

ESERCITAZIONE S9 L1

Una volta impostati gli ip delle due macchine come richiesto, possiamo avviare una scansione di nmap con service detection

Nmap -sV 191.168.240.150 (ip target)

```
(kali@kali)-[~]  
$ nmap -sV 192.168.240.150  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-29 11:18 CET  
Nmap scan report for 192.168.240.150  
Host is up (0.89s 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 20.56 seconds
```

Successivamente andiamo ad avviare il Firewall su Windows Xp, e ripetiamo lo stesso comando.

```
(kali@kali)-[~]  
$ nmap -sV 192.168.240.150  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-29 11:19 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 3.12 seconds
```

Possiamo notare facilmente che la seconda scansione, in seguito all'attivazione del firewall, non permette l'individuazione della macchina sulla rete, motivo per cui non c'è l'enumerazione delle porte e delle info del sistema operativo target.

Ovviamente l'intervento del firewall può essere mitigato andando a impostare alcuni parametri di esso, così da creare un equilibrio tra esposizione sulla rete e sicurezza dagli attacchi.