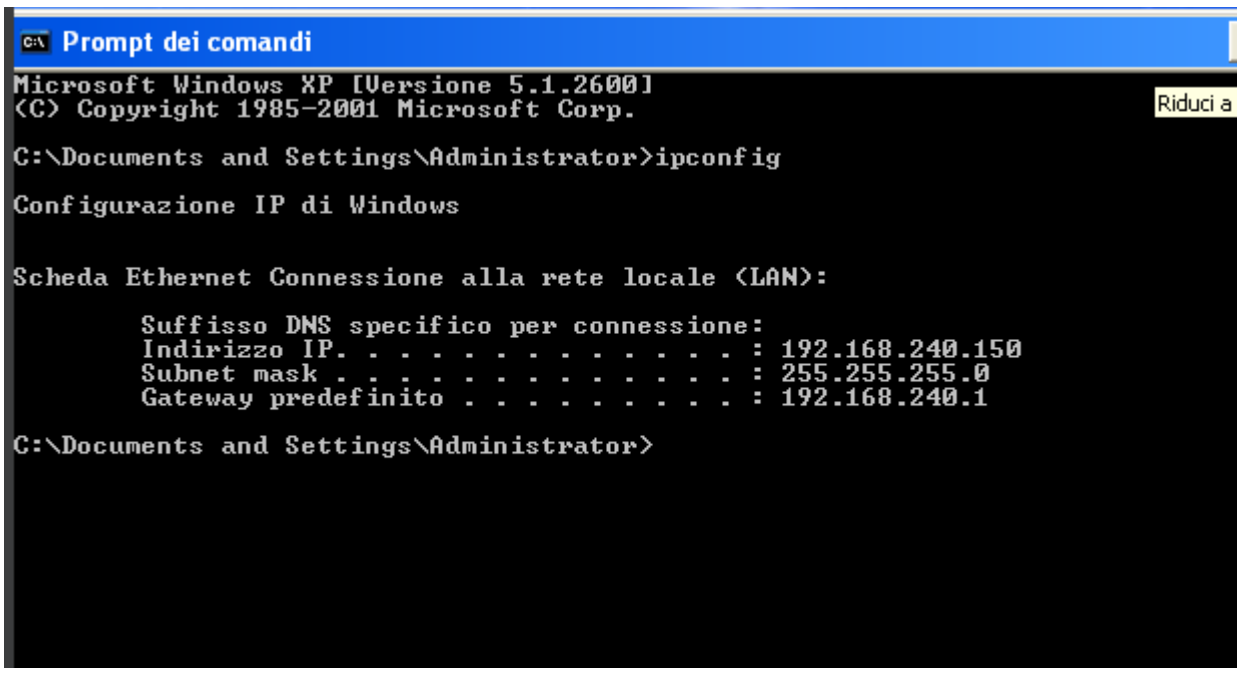
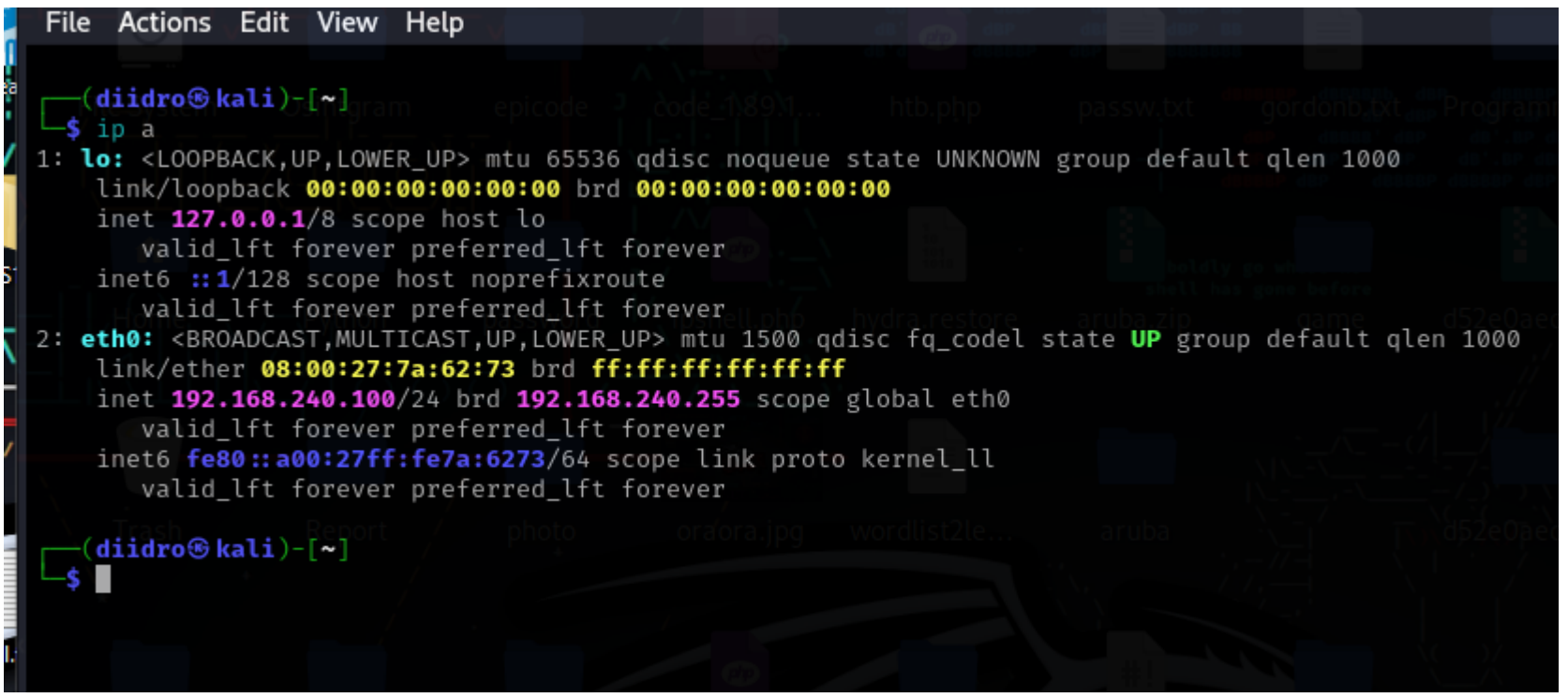
