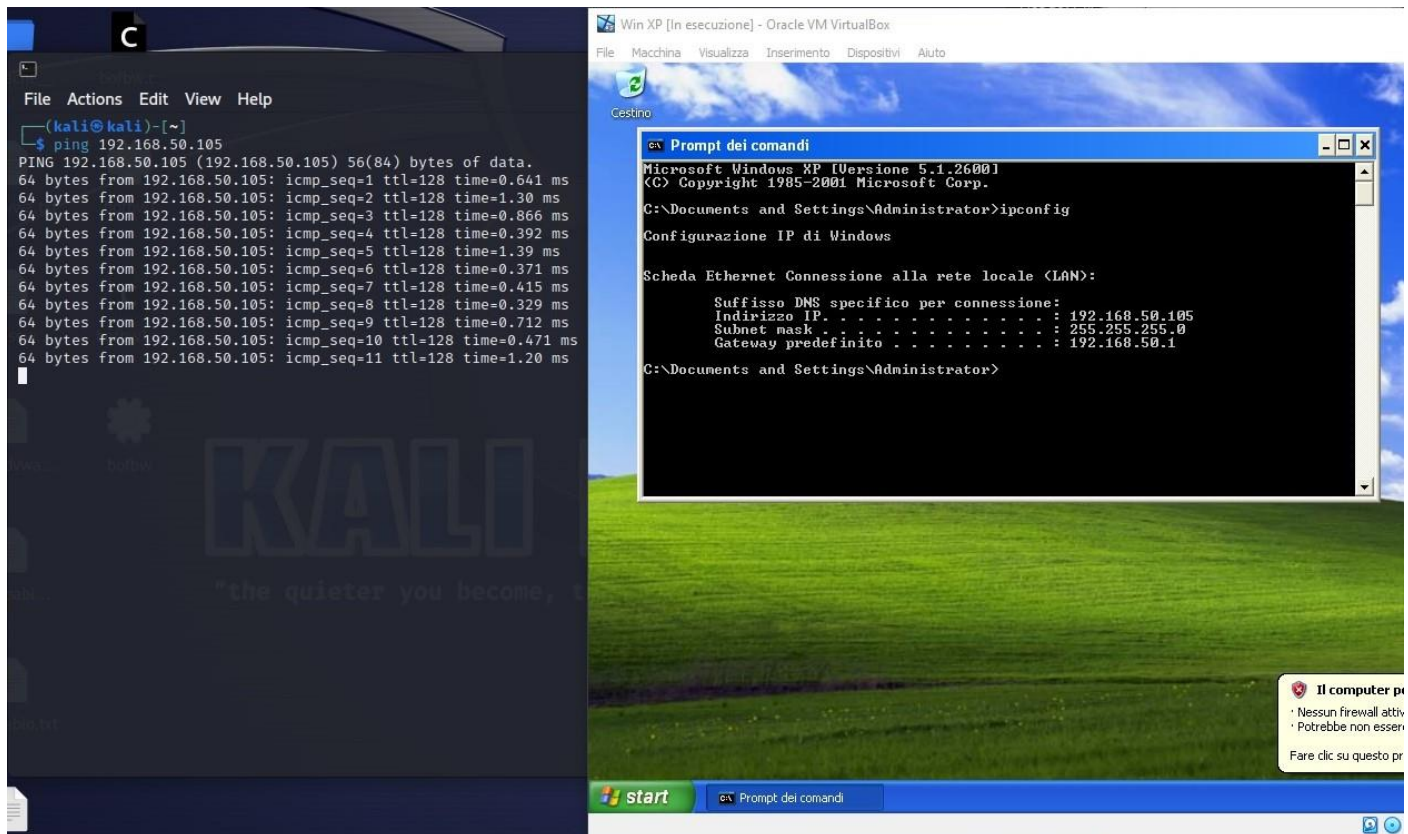


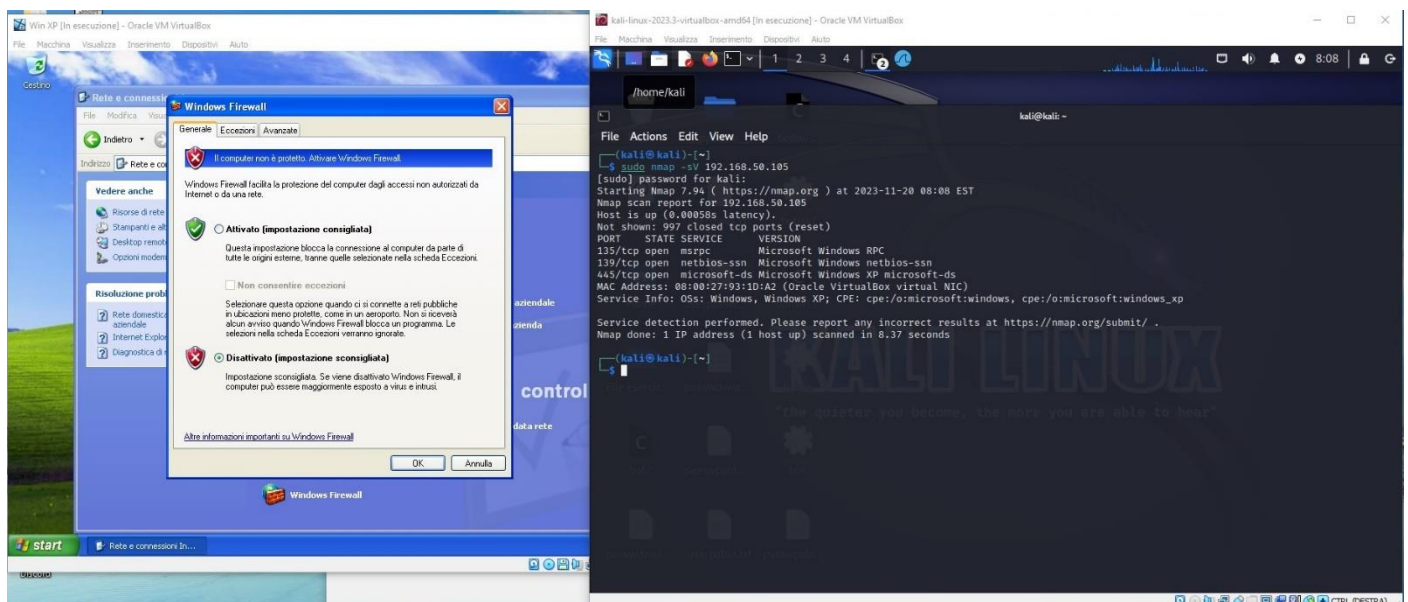
# S9/L1 Esercizio 20/11/2023

In questo esercizio ci viene richiesto di effettuare due scansioni con nmap sul sistema operativo Windows XP, la prima con il firewall disattivato e la seconda con il firewall attivato; di effettuare delle considerazioni tra le due scansioni e di ipotizzare quale sia la causa dei risultati diversi

