

# S9-L1

## Cambiamo gli IP

```
C:\ Prompt dei comandi
Microsoft Windows XP [Versione 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>ipconfig

Configurazione IP di Windows

Scheda Ethernet Connessione alla rete locale (LAN):

    Suffisso DNS specifico per connessione:
    Indirizzo IP. . . . . : 192.168.240.150
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . : 192.168.240.1

C:\Documents and Settings\Administrator>
```

```
File Actions Edit View Help

(diidro@kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:7a:62:73 brd ff:ff:ff:ff:ff:ff
    inet 192.168.240.100/24 brd 192.168.240.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe7a:6273/64 scope link proto kernel_ll
        valid_lft forever preferred_lft forever

(diidro@kali)-[~]
$
```

## Prova di ping

```
(diidro@kali)-[~]
$ ping -c4 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

(diidro@kali)-[~]
$
```

## Spegnamo il Firewall



Facciamo lo scan

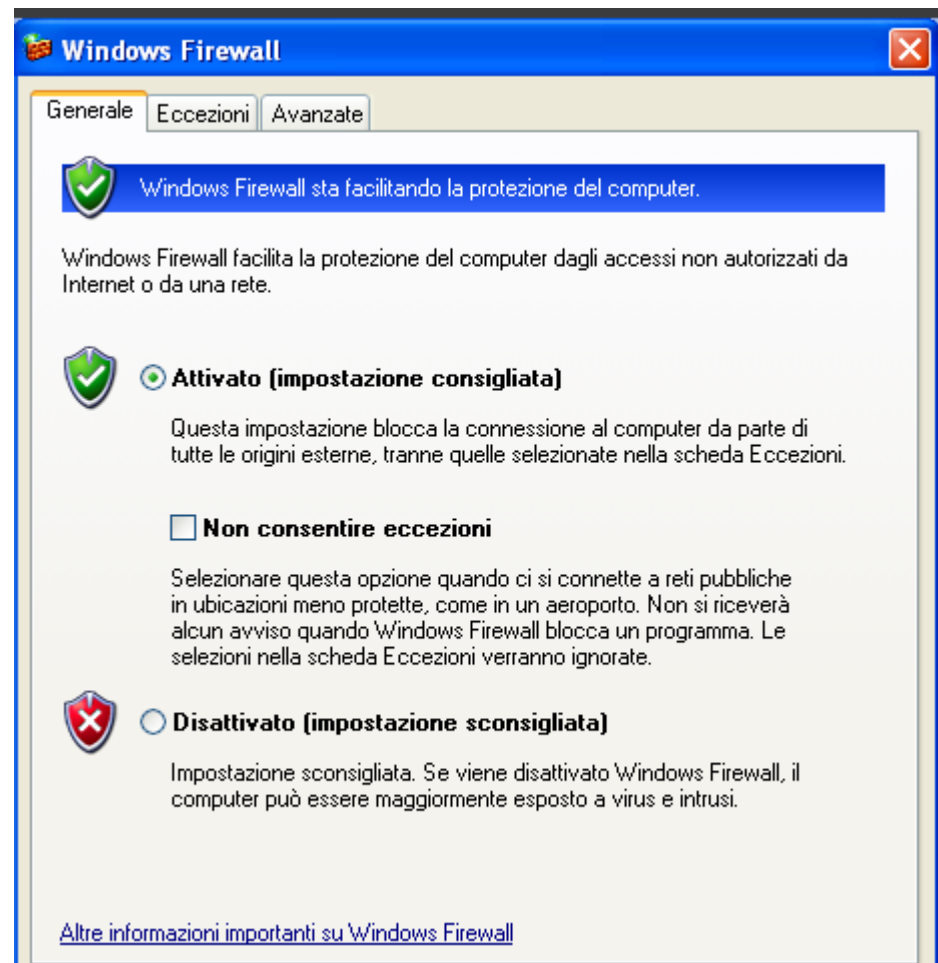
```
(diidro@kali)-[~]
$ nmap -sV 192.168.240.150 >> /home/diidro/Desktop/S8_L1.txt

(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
```

Considerazioni

	Source	Destination	Protocol	Length	Info
38	192.168.240.100	192.168.240.150	TCP	76	52128 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_P
59	192.168.240.100	192.168.240.150	TCP	76	46970 → 443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_P
61	192.168.240.100	192.168.240.150	TCP	76	46982 → 443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_P
81	192.168.240.100	192.168.240.150	TCP	76	52130 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_P
49	PCSSystemtec_7a:62:73		ARP	44	Who has 192.168.240.150? Tell 192.168.240.100
82	PCSSystemtec_6e:ee:c8		ARP	62	192.168.240.150 is at 08:00:27:6e:ee:c8

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.