

# S9L1

Come prima cosa andiamo a modificare l'indirizzo ip della macchina.

```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.240.100 netmask 255.255.255.0 broadcast 0.0.0.0
    inet6 fd00::bf4c:6994:1621:7b38 prefixlen 64 scopeid 0x0<global>
    inet6 fd00::a00:27ff:fec6:7684 prefixlen 64 scopeid 0x0<global>
    inet6 fe80::a00:27ff:fec6:7684 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:c6:76:84 txqueuelen 1000 (Ethernet)
    RX packets 4626 bytes 3763405 (3.5 MiB)
    RX errors 0 dropped 332 overruns 0 frame 0
    TX packets 3161 bytes 602293 (588.1 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 240 (240.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Una volta fatto ciò, andiamo ad effettuare prima una scansione sulla macchina windows xp con il firewall disattivato e dopo con il firewall attivato.

```
# nmap -sV -oN reportnmap.txt 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-05 16:21 CET
Nmap scan report for 192.168.240.150
Host is up (0.00013s 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: 08:00:27:6E:E0:8E (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 8.44 seconds

```
(root@kali)-[/home/gerardo]
```

```
# ls
```

```
Desktop    Downloads  Pictures   Templates  flag.txt      reportnmap    users.txt.bk
Documents  Music      Public     Videos    kali-autopilot reportnmap.txt zqpnskls.jpeg
```

```
(root@kali)-[/home/gerardo]
```

```
# nmap -sV -oN reportnmap.txt 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-05 16:23 CET
Nmap scan report for 192.168.240.150
Host is up (0.00028s latency).
All 1000 scanned ports on 192.168.240.150 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:6E:E0:8E (Oracle VirtualBox virtual NIC)
```

Come possiamo notare nella prima parte **nmap** ci da informazioni sulle porte, su i servizi e le versioni di quest'ultimi.

Nella seconda parte dove il firewall è acceso non ci da nulla di tutto questo, perchè va a bloccare le **richieste di scansione** di nmap.