

CONSEGNA S9/L1

L'esercizio di oggi è verificare in che modo l'attivazione del Firewall impatta il risultato di una scansione dei servizi dall'esterno.

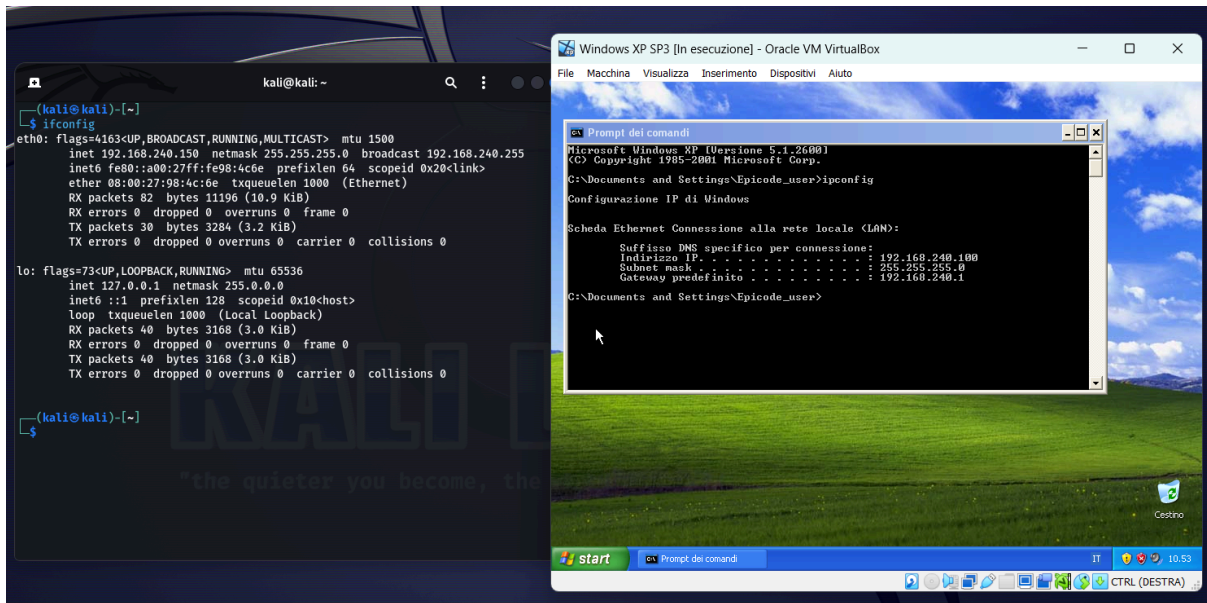
Per iniziare si apre **Kali** e **Windows XP** e si cambia l'**IP** delle due macchine.

Per *Kali* basterà aprire un terminale e usare il comando **sudo nano /etc/network/interfaces** mentre per *Windows XP* si dovrà premere **Start**, cliccare sul **Pannello di controllo**, recarsi nella sezione **"Rete e connessioni Internet"**, cliccare in basso su **"Connessioni di rete"**, fare **tasto destro** su **"Connessione alla rete locale (LAN)"** e cliccare su **"Proprietà"**, per poi selezionare il **protocollo internet (TCP/IP)** e inserire finalmente a mano l'IP.

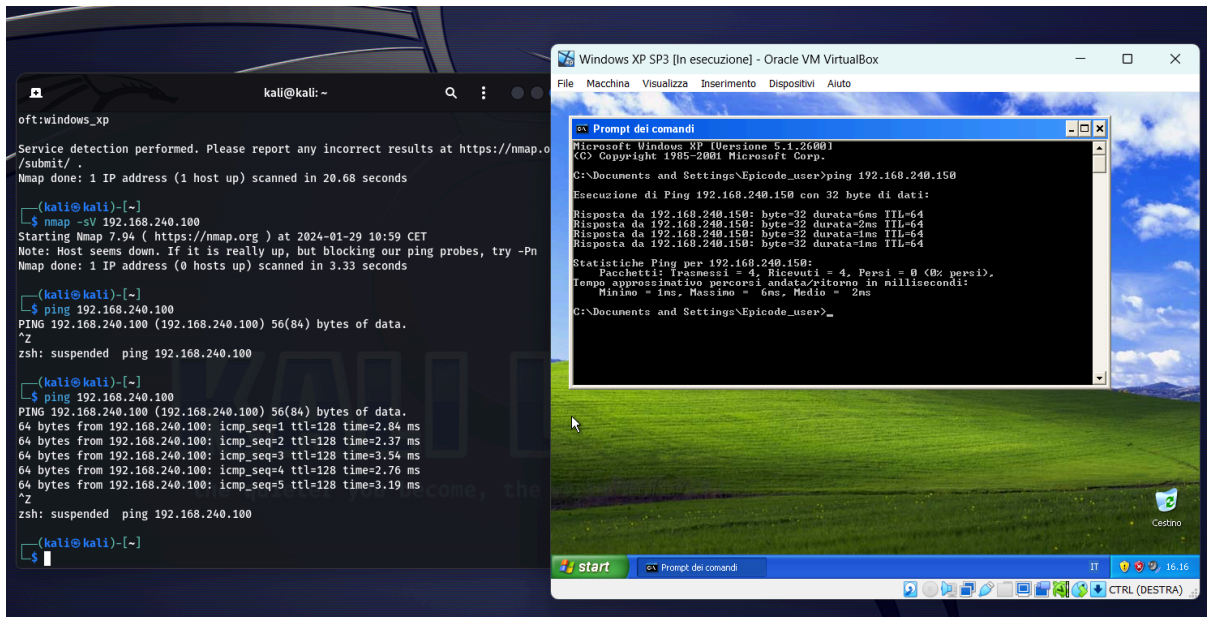
Gli IP da inserire sono:

- **192.168.240.150** per *Meta*
- **192.168.240.100** per *Windows XP*

Gli IP sono stati modificati correttamente, come da immagine



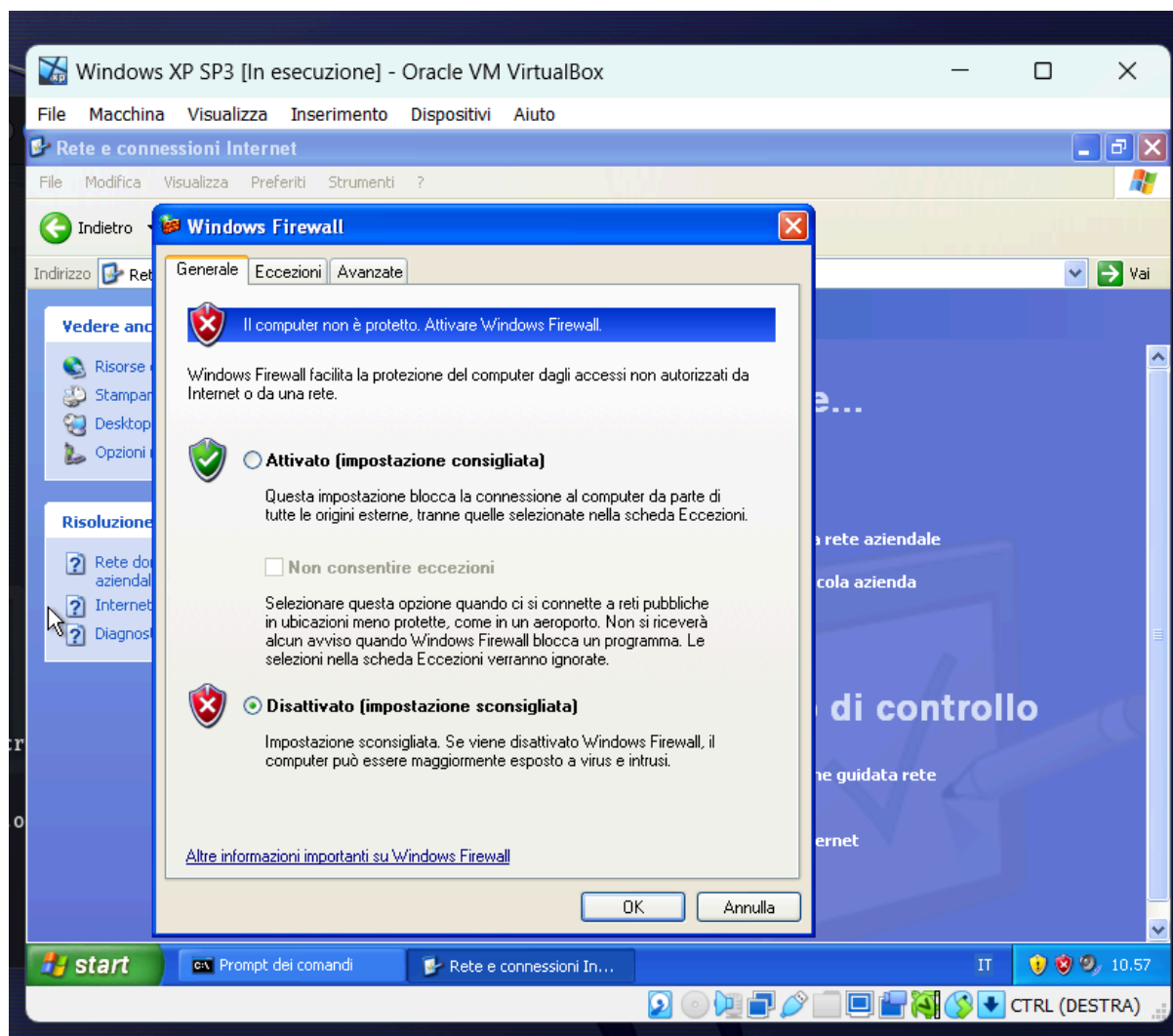
Ping funzionante, le due macchine comunicano correttamente.



Si fa partire la scansione con **nmap** per vedere la lista dei servizi attivi con lo **switch -sV**, in questo caso avendo il **firewall di Windows XP disabilitato**.

