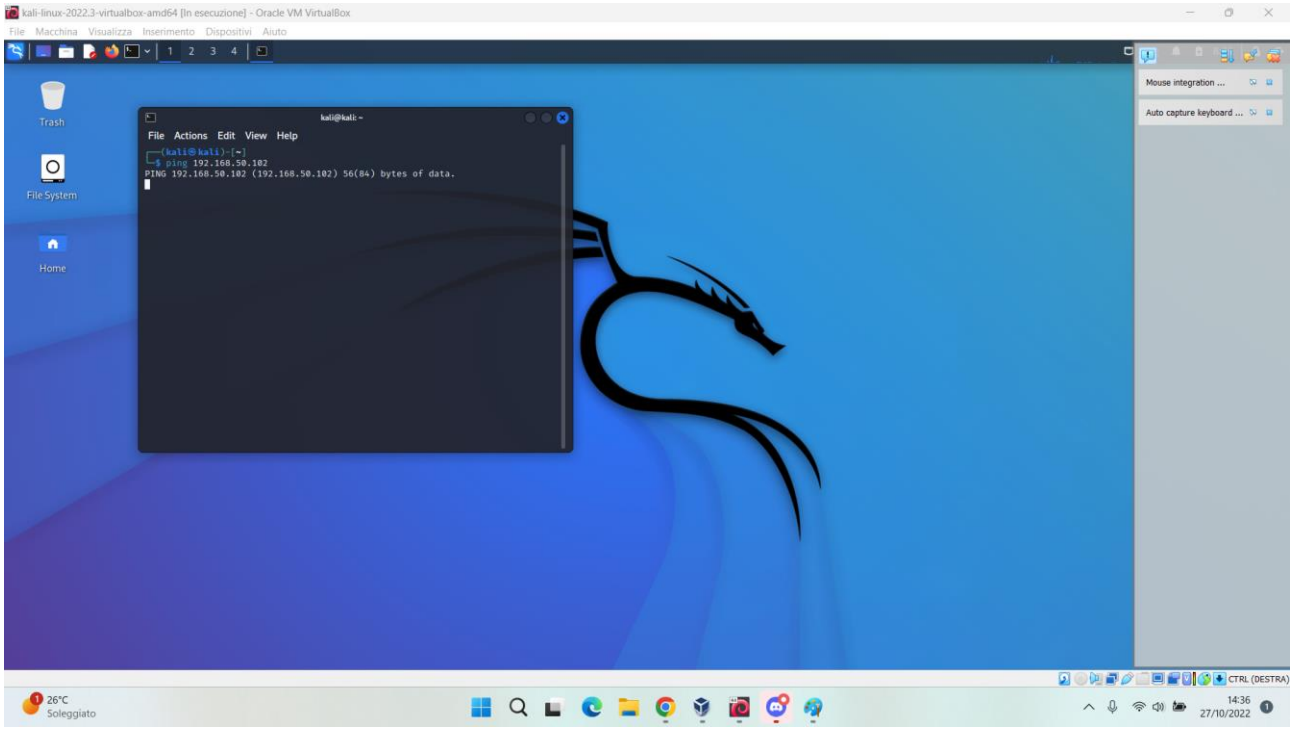
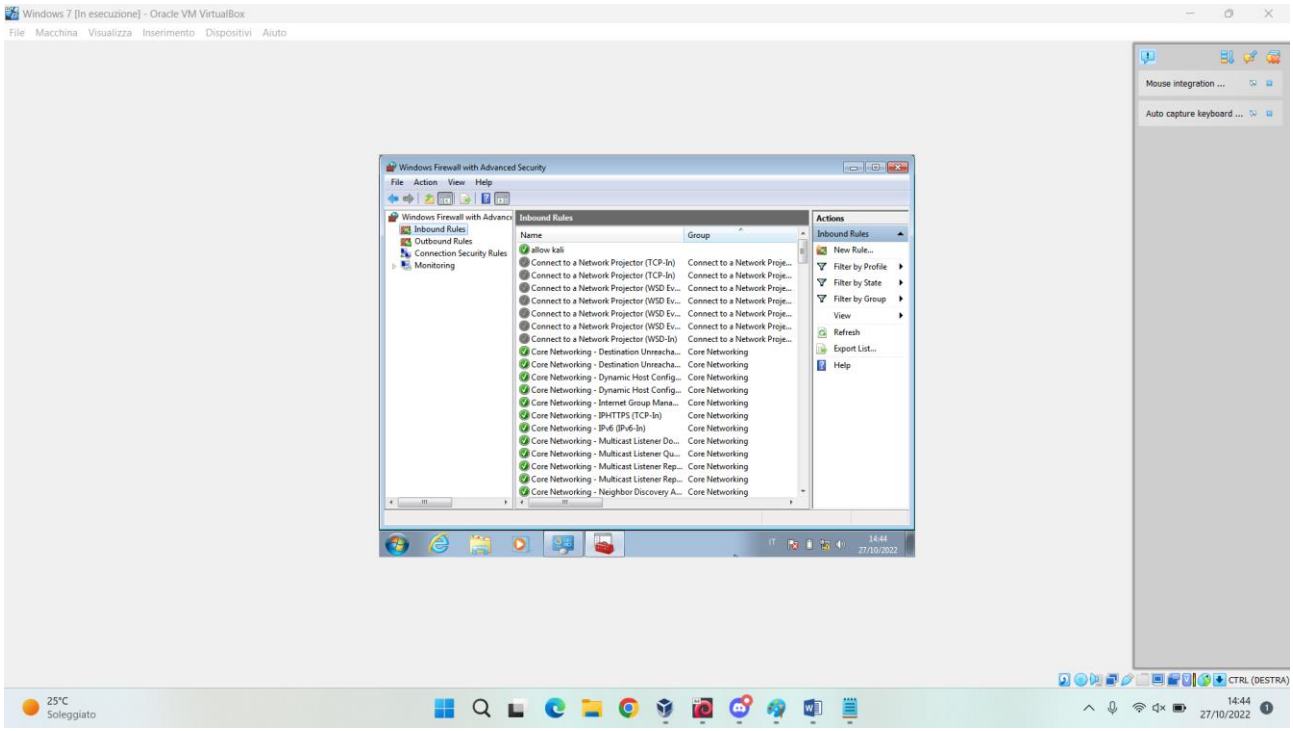
CREARE UNA REGOLA SUL FIREWALL E SNIFFARE TRAFFICO CON WIRESHARK

