Oggi andremo ad analizzare come, l'attivazione e la disattivazione del firewall di xp influisca sulla scansione dei servizi attivi sulla macchina effettutata con nmap.

Dopo aver settato gli ip come richiesto dalla traccia,effettuo una scansione con il firewall disattivato e, come si evince dallo screen, i servizi attivi sono 3:

```
┌──(alessio㉿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=1.04 ms
64 bytes from 192.168.240.150: icmp_seq=2 ttl=128 time=0.641 ms
^C
── 192.168.240.150 ping statistics ──
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.641/0.838/1.035/0.197 ms

┌──(alessio㉿kali)-[~]
└─$ nmap -sV 192.168.240.150
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-20 14:11 CET
Nmap scan report for 192.168.240.150
Host is up (0.0014s 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 8.10 seconds

┌──(alessio㉿kali)-[~]
└─$
```

```
┌──(alessio㉿kali)-[~]
└─$ nmap -sV 192.168.240.150 -o scanxp.txt
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-20 14:19 CET
Nmap scan report for 192.168.240.150
Host is up (0.60s 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 9.09 seconds

┌──(alessio㉿kali)-[~]
└─$ cat scanxp.txt
# Nmap 7.93 scan initiated Mon Mar 20 14:19:24 2023 as: nmap -sV -o scanxp.txt 192.168.240.150
Nmap scan report for 192.168.240.150
Host is up (0.60s 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 at Mon Mar 20 14:19:33 2023 -- 1 IP address (1 host up) scanned in 9.09 seconds
```

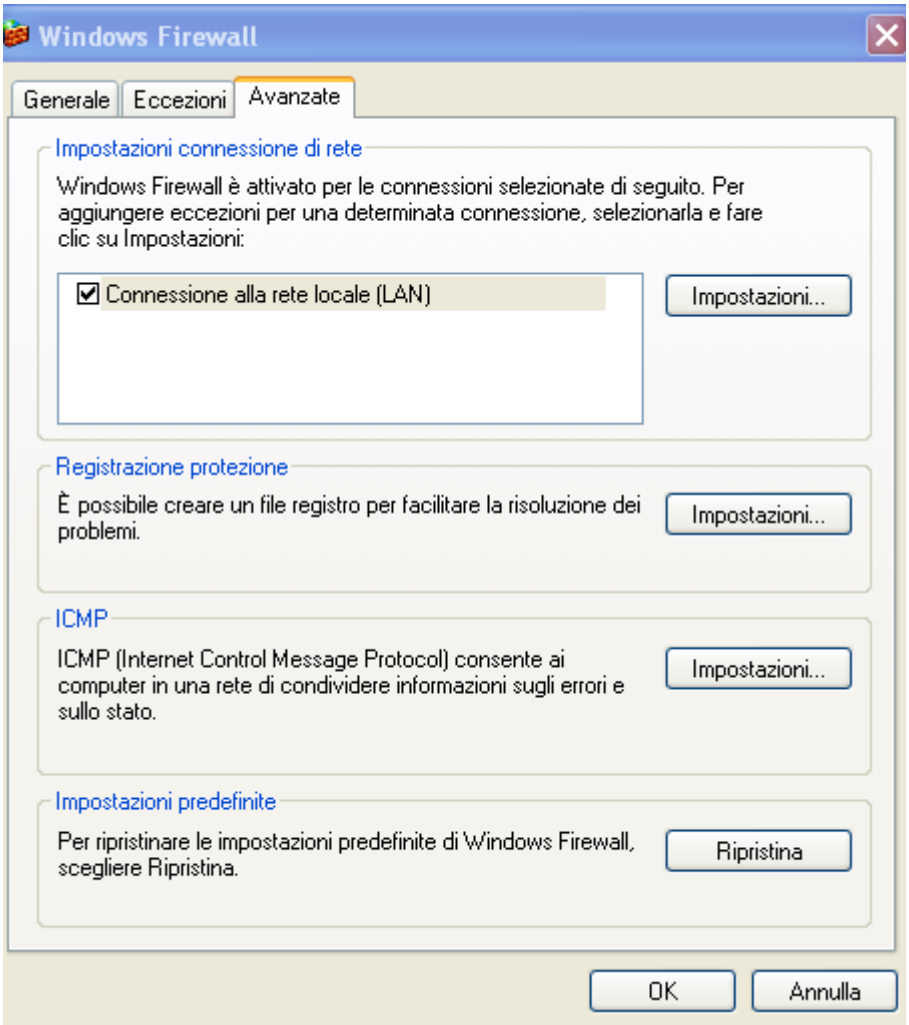
Ora invece effettuiamo la scansione con il firewall attivato:

