

Durante l'esecuzione di "nmap -sV" sul mio laboratorio virtuale utilizzando la macchina Kali, ho notato differenze significative nei risultati dello scan tra il firewall di Windows attivato e disattivato sulla macchina virtuale Windows XP:

- **Con firewall disattivato:**

```
(kali㉿kali)-[~]  
$ nmap -sV 192.168.240.150  
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-05 03:26 EST  
Nmap scan report for 192.168.240.150  
Host is up (0.00021s 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  
  
Service detection performed. Please report any incorrect results  
Nmap done: 1 IP address (1 host up) scanned in 20.69 seconds
```

- **Con firewall attivato:**

```
(kali㉿kali)-[~]  
$ nmap -sV -Pn 192.168.240.150  
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-05 03:30 EST  
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  
Nmap done: 1 IP address (1 host up) scanned in 217.22 seconds
```

Quando il firewall di Windows era disattivato, l'output di Nmap ha fornito informazioni dettagliate sui servizi attivi, inclusi i numeri di versione. Tuttavia, quando il firewall di Windows è stato attivato, l'output di Nmap ha indicato che le porte erano in uno stato "ignorato" e non ha fornito alcuna informazione sui servizi.

La differenza nei risultati può essere attribuita alla politica di sicurezza implementata dal firewall di Windows. Quando il firewall è attivo, filtra le richieste di Nmap e consente solo quelle che soddisfano le regole di sicurezza definite. Quando il firewall è disattivato, non c'è alcuna restrizione nelle comunicazioni.

La differenza nei risultati dello scan dunque è causata dalla presenza del firewall di Windows, che regola l'accesso alle porte e influenza la capacità di Nmap di ottenere informazioni sui servizi attivi sulla macchina virtuale Windows XP.