

Dopo aver impostato gli IP come da traccia, eseguiamo un nmap sulla macchina con Windows XP sprovvisto di firewall:

```
(kali@kali)-[~]
$ nmap -sV 192.168.240.150 -oX XP
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 06:28 EDT
Nmap scan report for 192.168.240.150
Host is up (0.00091s 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 7.69 seconds
```

Come si può osservare vi sono 3 servizi in ascolto sulle tre porte 135, 139 e 445.

Andando ad attivare il firewall su XP , eseguiamo di nuovo un nmap con l'opzione -Pn (no ping):

```
(kali@kali)-[~]
$ nmap -sV 192.168.240.150 -oX XP2 -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 06:31 EDT
Nmap scan report for 192.168.240.150
Host is up (0.0021s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
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 10.97 seconds
```

Ora le porte aperte sono 2 anziché 3, attivando invece sul firewall la modalità di protezione massima (spuntando l'opzione "non consentire eccezioni") la situazione diventa questa:

```
(kali@kali)-[~]
$ nmap -sV 192.168.240.150 -oX XP2 -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 06:32 EDT
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)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 204.04 seconds
```

Abbiamo un filtraggio completo da parte del firewall di tutte le porte accessibili prima, riducendo drasticamente dunque le possibilità ad un attaccante di intrufolarsi all'interno della rete.