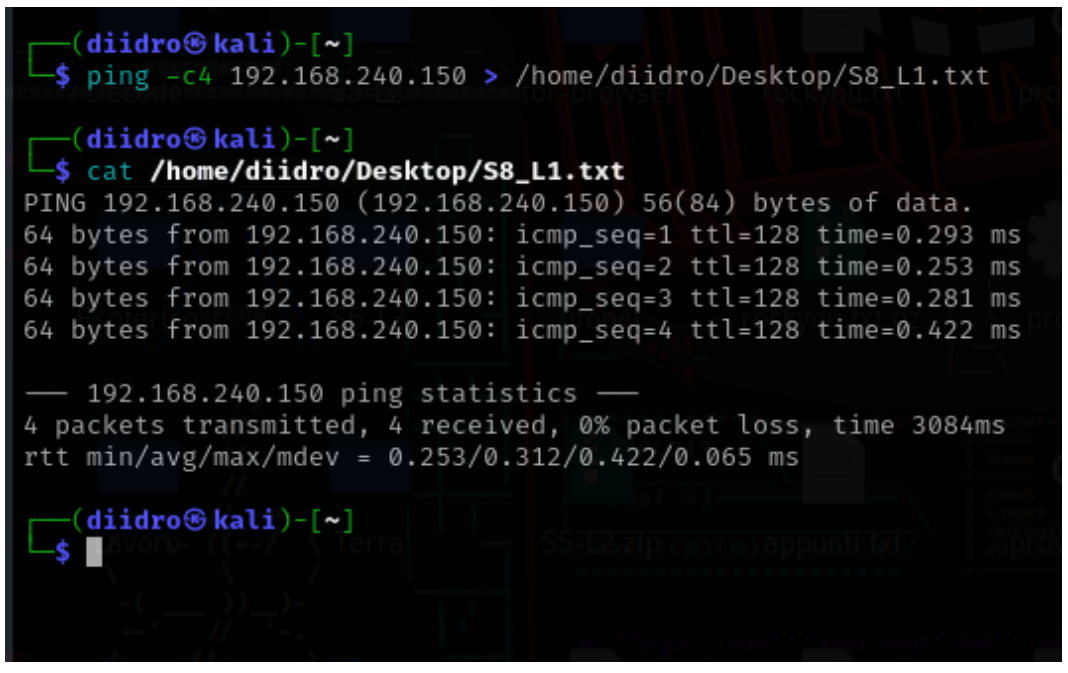
S9-L1