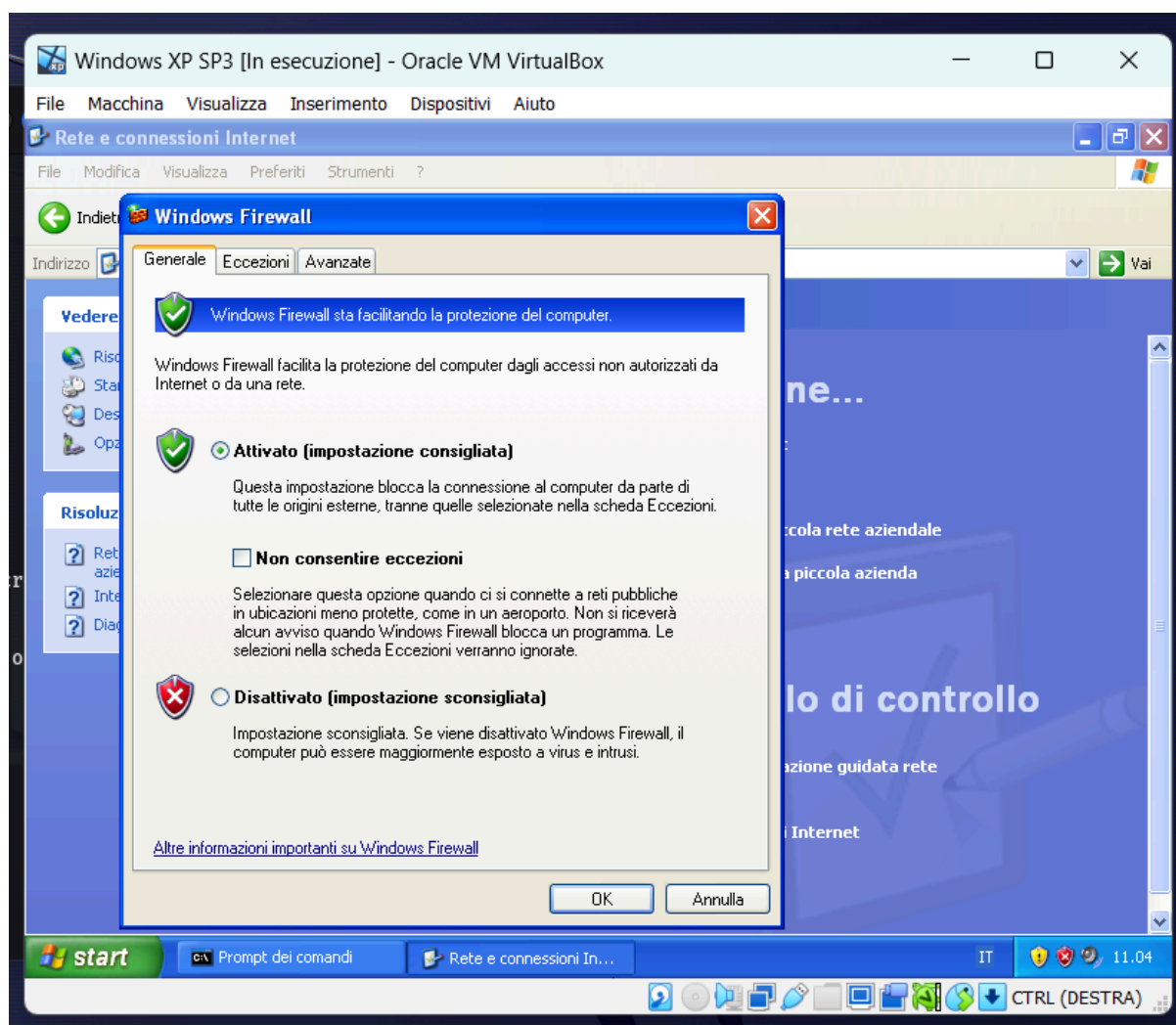
```
(kali@kali)-[~]
└─$ nmap -sV 192.168.240.100
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-29 10:51 CET
Nmap scan report for 192.168.240.100
Host is up (0.0028s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE        VERSION
135/tcp    open  msrpc          Microsoft Windows RPC
139/tcp    open  netbios-ssn    Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds   Microsoft Windows XP microsoft-ds
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 20.68 seconds
```



Il firewall è disattivato e infatti la scansione dei servizi attivi con nmap rivela **3 porte tcp aperte**, rispettivamente dei servizi **msrpc**, **netbios-ssn**, **microsoft-ds**.

Ora rifacciamo la stessa scansione con nmap però questa volta **abilitiamo il firewall di Windows XP**.



```
(kali@kali)-[~]
$ nmap -sV 192.168.240.100
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-29 10:59 CET
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.33 seconds
```

In questo caso il firewall abilitato **blocca tutte le connessioni esterne** su *Windows XP*,
tranne per quelle abilitate nella **scheda Eccezioni**.
Il nostro **nmap in ingresso** viene quindi **bloccato**, non permettendoci di vedere nessun
servizio attivo e vulnerabile sulla macchina.