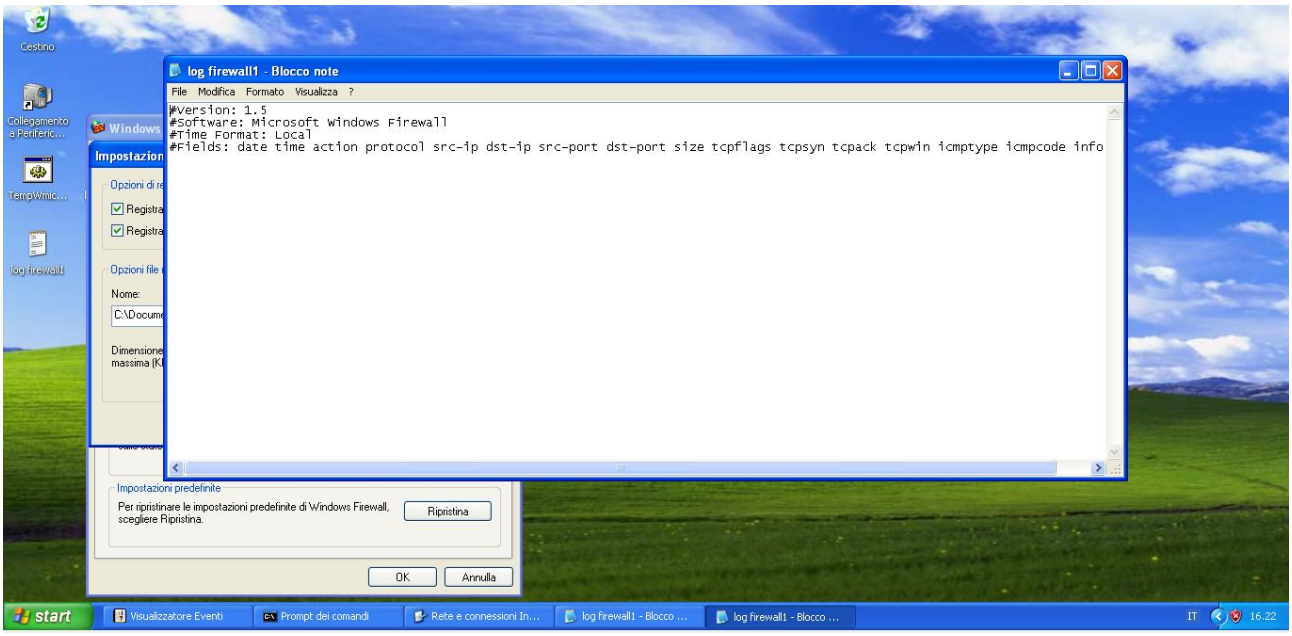
```
┌──(alessio㉿kali)-[~]
└─$ nmap -sV 192.168.240.150 -o scanxp1.txt
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-20 14:20 CET
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 4.27 seconds

┌──(alessio㉿kali)-[~]
```

come possiamo notare, i 3 servizi attivi prima, ora non risultano.

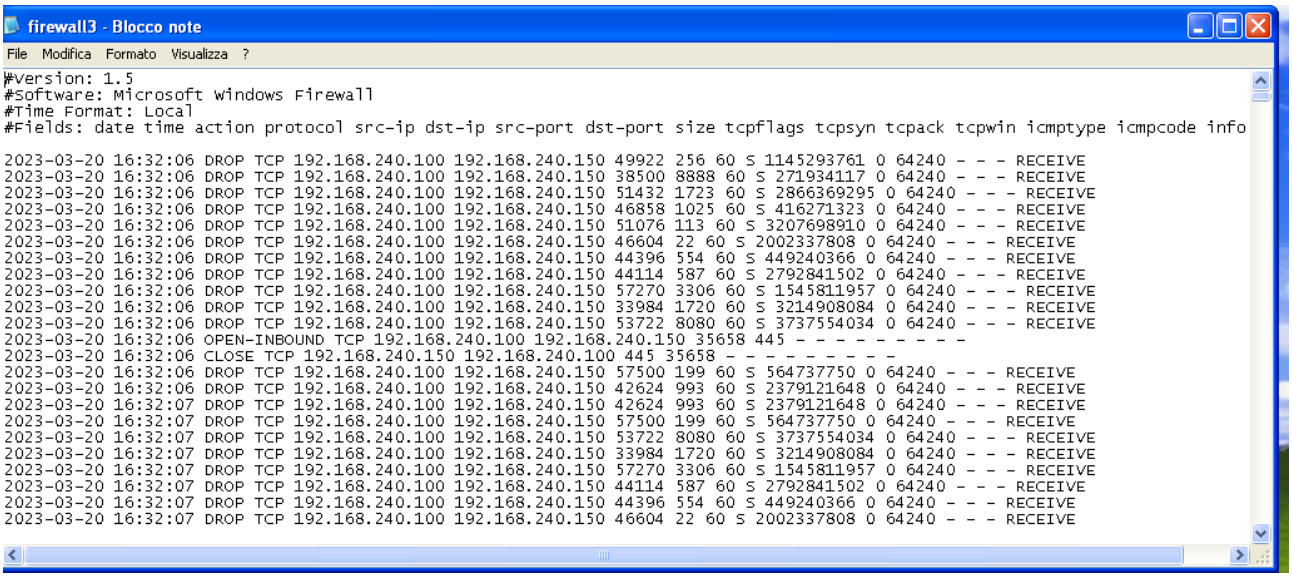
Il motivo e che il firewall su xp e impostato affinche non si permetta la scansione delle porte che, la maggior parte delle volte, e l 'ultimo passo prima di un attacco cyber (a meno che la scansione non venga effettuata da un whyte hacker che sta eseguendo un penetretion test ma, in questo caso, avrebbe accesso alle impostazioni del firewall).

Ora analizziamo pero il comportamento del firewall nello specifico analizzando i suoi log. I log erano disabilitati e, dopo una ricerca su internet, ho scoperto che bisognava attivarli e salvare il file dei futuri log dove ci risultava piu comodo.. io personalmente l'ho salvato sul desktop:





Dopo, ovviamente, spegnendo il firewall il file del log rimane vuoto ma, attivandolo, nel file vengono salvate tutte le azioni che il firewall in questione esegue. Diamogli un occhiata:



Possiamo vedere come su come nella maggior parte dei casi il firewall con l'azione drop blocca la connessione alla macchina kali (192.168.240.100, src ip).

Possiamo notare anche la porta src di xp e la dest prt di kali, possiamo notare anche il syn ack con il quale si prova ad effettuare la connessione TCP e, possiamo anche notare, fra le informazioni , il codice icmp che e un protocollo gia visto ad esempio perche viene usato nei ping .