Cambiamo gli IP





Prova di ping

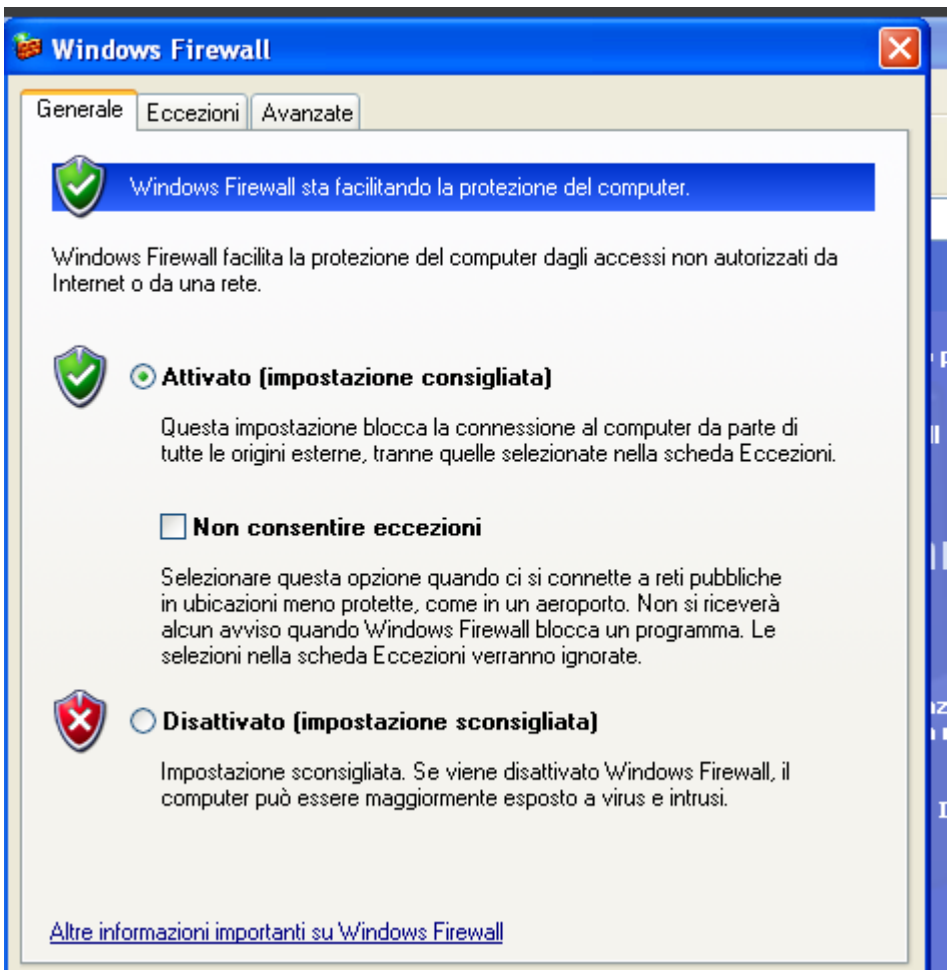


Spegnamo il Firewall

Facciamo lo scan

```
┌──(diidro㉿kali)-[~]
└─$ nmap -sV 192.168.240.150 >> /home/diidro/Desktop/S8_L1.txt

┌──(diidro㉿kali)-[~]
└─$ cat /home/diidro/Desktop/S8_L1.txt
PING 192.168.240.150 (192.168.240.150) 56(84) bytes of data.
64 bytes from 192.168.240.150: icmp_seq=1 ttl=128 time=0.293 ms
64 bytes from 192.168.240.150: icmp_seq=2 ttl=128 time=0.253 ms
64 bytes from 192.168.240.150: icmp_seq=3 ttl=128 time=0.281 ms
64 bytes from 192.168.240.150: icmp_seq=4 ttl=128 time=0.422 ms

── 192.168.240.150 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3084ms
rtt min/avg/max/mdev = 0.253/0.312/0.422/0.065 ms
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 08:31 EDT
Nmap scan report for 192.168.240.150
Host is up (0.00061s 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 20.61 seconds
```