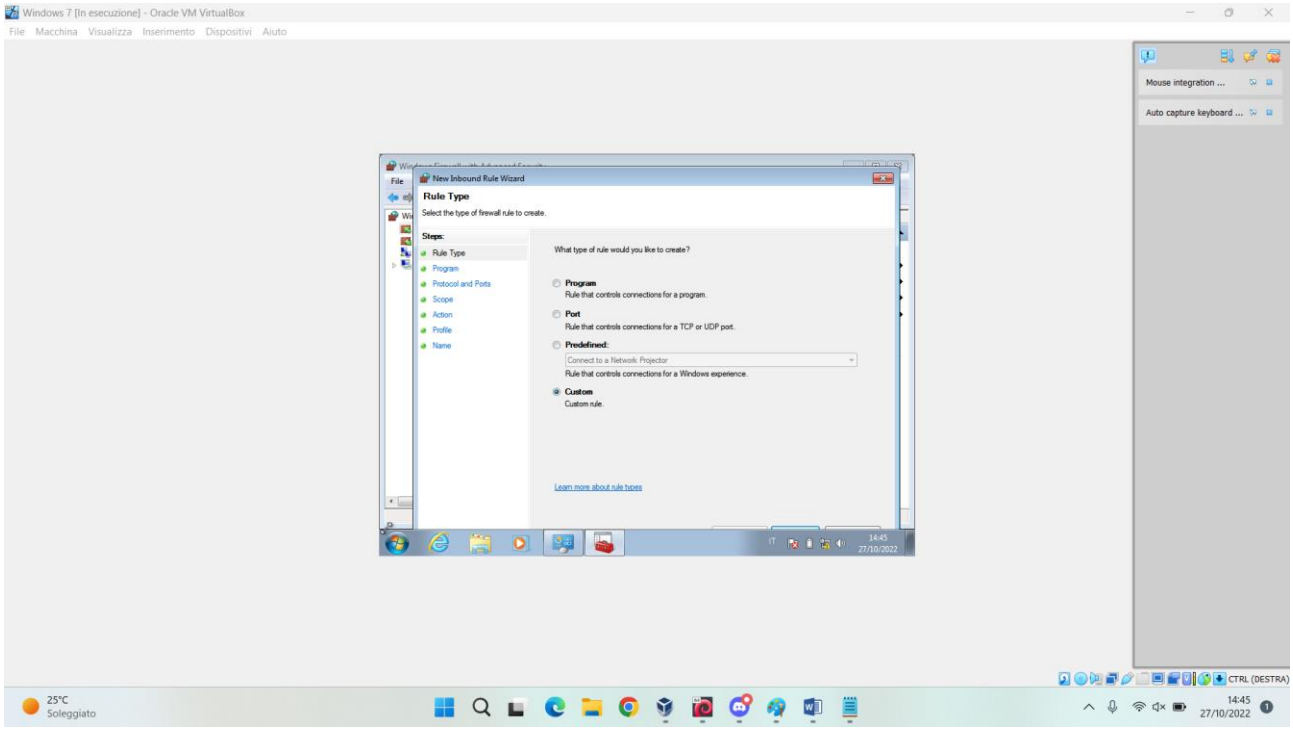
Possiamo vedere come, una volta riattivato il firewall, l'IP di Windows 7 non è più raggiungibile:



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:

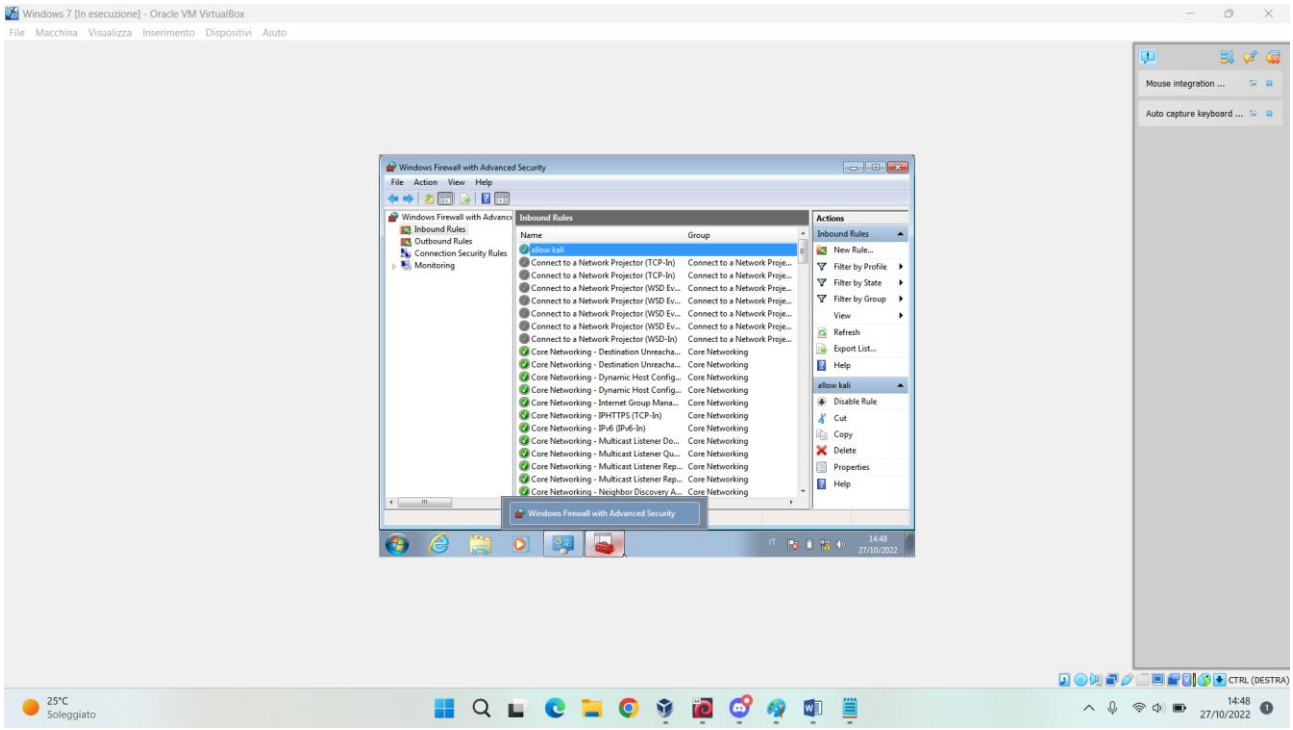


Selezioniamo Inbound Rules e successivamente New