
21	8.069595789	192.168.50.100	192.168.50.102	ICMP	98	Echo (ping) request id=0x80e2, seq=9/2304, ttl=64 (reply in 22)
22	8.070415955	192.168.50.102	192.168.50.100	ICMP	98	Echo (ping) reply id=0x80e2, seq=9/2304, ttl=128 (request in 21)

Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface eth0, id 0
Ethernet II, Src: PcsCompu_22:46:4f (08:00:27:22:46:4f), Dst: PcsCompu_44:8f:fc (08:00:27:22:46:4f)
Internet Protocol Version 4, Src: 192.168.50.100, Dst: 192.168.50.102
Internet Control Message Protocol

0000 08 00 27 22 46 4f 08 00 27 22 46 4f 08 00 45 00 ... 'D'...'FD' E
0010 00 54 cb 9e 40 00 48 01 00 e7 c0 a8 32 64 c0 a8 ... T @ @ ... 2d
0020 32 66 08 00 07 0d 00 e2 00 01 b6 8a 5a 63 00 00 ... 2f 2c
0030 00 00 2d 4d 03 00 00 00 00 00 10 11 12 13 14 15 ... 7f..... 17e5
0040 18 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 ... 81(1)...../012345
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 ...
0060 36 37

Wireshark interface: eth0/JUUL.pcapng
Packets: 22 - Displayed: 22 (100.0%)
Profile: Default