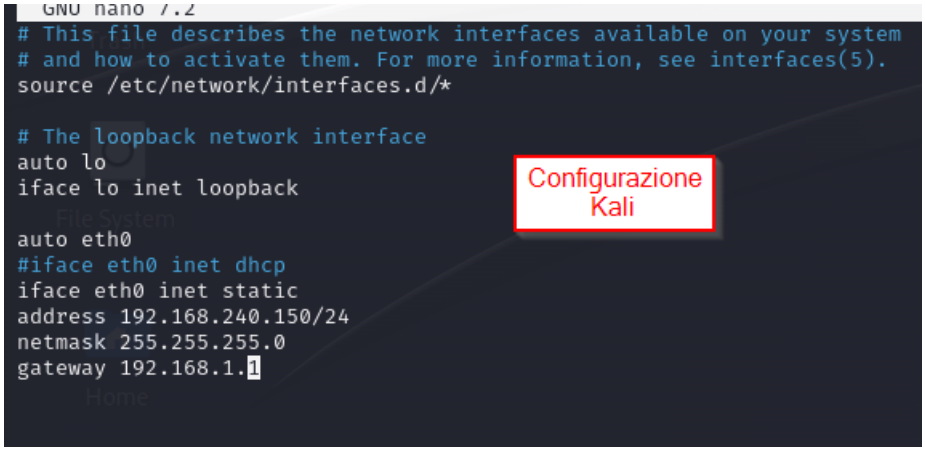
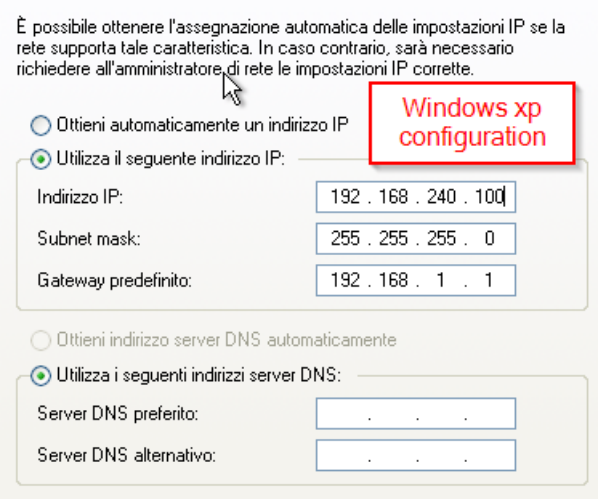
ESERCIZIO W18D1

L’esercizio ci porta a considerare le differenze di nmap scanning su windows xp con firewall e senza firewall. Configuriamo la rete dei due dispositivi, Kali e WIndoes xp, come requisito fondamentale.