Rules; si aprirà così questa schermata:



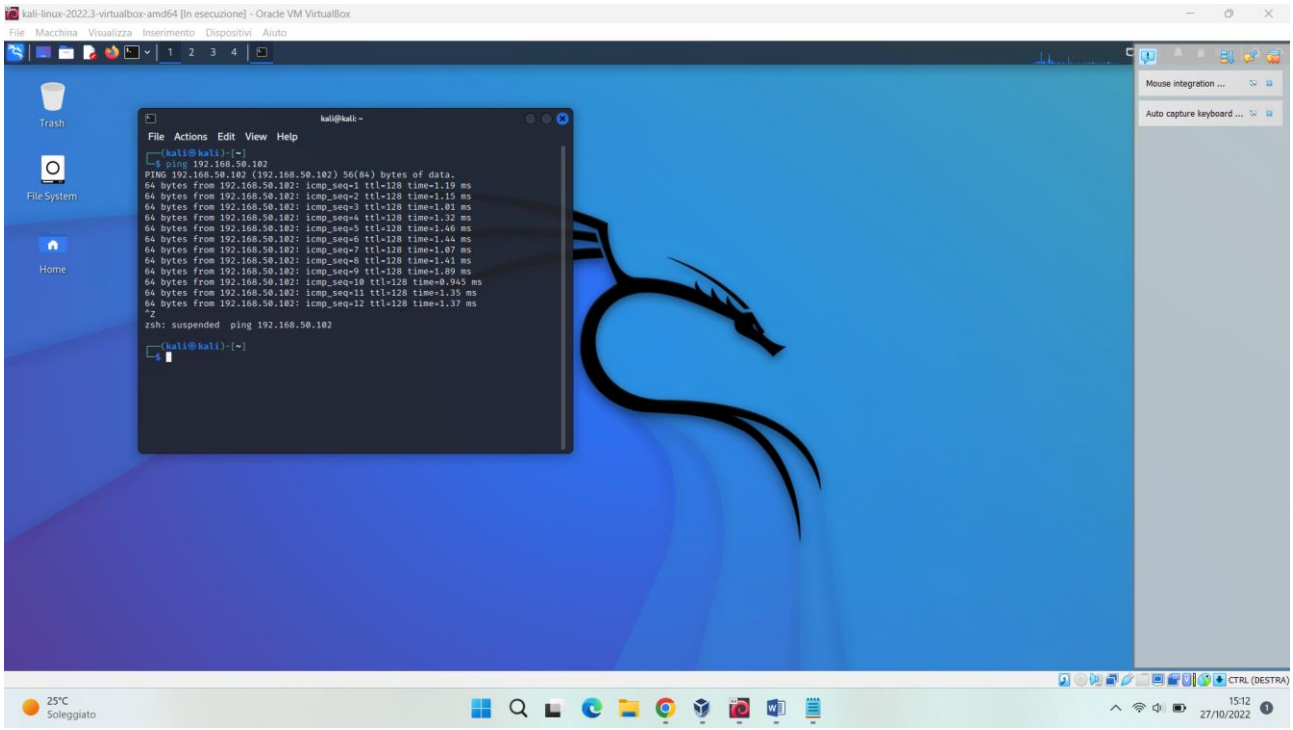
Procediamo quindi a creare la nuova regola modificando le seguenti voci:

- 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)

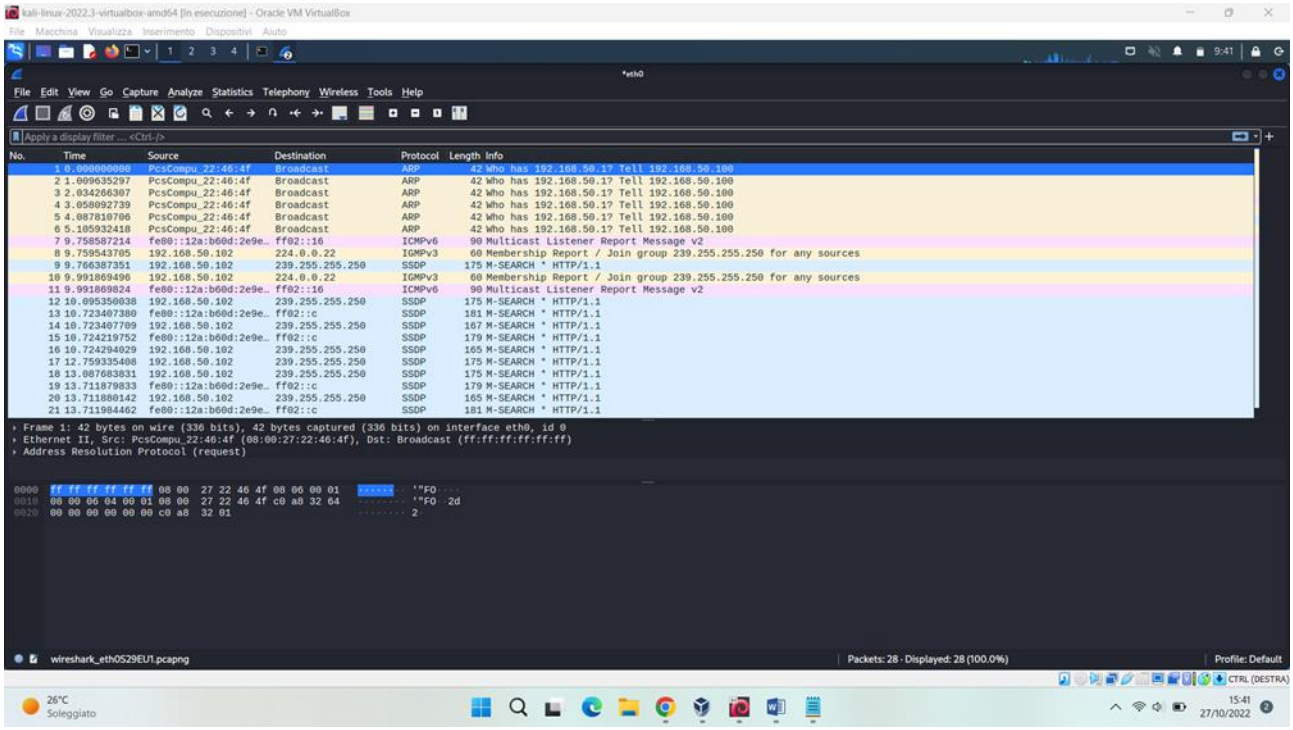


Riavviamo il sistema per rendere effettive le modifiche.

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: