

Esercizio S9-L1

L'esercizio prevedeva di fare un test sulle differenze percepite da due scan nmap verso macchina windows xp, la prima con firewall disattivato, la seconda con firewall attivo.

```
(gimp@kali)-[~]
$ nmap -sV 192.168.200.200
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-20 15:39 CET
Nmap scan report for 192.168.200.200
Host is up (0.0011s 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 20.48 seconds

(gimp@kali)-[~]
$ nmap -sV 192.168.200.200
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-20 15:40 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 3.08 seconds
```

La prima scansione con firewall disattivato non ha creato problemi, vengono restituite tre porte aperte.

Nella scansione con firewall disattivato invece l'host non viene proprio raggiunto. Questo è ricollegabile alla funzione del firewall dinamico. Provando infatti a fare un altro test, usando il ping, esso che prima non aveva problemi a raggiungere il dispositivo ora non lo rilevava neanche. Queste perché il firewall dinamico blocca ogni connessione esterna e autorizza connessioni esterne solo se prima la richiesta è stata fatta dall'interno. Infatti, provando a pingare il dispositivo kali da windows xp non si hanno problemi di connessione.

Ho provato a fare un ulteriore test, usando la stessa scansione nmap ma togliendo il ping, quindi utilizzando solo la 3way handshake del protocollo tcp. In questo caso viene rilevato che l'host è attivo ma le porte non vengono mostrate, rimangono nello stato di porte filtrate.

```
(gimp@kali)-[~]
$ nmap -sV -Pn 192.168.200.200
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-20 15:42 CET
Stats: 0:03:08 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 83.00% done; ETC: 15:45 (0:00:36 remaining)
Stats: 0:03:27 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 92.00% done; ETC: 15:45 (0:00:17 remaining)
Nmap scan report for 192.168.200.200
Host is up.
All 1000 scanned ports on 192.168.200.200 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 223.71 seconds
```