Esercizio S9L1

L'esercizio di oggi è verificare in che modo l'attivazione del Firewall impatta il risultato di una scansione dei servizi dall'esterno. Per questo motivo:

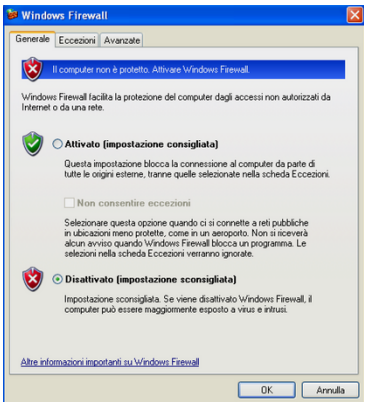
- Assicuratevi che il Firewall sia disattivato sulla macchina Windows XP.
- Effettuate una scansione con nmap sulla macchina target (utilizzate lo switch –sV, per la service detection).
- Abilitare il Firewall sulla macchina Windows XP.
- Effettuate una seconda scansione con nmap, utilizzando ancora una volta lo switch –sV.

Che differenze notate? E quale può essere la causa del risultato diverso?

Requisiti:

- Configurate l'indirizzo di Windows XP come di seguito: 192.168.240.150
- Configurate l'indirizzo della macchina Kali come di seguito: 192.168.240.100

Con il firewall disattivato ci ha permesso di pingare e di fare la scansione senza problemi mostrandoci quindi che le due macchine communicasserò e, le porte e i servizi aperte con le loro versioni invece con il firewall attivo ci mostrava che le macchine non communicano e che le porte sono filtrate.




```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.240.150
PING 192.168.240.150 (192.168.240.150) 56(84) bytes of data.
64 bytes from 192.168.240.150: icmp_seq=1 ttl=128 time=4.22 ms
64 bytes from 192.168.240.150: icmp_seq=2 ttl=128 time=2.94 ms
^C
— 192.168.240.150 ping statistics —
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 2.936/3.578/4.221/0.642 ms

┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.240.150
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-20 07:08 EST
Nmap scan report for 192.168.240.150
Host is up (1.0s 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:microsof
t:windows_xp

Service detection performed. Please report any incorrect results at https://nmap.org/s
ubmit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.94 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.240.150
PING 192.168.240.150 (192.168.240.150) 56(84) bytes of data.
^C
— 192.168.240.150 ping statistics —
8 packets transmitted, 0 received, 100% packet loss, time 7164ms


┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.240.150
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-20 08:39 EST
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 3.13 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -Pn 192.168.240.150
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-20 08:40 EST
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)

Nmap done: 1 IP address (1 host up) scanned in 215.39 seconds
```

La causa di tutto ciò è esattamente il firewall dato che blocca tutte le connessioni che arrivano dall'esterno tranne le eccezioni.