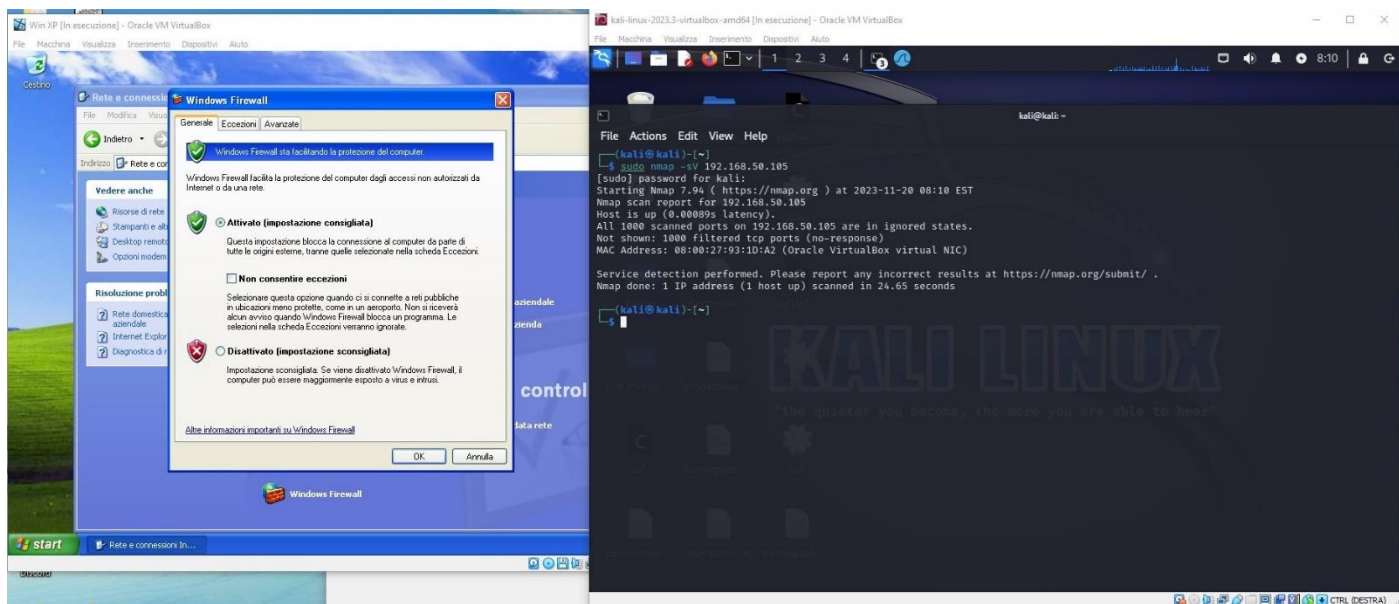
Come sempre, prima di ogni cosa, controlliamo che le due macchine siano in comunicazione tra loro



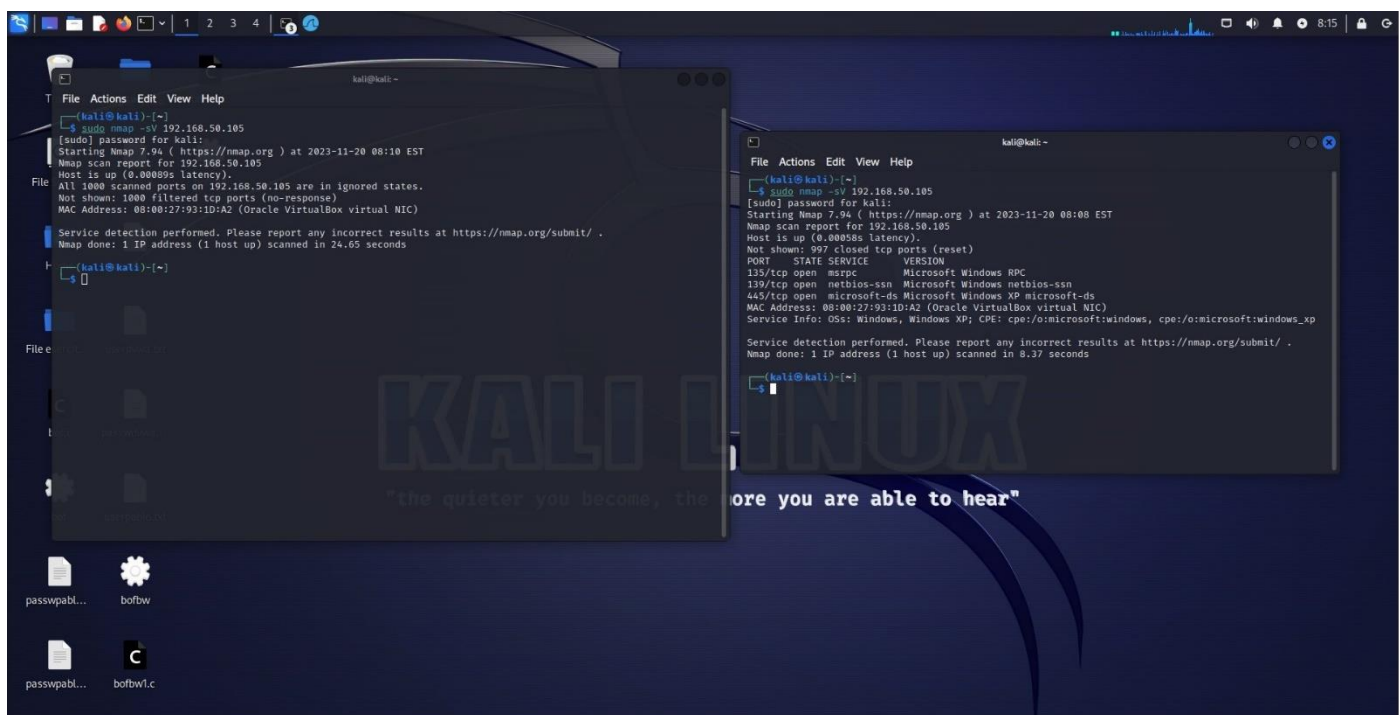
Effettuiamo la prima scansione con il firewall disattivato



