

## PRATICA S9L1

Dopo aver configurato gli indirizzi ip sulle macchine kali e windows xp, proviamo una scansione con lo switch -sV per verificare i servizi attivi e la relativa versione in ascolto sulla macchina target windows xp:

```
(luca@kali)-[~]
$ nmap -sV 192.168.240.150
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-20 11:34 CET
Nmap scan report for 192.168.240.150
Host is up (0.0043s 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 19.80 seconds
```

Troviamo diverse porte in ascolto, che potrebbero essere usate da una eventuale attaccante come possibili obiettivi di un exploit sulla macchina. Vediamo come cambia la situazione andando ad attivare il firewall su Windows XP. Facciamo due scansioni:

```
(luca@kali)-[~]
$ nmap -sV 192.168.240.150
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-20 11:36 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 3.12 seconds
```

Notiamo che questa scansione ci informa che il target risulta (erroneamente) essere down o irraggiungibile. Questo perché di default nmap usa il protocollo ICMP per verificare la raggiungibilità, ma questo protocollo viene rifiutato di default dal firewall di windows. Non ricevendo risposta quindi nmap trae la suddetta conclusione. Proviamo quindi ad inserire l'opzione -Pn, che tratta il target come se avesse ricevuto risposta positiva al ping e passa direttamente alla fase successiva di scansione vera e propria:

```
(luca@kali)-[~]
$ nmap -sV 192.168.240.150 -Pn
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-20 11:36 CET
Nmap scan report for 192.168.240.150
Host is up.
All 1000 scanned ports on 192.168.240.150 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 214.76 seconds
```

La risposta è leggermente diversa. Nmap conclude che il target è UP, ma anche in questo caso non riesce a concludere se vi siano porte in ascolto. Da una risposta di questo tipo possiamo quindi concludere che l'obiettivo della nostra scansione sia protetto da un firewall, che non consente quindi connessioni in ingresso (a meno che non abbia una policy specifica).