

## Firewall windows

obiettivo del esercizio di oggi è vedere l'interazione del firewall con programmi di scan come nmap. Nel esercizio di oggi vengono effettuati due scan, il primo con il firewall spento il secondo con il firewall attivo

```
(kali@kali) [~]
$ nmap -sV -o report 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 06:48 EDT
Nmap scan report for 192.168.240.150
Host is up (0.00016s 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: OS: 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 20.38 seconds

(kali@kali) [~]
$ nmap -sV -o report 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 06:49 EDT
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

(kali@kali) [~]
$
```

Come possiamo vedere nella foto all'attivazione del firewall la richiesta iniziale di ping di nmap viene bloccata prevenendo lo scan