Poi la seconda scansione con il firewall attivato



E mettiamo a confronto le due scansioni



Oltre alle normali informazioni che ci fornisce nmap (versione del programma, data e ora in cui è stata eseguita la scansione e il dispositivo su cui è stata effettuata), possiamo rilevare che in entrambi i casi l'host risulta online e il MAC Address fornito fa riferimento alla scheda di rete virtuale di Virtual Box.

**Possiamo invece notare che le risposte alle scansioni sono nettamente differenti:**

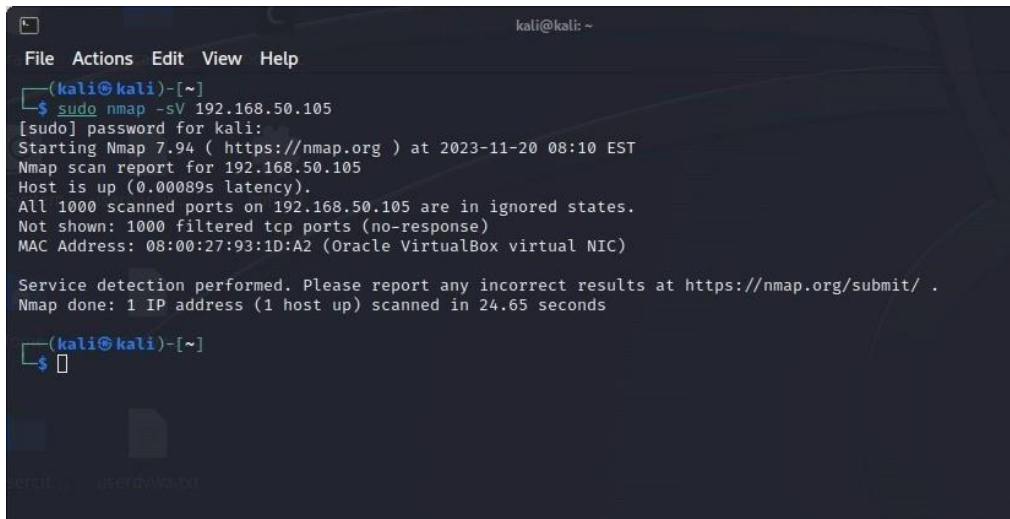
# Scansione con firewall disattivato

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ sudo nmap -sV 192.168.50.105  
[sudo] password for kali:  
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-20 08:08 EST  
Nmap scan report for 192.168.50.105  
Host is up (0.00058s latency).  
Not shown: 997 closed tcp ports (reset)  
PORT      STATE SERVICE      VERSION  
135/tcp   open  msrpc        Microsoft Windows RPC  
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn  
445/tcp   open  microsoft-ds Microsoft Windows XP microsoft-ds  
MAC Address: 08:00:27:93:1D:A2 (Oracle VirtualBox virtual NIC)  
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 8.37 seconds  
  
