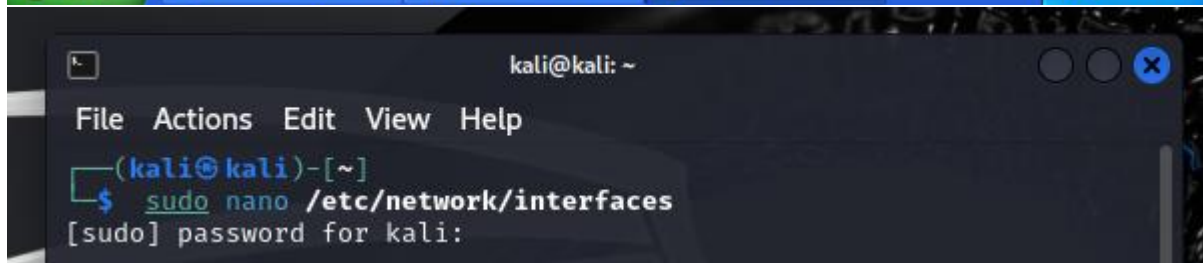
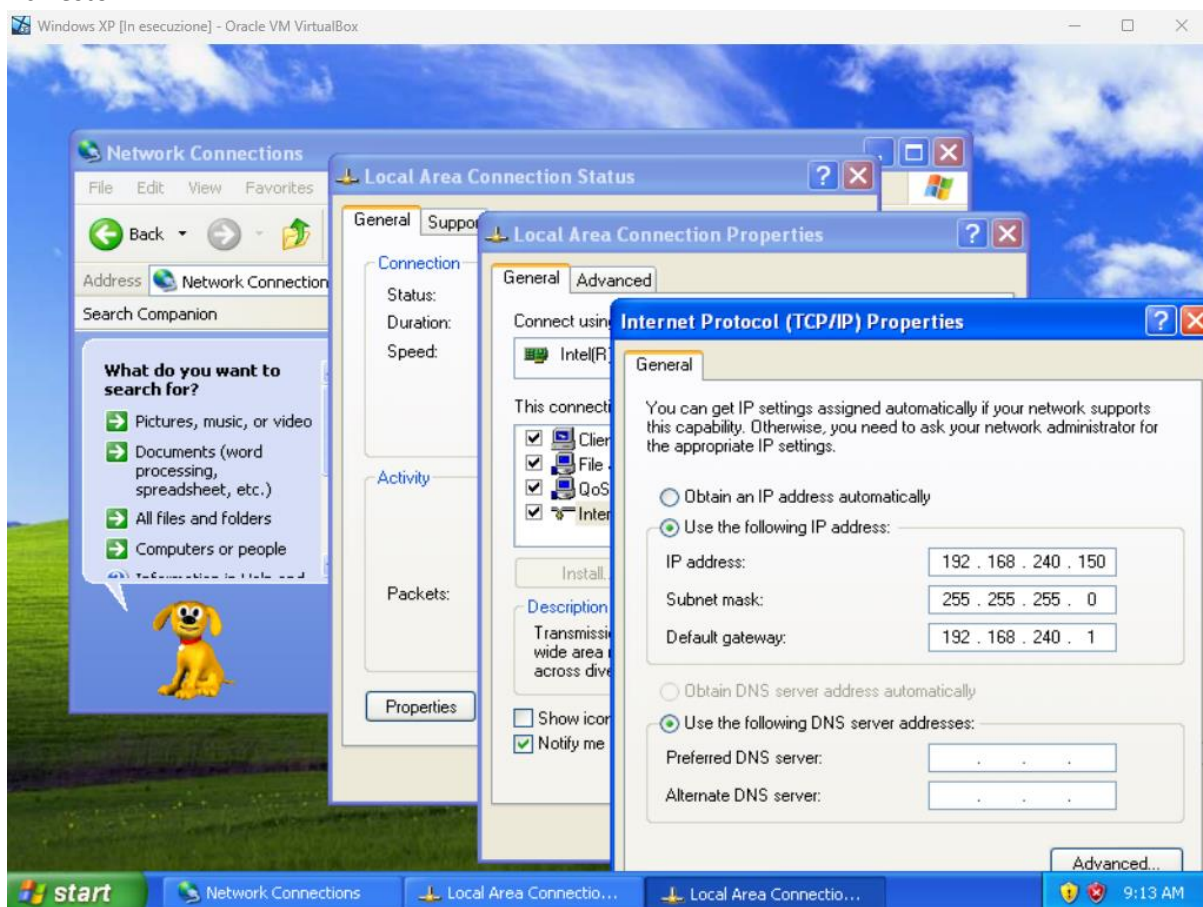


Per prima cosa, soddisfiamo i requisiti del laboratorio, impostando gli IP delle macchine come richiesto.



```
auto eth0
iface eth0 inet static
address 192.168.240.100
gateway 192.168.240.1
```

```
(kali@kali)-[~]
$ sudo /etc/init.d/networking restart
Restarting networking (via systemctl): networking.service.
```



Accertiamoci che il Firewall di Windows sia disattivato e lanciamo la scansione verso il nostro target con lo switch -sV. La scansione ci riporta 3 servizi in ascolto rispettivamente sulle porte TCP

135,139,445.

Security essentials

Security Center helps you manage your Windows security settings. To help protect your computer, make sure the three security essentials are marked ON. If the settings are not ON, follow the recommendations. To return to the Security Center later, open Control Panel.

[What's new in Windows to help protect my computer?](#)

 **Firewall** OFF 

Windows detects that your computer is not currently protected by a firewall. Click Recommendations to learn how to fix this problem. [How does a firewall help protect my computer?](#)

Note: Windows does not detect all firewalls.

Recommendations...

```
(kali㉿kali)-[~]
$ nmap -sV 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 04:29 EDT
Nmap scan report for 192.168.240.150
Host is up (0.00084s 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 a
t https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.35 seconds
```

Attiviamo il Firewall di Windows XP e procediamo nuovamente alla scansione.

Security essentials

Security Center helps you manage your Windows security settings. To help protect your computer, make sure the three security essentials are marked ON. If the settings are not ON, follow the recommendations. To return to the Security Center later, open Control Panel.

[What's new in Windows to help protect my computer?](#)



```
(kali㉿kali)-[~]  
$ nmap -sV 192.168.240.150  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 04:30 EDT  
Note: Host seems down. If it is really up, but blocking our ping p  
robes, try -Pn  
Nmap done: 1 IP address (0 hosts up) scanned in 3.08 seconds
```

Il risultato della scansione ci riporta che la macchina o non è accesa, oppure se è accesa sta bloccando l'host discovery di nmap. Ci consiglia quindi di provare con il parametro `-Pn`. Questo accade perché il Firewall sta bloccando il traffico in entrata con protocollo ICMP (il ping). Proviamo a sfruttare lo switch `-Pn` per evitare il ping e passare direttamente alla scansione dei servizi.

```
(kali㉿kali)-[~]  
$ nmap -sV 192.168.240.150 -Pn  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 04:31 EDT  
Nmap scan report for 192.168.240.150  
Host is up.  
All 1000 scanned ports on 192.168.240.150 are in ignored states.  
Not shown: 1000 filtered tcp ports (no-response)  
  
Service detection performed. Please report any incorrect results a  
t https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 222.76 seconds
```

Utilizzando lo switch `-Pn`, la scansione salterà il ping e passerà alla service discovery. A questo giro tutte le porte sembrano filtrate, ovvero non hanno risposto alle richieste dello scanner. L'abilitazione del Firewall sta di fatto bloccando la scansione dall'esterno verso i servizi attivi sulla macchina Windows XP. Di conseguenza possiamo dire che il Firewall sta preventivamente riducendo rischi di attacchi dall'esterno, rendendo inaccessibili dall'esterno i servizi sulle porte 135,139,445 TCP.