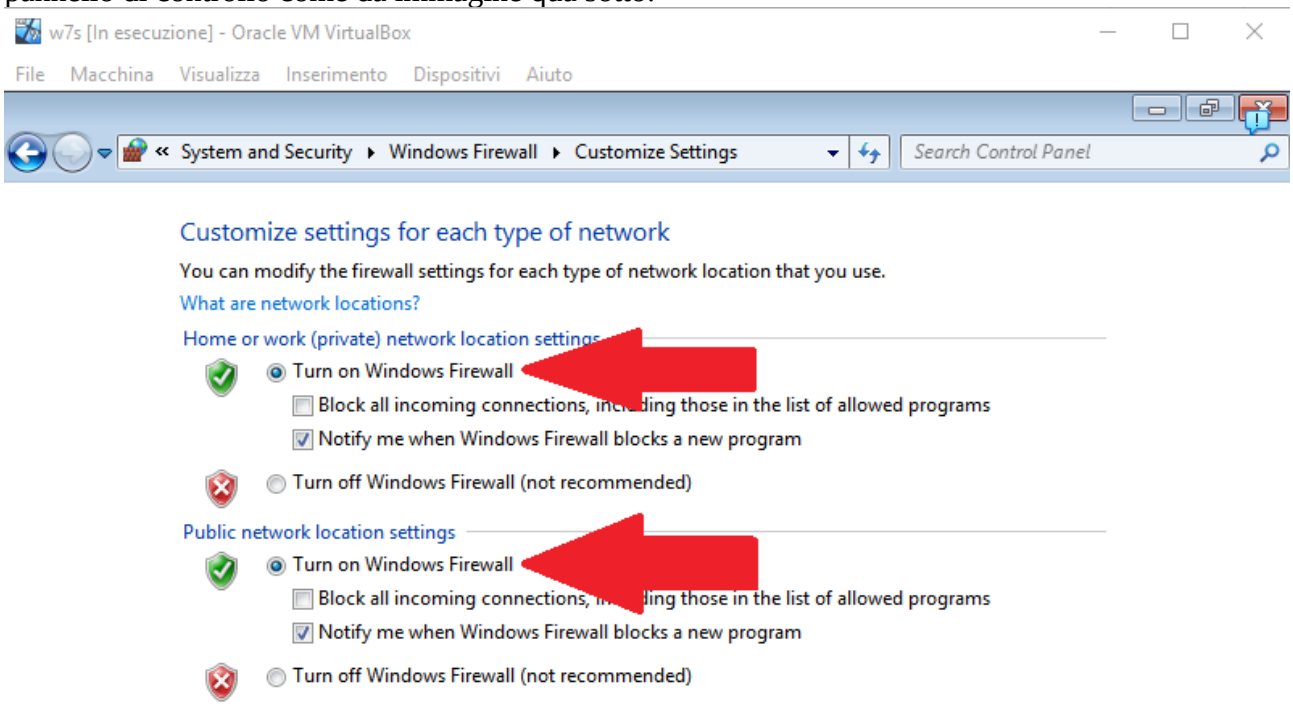
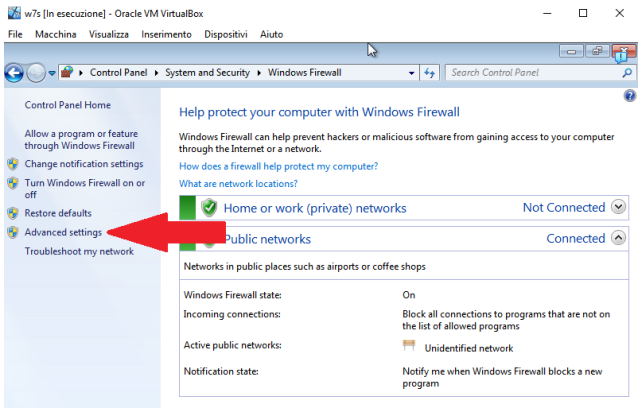
ESERCIZIO 4

CONFIGURAZIONE DELLA POLICY DI WINDOWS FIREWALL E TEST DI SNIFFING SU RETE SIMULATA CON INETSIM

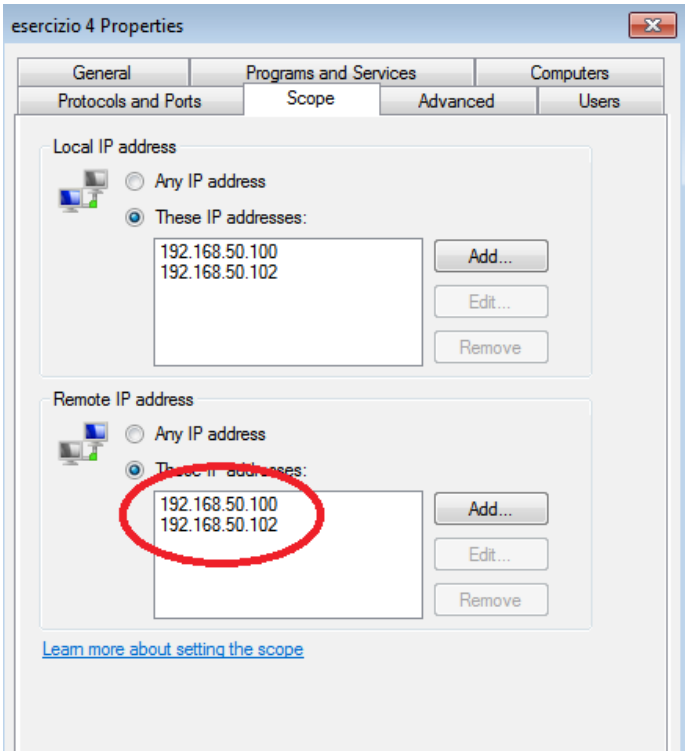
Come prima cosa sono andato a riattivare il firewall di Windows nell'apposito menù accessibile dal pannello di controllo come da immagine qua sotto:



