Esercizio

Differenza tra le scansioni con e senza firewall.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -T4 192.168.104.150 -o scansioneSenzaFirewall
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-08 16:14 CEST
Nmap scan report for 192.168.104.150
Host is up (0.0062s 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 20.66 seconds
```

Senza il firewall possiamo vedere quali sono le porte aperte, i servizi attivi e la versione del sistema operativo che stiamo attaccando.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -T4 192.168.104.150 -o scansioneConFirewall
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-08 16:17 CEST
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 2.28 seconds
```

Con il firewall invece non abbiamo avuto alcun tipo d'informazione riguardante le porte o le altre info che abbiamo ottenuto con la scansione senza il firewall. Questo perché il firewall blocca la connessione dall'esterno.