

In questo esercizio andiamo a vedere la differenza tra un firewall attivo o meno, su windows XP, tramite Nmap.

Possiamo notare subito con una scansione `-sV` (Per le versioni dei servizi attivi), senza firewall, le varie versioni dei servizi sulle porte in ascolto ed il sistema operativo attualmente in uso (windows XP).

Attivando il firewall invece, la stessa scansione non ci dà alcun risultato. Nmap ci consiglia di utilizzare `-Pn` per non inviare ping (protocollo ICMP).

Così facendo riusciamo a vedere il sistema operativo, ma non tutte le porte ed i servizi attivi su esse.

```
(dan@Kali)-[~]
$ nmap -sV 192.168.240.150
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-20 12:35 CET
Nmap scan report for 192.168.240.150
Host is up (0.00021s latency).
Not shown: 996 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
3389/tcp   open  ms-wbt-server  Microsoft Terminal Services
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 21.09 seconds

(dan@Kali)-[~]
$ nmap -sV 192.168.240.150
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-20 12:36 CET
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 3.10 seconds

(dan@Kali)-[~]
$ nmap -sV -Pn 192.168.240.150
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-20 12:36 CET
Nmap scan report for 192.168.240.150
Host is up (0.00062s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE        VERSION
3389/tcp   open  ms-wbt-server  Microsoft Terminal Services
Service Info: OS: Windows XP; CPE: 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 28.06 seconds

(dan@Kali)-[~]
$
```