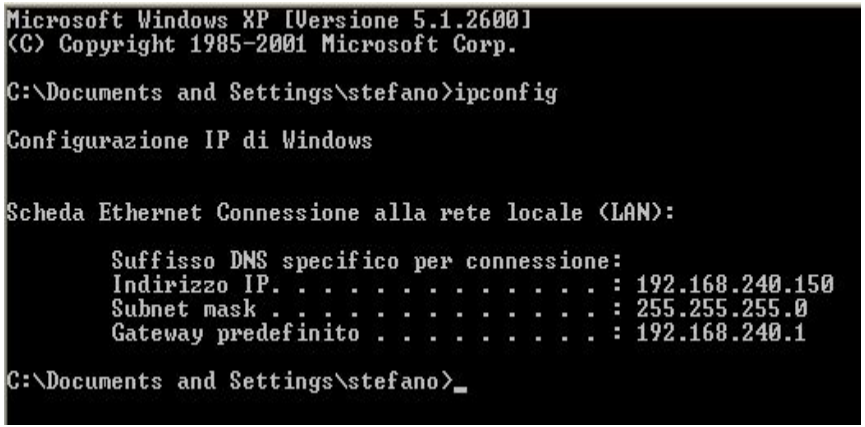
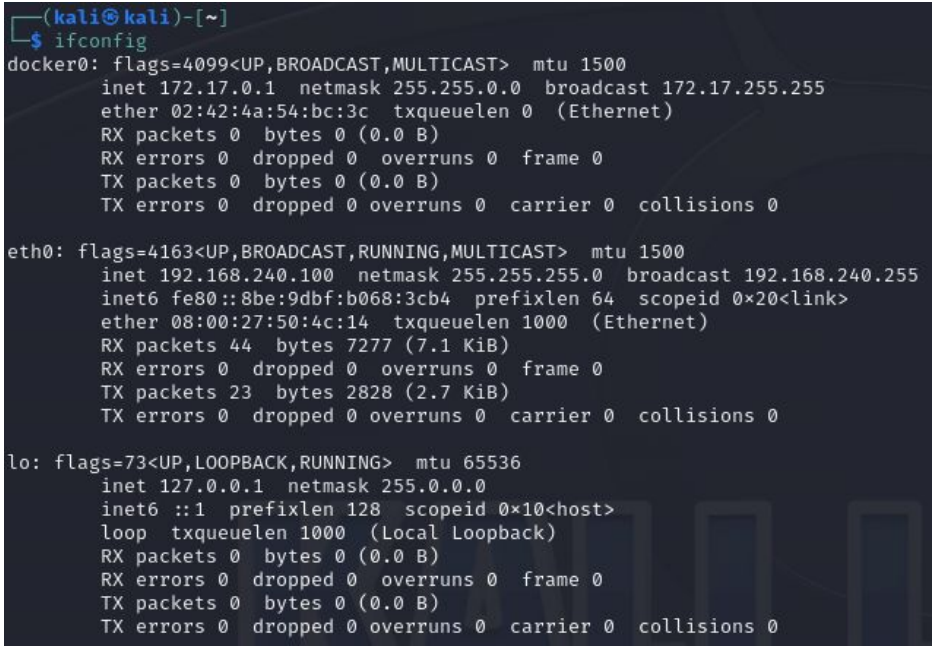
Nell’esercizio di oggi verificheremo come il firewall influisce su un potenziale attacco. Per eseguire questo test ci avvarremo di una macchina windows xp e di kali linux.
Cominciamo avviando le macchine e impostando gli indirizzi IP come richiesto dall’esercizio.





Avviamo poi la scansione di nmap con il firewall di windows spento. Come possiamo vedere dalla figura accanto la scansione viene effettuata senza problemi.

```
# Nmap 7.94SVN scan initiated Mon Feb  5 11:55:17 2024 as: nmap -sV -o "no fw scan"
192.168.240.150
Nmap scan report for 192.168.240.150
Host is up (0.00044s 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 at Mon Feb  5 11:55:37 2024 -- 1 IP address (1 host up) scanned in 20.79 seconds
```

A questo punto eseguiamo lo stesso procedimento con il firewall attivo. Come possiamo vedere la scansione in questo caso non ci fornisce risultati. Questo è dovuto al fatto che normalmente nmap usa un ping scan per effettuare la scansione delle porte, che viene bloccato di default dal firewall di windows. Questa tecnica non è molto affidabile poichè nmap non è in grado di capire se una porta è chiusa o filtrata, infatti ci suggerisce di provare a disabilitare il ping con il comando -Pn.

Da questo comprendiamo quanto può essere cruciale il ruolo del firewall, poiché non potendo acquisire informazioni sul target diventa molto difficile attaccarlo.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-05 15:19 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 3.12 seconds
```

```
# Nmap 7.94SVN scan initiated Mon Feb  5 12:02:08 2024 as: nmap -sV -o "fw scan"
192.168.240.150
# Nmap done at Mon Feb  5 12:02:12 2024 -- 1 IP address (0 hosts up) scanned in 3.19 seconds
```