Claudio De cicco
19/12/2022

Report

Come prima operazione andiamo a cambiare gli Ip come richiesto e faccio un controllo se le macchine comunicano tramite un ping.

```
┌──(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=26 ttl=128 time=0.490 ms
64 bytes from 192.168.240.150: icmp_seq=27 ttl=128 time=1.04 ms
64 bytes from 192.168.240.150: icmp_seq=28 ttl=128 time=0.407 ms
64 bytes from 192.168.240.150: icmp_seq=29 ttl=128 time=0.880 ms
64 bytes from 192.168.240.150: icmp_seq=30 ttl=128 time=1.56 ms
64 bytes from 192.168.240.150: icmp_seq=31 ttl=128 time=0.876 ms
^C
── 192.168.240.150 ping statistics ──
31 packets transmitted, 6 received, 80.6452% packet loss, time 30845ms
rtt min/avg/max/mdev = 0.407/0.875/1.562/0.380 ms
```

A questo punto con il firewall di xp disabilitato vado a fare una scansione con nmap con switch -sV.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.240.150
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-19 08:12 EST
Nmap scan report for 192.168.240.150
Host is up (0.00054s 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 20.99 seconds
```

Come risultato abbiamo la lista delle porte aperte del loro servizio e della loro versione.

Come seconda prova lanciamo un'altra scansione ma andando ad attivare il firewall su xp.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.240.150
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-19 08:12 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 3.62 seconds
```

In questo caso nmap ci dice che non è riuscito a stabilire una connessione perché l'host sembra essere "down", questo perché,come ci suggerisce anche nelle proprietà xp, il firewall blocca tutte le connessioni in entrata tranne quelle scelte o selezionate dall'utente.Questo permette quindi di avere meno rischi , ma anche un funzionamento limitato per alcuni programmi. Per migliorare questa situazione si protrebbero creare delle regole personalizzate o di attivarne di già esistenti , aumentando però il rischio di protezione.


Windows Firewall
Generale
Eccezioni
Avanzate
Windows Firewall sta bloccando le connessioni di rete in ingresso, ad eccezione dei programmi e dei servizi selezionati di seguito. Aggiungendo eccezioni si può migliorare il funzionamento di alcuni programmi, ma possono aumentare i rischi di protezione.
Programmi e servizi:
Nome
Assistenza remota
Condivisione file e stampanti
Desktop remoto
Diagnostica rete per Windows XP
Framework UPnP