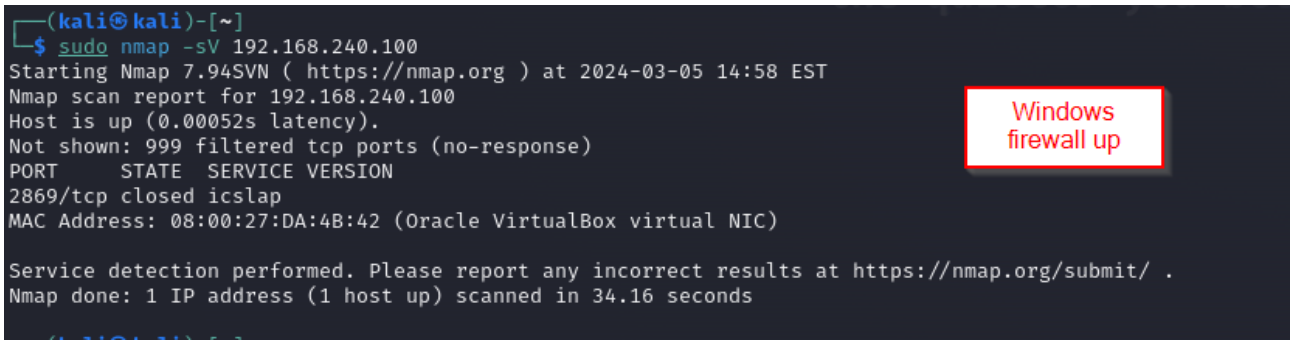
Configurazione rete

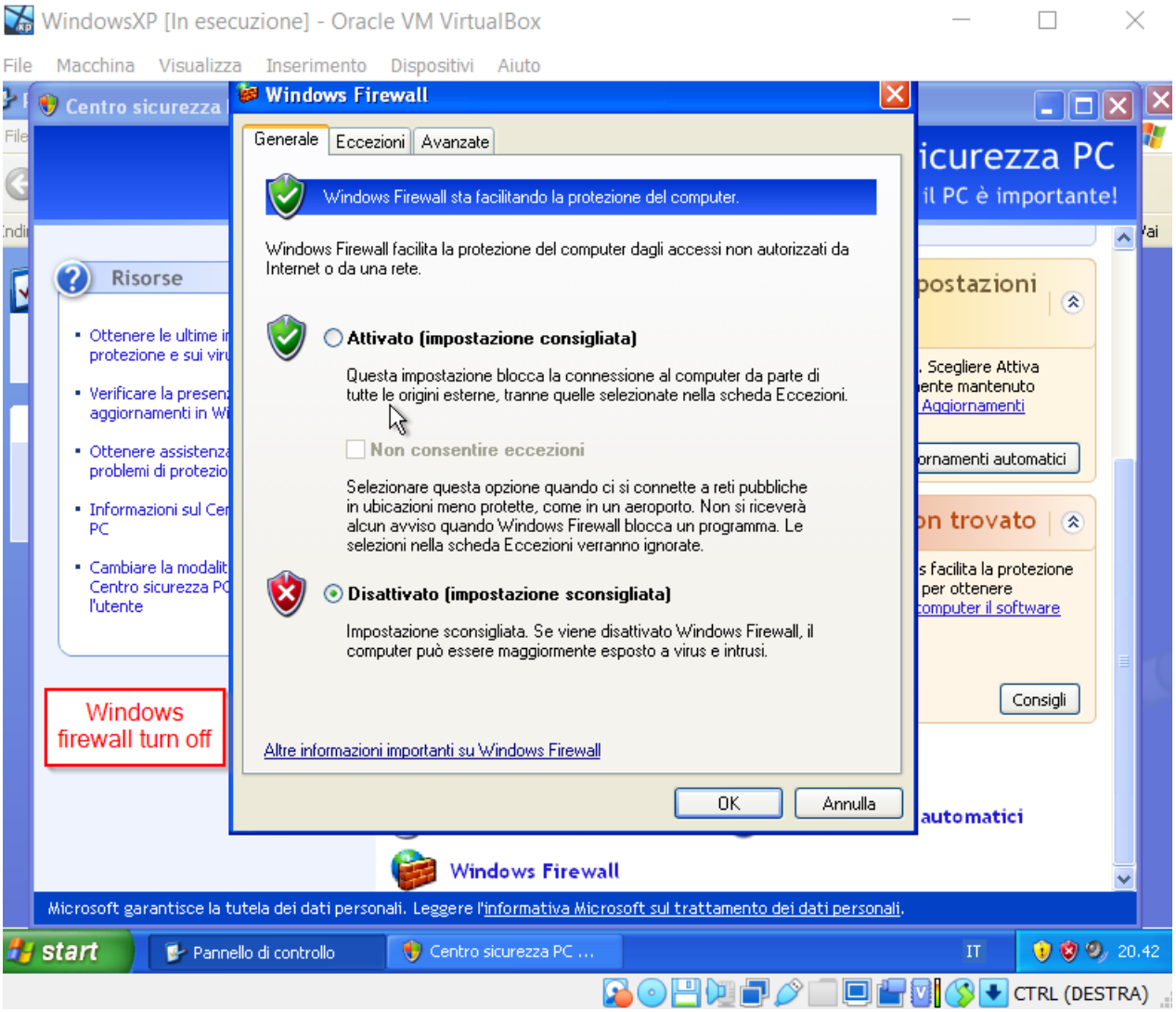




Scansione nmap con firewall e senza firewall

In base alla presenza o meno del firewall di Windows XP, avremo una certa differenza di banner catturati.





```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.240.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-05 14:52 EST
Nmap scan report for 192.168.240.100
Host is up (0.00054s 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:DA:4B:42 (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 21.82 seconds
```

no firewall
nmap