# PROGETTO S9/L1

**SCOPO:s Verificare in che modo l'attivazione del Firewall impatta il risultato di una scanzione dei servizi dall'esterno.E per fare questo, dobbiamo fare la scanzione usando lo strumento "nmap" della macchina windows XP con Firewall attivato e con Firewall disattivato,Trovare le eventuali differenze e motivarle.**

Come prima cosa cerchiamo capire che cos'è windows xp e cos'è nmap? .

### 1-) Windows XP

È un systema d'exploitazione sviluppato da Microsoft,è stato lanciato nel 2001 ed è stato ampiamente utilizzato in tutto il mondo. Lo usiamo come macchina vulnerabile per lanciare diversi attachi e questo perché non riceve più aggiornamento di sicurezza di Microsoft da Aprile 2014.

### 2-) Nmap

Nmap(Network Mapper),è un strumento di scanzione di rete open source utilizzata per esaminare la sicurezza di un computer o di una rete.è progettato per scoprire host e servizi in una rete,identificare i dispositivi e determinare quali servizi e porte sono in esecuzione su tali dispositivi.

### 3-) Fase Applicativa

Abbiamo come prima cosa cambiato l'ip di windows xp e l'ip di kali linux inserendo quello richiesto nell'esercizio. Poi abbiamo verificato che il Firewall di windows xp sia disattivato come possiamo vedere sulle schermate seguente:

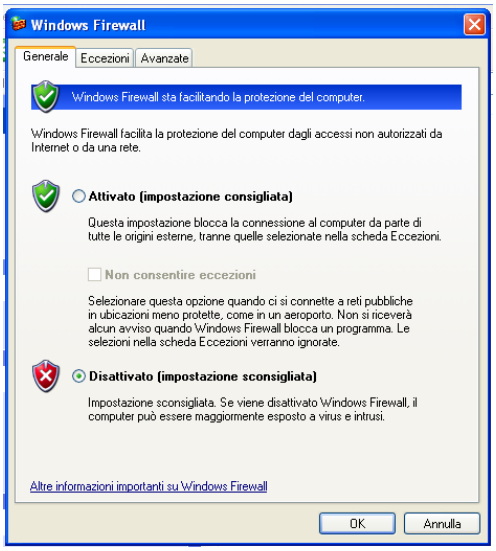
# PROGETTO S9/L1

```
┌──(georgesf㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.240.100  netmask 255.255.255.0  broadcast 192.168.240.25
5
        inet6 fe80::a00:27ff:fe3c:d210  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:3c:d2:10  txqueuelen 1000  (Ethernet)
        RX packets 1790  bytes 124191 (121.2 KiB)
        RX errors 0  dropped 553  overruns 0  frame 0
        TX packets 3580  bytes 261752 (255.6 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 4538  bytes 254766 (248.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4538  bytes 254766 (248.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Dopo ho fatto il ping per vedere se pingavano le macchine tra di loro ecco il risultato:

```
┌──(georgesf㉿kali)-[~]
└─$ ping 192.168.240.150
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=1.32 ms
64 bytes from 192.168.240.150: icmp_seq=2 ttl=128 time=0.473 ms
64 bytes from 192.168.240.150: icmp_seq=3 ttl=128 time=1.38 ms
64 bytes from 192.168.240.150: icmp_seq=4 ttl=128 time=1.40 ms
64 bytes from 192.168.240.150: icmp_seq=5 ttl=128 time=1.44 ms
64 bytes from 192.168.240.150: icmp_seq=6 ttl=128 time=1.35 ms
64 bytes from 192.168.240.150: icmp_seq=7 ttl=128 time=1.12 ms
^C
── 192.168.240.150 ping statistics ──
7 packets transmitted, 7 received, 0% packet loss, time 6015ms
rtt min/avg/max/mdev = 0.473/1.211/1.436/0.316 ms
```




Dopo questa verificazione abbiamo lanciato la scanzione e ottenuto il risultato seguente:

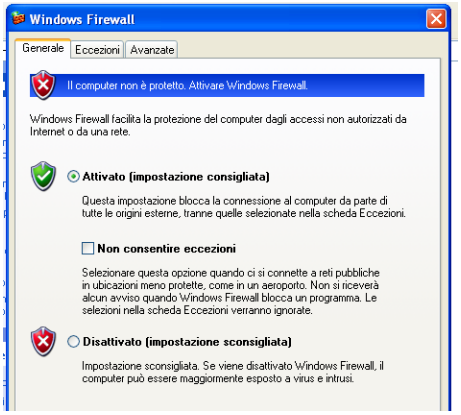
# PROGETTO S9/L1

```
┌──(georgesf㉿kali)-[~]
└─$ nmap -sV 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-05 15:38 CET
Nmap scan report for 192.168.240.150
Host is up (0.00018s 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://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.44 seconds
```

Come possiamo vedere abbiamo 3 porte aperti.

Dopo questo abbiamo attivato il Firewall come possimo vedere sull'imagine seguente:




Dopo questo abbiamo di nuovo lanciato la scanzione e ottenuto il risultato seguente.

```
┌──(georgesf㉿kali)-[~]
└─$ nmap -sV 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-05 15:46 CET
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 3.11 seconds

┌──(georgesf㉿kali)-[~]
└─$ nmap -Pn 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-05 15:47 CET
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)

Nmap done: 1 IP address (1 host up) scanned in 214.50 seconds
```

Come possiamo vedere non ci sono più porte aperte. Dopo aver utilizzato -sV e che non riusciamo a trovare porte aperte. Il compilater ci ha chiesto di provare -Pn quello che abbiamo fatto ma anche così non riusciamo ad avere porte aperte.

# PROGETTO S9/L1

Quindi in conclusione se il Firewall è attivo tutte le porte rimangono chiuse ma se è disattivato la scanzione ci da delle porte aperte.

La causa del risultato può essere dovuto al fatto che il firewall non per traffico in ingresso.