Successivamente sono andato sulle impstazioni avanzate per aggiungere la policy in modo tale che kali e windows possano comunicare tra loro nella categoria inbound rules:



Dal menù ho selezionato di aggiungere un’eccezione per gli indirizzi IP come mostrati in figura:

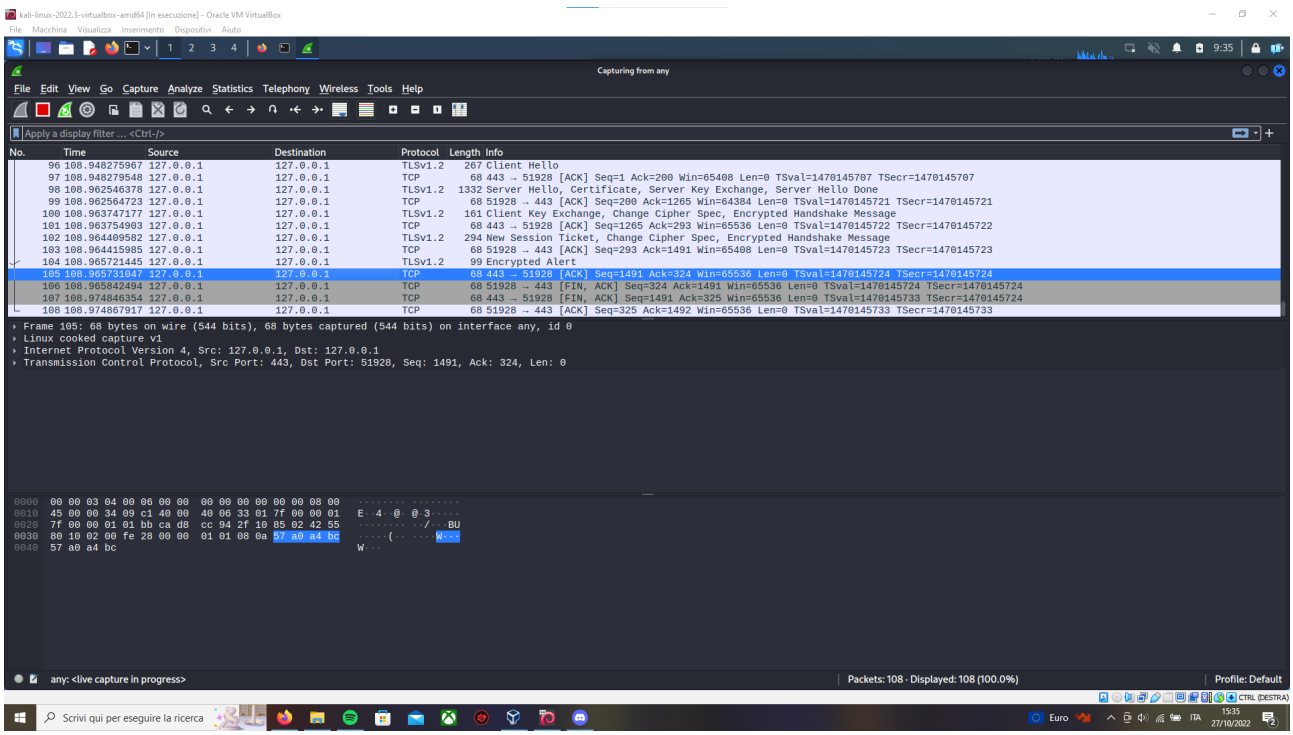


Infine ho verificato che effettivamente le 2 macchine fossero in grado di comunicare lanciando il comando ping dal terminale di kali, e così è stato:

```
┌──(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=0.484 ms
64 bytes from 192.168.50.102: icmp_seq=2 ttl=128 time=0.426 ms
64 bytes from 192.168.50.102: icmp_seq=3 ttl=128 time=0.430 ms
64 bytes from 192.168.50.102: icmp_seq=4 ttl=128 time=0.426 ms
64 bytes from 192.168.50.102: icmp_seq=5 ttl=128 time=0.431 ms
64 bytes from 192.168.50.102: icmp_seq=6 ttl=128 time=0.430 ms
^Z
zsh: suspended  ping 192.168.50.102
```

Dopodichè sono passato alla fase successiva dell'esercizio. Il primo passo è stato quello di avviare initsim tramite comando da terminale:

successivamente ho controllato tramite browser l'indirizzo IP che era segnato nel teminale per controllare che fosse effettivamente partito. Avuto conferma di ciò ho avviato wireshark che mi ha restituito questa schermata:



Dalla schermata qui sopra possiamo vedere come wireshark ha fatto sniffing sui pacchetti che il server ha inviato a kali linux come dimostrano gli indirizzi IP presenti in nell'immagine qui sopra.