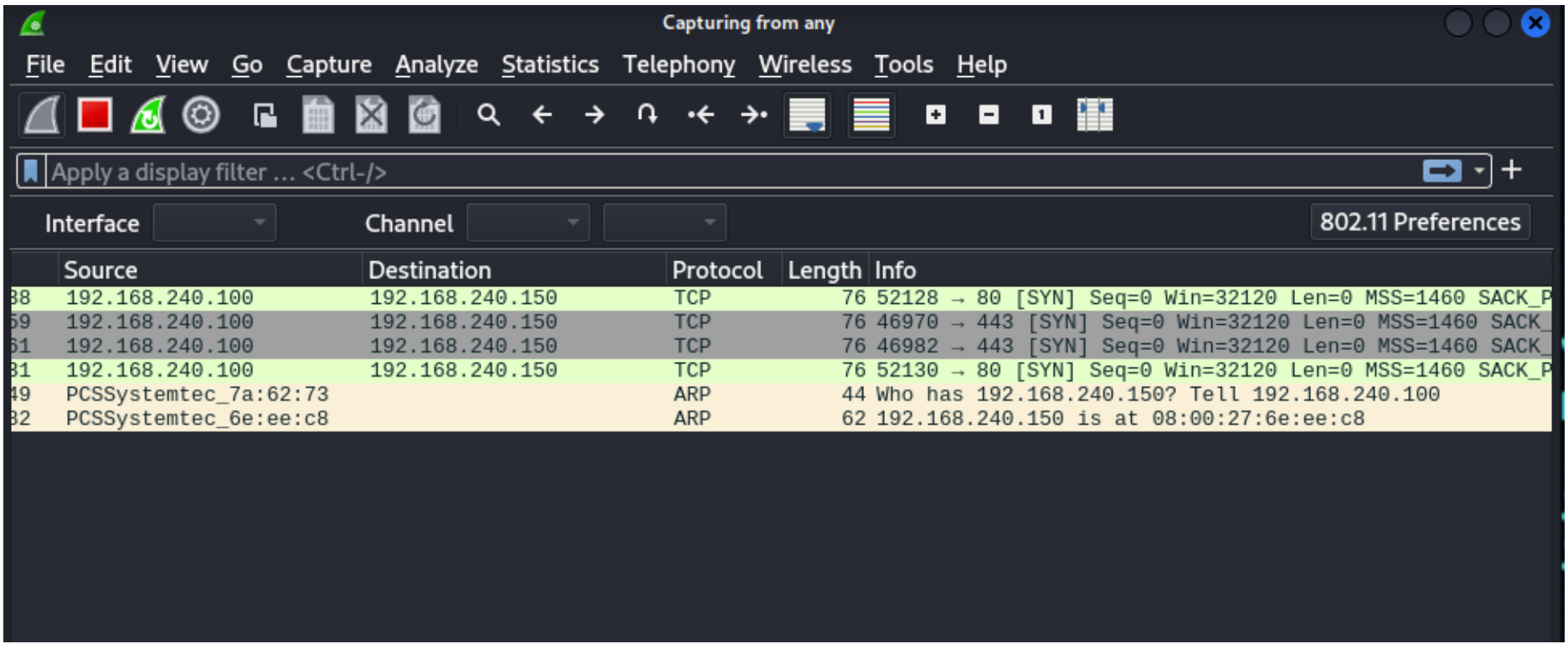
Attiviamo il firewall



Riproviamo lo scan

```
┌──(diidro㉿kali)-[~]
└─$ nmap -sV 192.168.240.150 >> /home/diidro/Desktop/S8_L1.txt

┌──(diidro㉿kali)-[~]
└─$ cat /home/diidro/Desktop/S8_L1.txt
PING 192.168.240.150 (192.168.240.150) 56(84) bytes of data.
64 bytes from 192.168.240.150: icmp_seq=1 ttl=128 time=0.293 ms
64 bytes from 192.168.240.150: icmp_seq=2 ttl=128 time=0.253 ms
64 bytes from 192.168.240.150: icmp_seq=3 ttl=128 time=0.281 ms
64 bytes from 192.168.240.150: icmp_seq=4 ttl=128 time=0.422 ms

── 192.168.240.150 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3084ms
rtt min/avg/max/mdev = 0.253/0.312/0.422/0.065 ms


Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 08:31 EDT
Nmap scan report for 192.168.240.150
Host is up (0.00061s 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 20.61 seconds


Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 08:35 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 3.10 seconds

┌──(diidro㉿kali)-[~]
└─$
```

Considerazioni



Da wireshark vediamo come il three hand shake non va a buon fine, manca l'ACK.
Le porte tramite le quali ha tentato sono la 80 e 443, rispettivamente http ed https, poichè, probabilmente, alcuni firewall sono configurati per consentire il traffico su porte standard come 80 e 443, ma bloccare altre porte.
Nmap potrebbe provare a inviare pacchetti a queste porte per verificare se sono aperte, anche se il firewall è attivo.