

Avendo il firewall spento la funzione nmap ci mostra quali sono le porte aperte, attraverso questa azione ci permette conoscere quali sono le porte che possono essere sfruttate da attaccanti esterni perche l'assenza di firewall espone la macchina

```
(kali㉿kali)-[~]  
$ nmap -sV 192.168.240.150  
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-20 05:06 EST  
Nmap scan report for 192.168.240.150  
Host is up (0.00039s 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 20.40 seconds
```

Avendo il firewall acceso invece, possiamo osservare che nmap non rileva niente, viene bloccato. Nelle note della funzione stessa possiamo leggere che è stato bloccato il ping verso la macchina attaccata.

```
(kali㉿kali)-[~]  
$ nmap -sV 192.168.240.150  
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-20 05:07 EST  
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 3.13 seconds
```

Il firewall serve per filtrare l'accesso di pacchetti da fonti esterne e di limitarne il movimento o bloccarle, come in questo caso nmap. Il firewall è un ottimo muro di difesa dato che oltre a filtrare il traffico di pacchetti, ci protegge da intrusi e gestisce connessioni che possono essere sospette.