(kali@kali)-[~]  
$
```

## Risultati:

- Tempo di latenza per raggiungere l'host è di 0.00058 secondi
- 997 porte tcp sull'host scansionate risultano chiuse, mentre 3 risultano aperte  
135 (MSRPC Microsoft Remote Procedure Call), la porta utilizzata comunemente per la comunicazione tra client e server nel contesto delle chiamate di procedura remote implementato in modo specifico da Microsoft  
139 (NetBios-ssn), questo protocollo è utilizzato per la condivisione di risorse di rete, come file e stampanti, in ambienti basati su Microsoft Windows  
445 (Microsoft-ds), il protocollo samba che rende possibile la comunicazione tra sistemi operativi diversi su una stessa rete  
Queste porte ci forniscono informazioni dalle quali si può dedurre che il sistema operativo sulle quali sono attive sia Windows, presumibilmente XP (sulla riga della porta 445 è facilmente visibile e viene anche rilevato due righe più in basso dal "Service Info")
- Anche qui è stato rilevato 1 host attivo
- Il tempo di scansione questa volta è di 8,37 secondi

# Scansione con firewall attivato



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ sudo nmap -sV 192.168.50.105  
[sudo] password for kali:  
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-20 08:10 EST  
Nmap scan report for 192.168.50.105  
Host is up (0.00089s latency).  
All 1000 scanned ports on 192.168.50.105 are in ignored states.  
Not shown: 1000 filtered tcp ports (no-response)  
MAC Address: 08:00:27:93:1D:A2 (Oracle VirtualBox virtual NIC)  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 24.65 seconds  
  
(kali@kali)-[~]  
$
```

Risultati:

- Tempo di latenza per raggiungere l'host è di 0.000**89** secondi
- 1000 porte tcp sull'host scansionate (tcp = Transmission Control Protocol, protocollo di comunicazione). Tutte risultano come "ignored states", questo significa che non abbiamo ottenuto risposte significative dalle porte scansionate, nmap, dunque, non ha ricevuto alcuna risposta e non ha potuto determinare lo stato delle porte
- Ha rilevato 1 host attivo
- Il tempo di scansione è stato di 24,65 secondi

## Conclusioni

La prima scansione è più dettagliata, fornisce informazioni specifiche sullo stato delle porte e sui servizi in esecuzione sull'host. Mostra, inoltre, che l'host sembra eseguire un sistema operativo Windows (presumibilmente, come detto, XP)

La seconda scansione fornisce solo informazioni di base sullo stato dell'host (online) e sul tempo di latenza (nettamente più ampio come anche il tempo di scansione), ma senza entrare nei dettagli delle porte e dei servizi

Sicuramente tale differenza è dovuta allo stato del firewall. Normalmente quando è disattivato permette il libero passaggio del traffico attraverso tutte le porte, almeno attraverso quelle su cui i servizi sono in esecuzione.

Nel caso del firewall attivo nmap potrebbe non aver rilevato le porte aperte per due motivi: il primo è che potrebbero esserci delle regole del firewall che impediscono la risposta di queste porte, il secondo (avendo rilevato un tempo di scansione superiore rispetto alla scansione con il firewall disattivato) è che potrebbe anche essere presente il timeout per le risposte durante la scansione: se una porta non risponde entro un tempo limite nmap potrebbe considerarla chiusa o filtrata e passare alla successiva.