

Progetto S9-L1

Studente: Simone Mininni

Task: Osservare il differente comportamento della scansione con nmap di windowsXP con il firewall on/off.

Nella situazione iniziale dove il firewall di windowsXP è disattivato notiamo che la scansione con nmap va facilmente a buon fine restituendoci il s.o. del target e i servizi attivi su determinate porte come il protocollo netbios e samba.

```
└─$ nmap -sV 192.168.200.200
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-20 15:53 CET
Nmap scan report for 192.168.200.200
Host is up (0.0020s 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 19.74 seconds
```

Con il firewall attivato, l' output di nmap è poco esplicito.

```
└─$ nmap -sV 192.168.200.200
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-20 16:01 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
```

Notiamo che il target su cui effettuiamo la scansione blocca il ping in entrata, infatti il firewall di windows blocca le icmp requests in entrata.

Inserendo lo switch -Pn(nmap durante la scansione non invia un pacchetto icmp), notiamo che l' host è attivo ma le porte sono filtrate, quindi non riusciamo a stabilire quali porte sono effettivamente chiuse e quali aperte, questo dovuto proprio alla presenza del firewall. Si potrebbe tentare di evadere il firewall utilizzando delle tecniche specifiche con nmap.

```
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 214.73 seconds
```