

CS1803

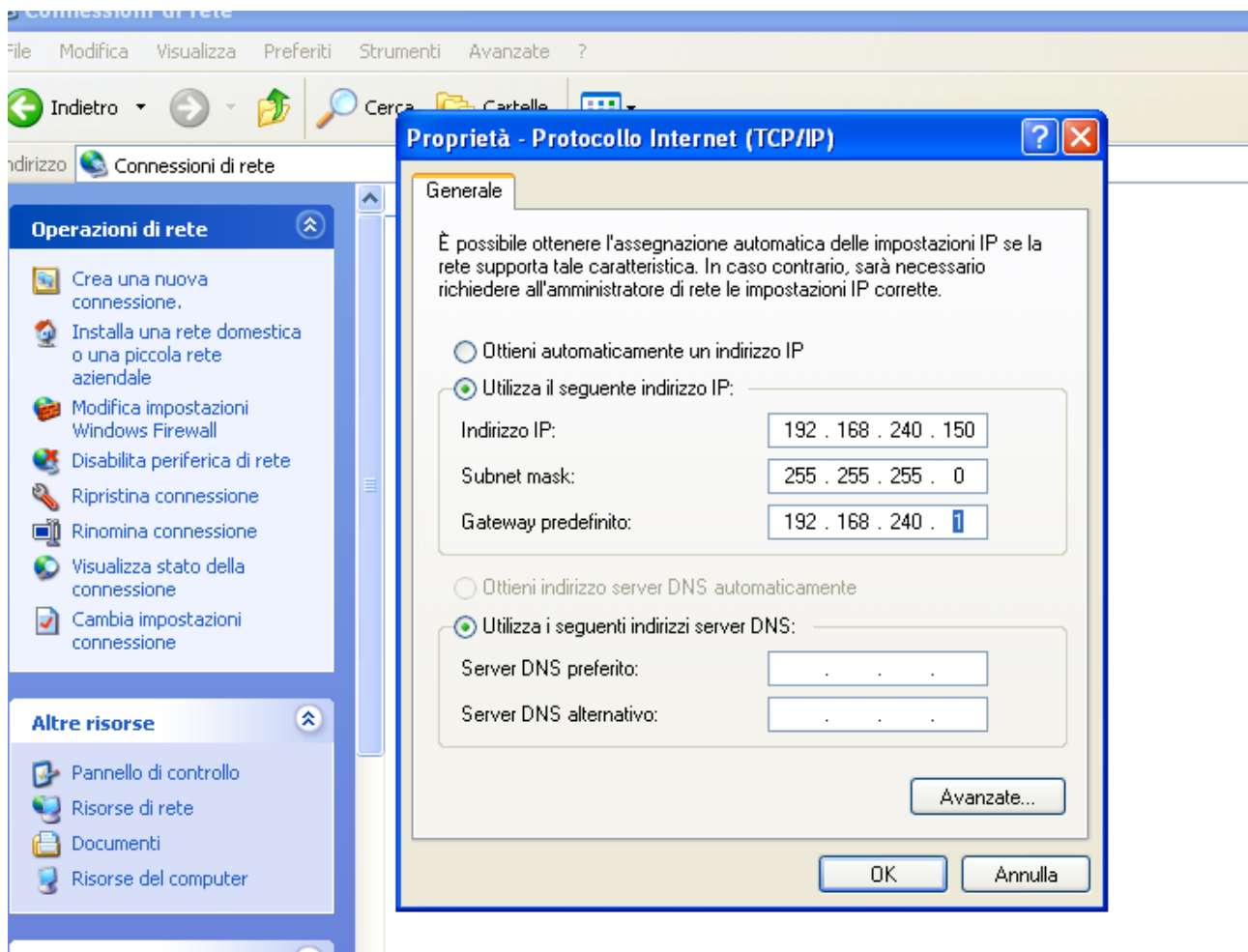
Per prima cosa impostiamo gli indirizzi IP richiesti

```
GNU nano 7.2 /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 192.168.240.100/24
gateway 192.168.240.1
```



Una volta che ci siamo accertati che il firewall sia disattivato facciamo una scansione nmap verso il target win xp con lo switch -sV

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ nmap -sV 192.168.240.150  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 07:21 EDT  
Nmap scan report for 192.168.240.150  
Host is up (0.00088s 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 20.56 seconds  
  
(kali@kali)-[~]  
$
```

Come possiamo vedere la scansione ci riporta 3 servizi in ascolto rispettivamente sulle porte TCP 135,139,445.

Se proviamo ad attivare il firewall è a rifare lo stesso tipo di scansione

```
(kali@kali)-[~]  
$ nmap -sV 192.168.240.150  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 07:24 EDT  
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 3.08 seconds  
  
(kali@kali)-[~]  
$ nmap -sV -Pn 192.168.240.150  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 07:24 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 at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 216.63 seconds  
  
(kali@kali)-[~]  
$
```

Il risultato della scansione ci riporta che la macchina o non è accesa, oppure se è accesa sta bloccando l'host discovery di nmap.

Mentre se proviamo lo switch -Pn, come ci suggerisce, il risultato è che tutte le porte sembrano filtrate, quindi bloccate dal firewall