

CS-Operation

Cambio gli indirizzi delle due macchine e verifico la connessione con il ping

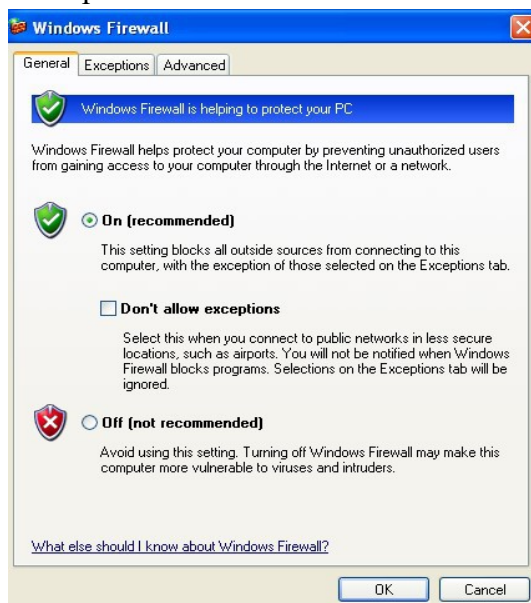
```
(kali@kali)-[~]
$ ping 192.168.240.150
PING 192.168.240.150 (192.168.240.150) 56(84) bytes of data.
64 bytes from 192.168.240.150: icmp_seq=1 ttl=128 time=1.28 ms
64 bytes from 192.168.240.150: icmp_seq=2 ttl=128 time=1.46 ms
64 bytes from 192.168.240.150: icmp_seq=3 ttl=128 time=1.65 ms
^X64 bytes from 192.168.240.150: icmp_seq=4 ttl=128 time=2.32 ms
^C
— 192.168.240.150 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3058ms
rtt min/avg/max/mdev = 1.276/1.678/2.324/0.395 ms
```

Verificata la connessione avvio nmap tenendo le impostazioni del firewall di windows su off

```
(kali@kali)-[~]
$ cat WindowsXP.txt
# Nmap 7.93 scan initiated Thu Nov 16 07:25:52 2023 as: nmap -sV -o WindowsXP.txt 192.168.240.150
Nmap scan report for 192.168.240.150
Host is up (0.00035s latency).
Not shown: 997 closed tcp ports (reset)
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
MAC Address: 08:00:27:B4:3F:C7 (Oracle VirtualBox virtual NIC)
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 at Thu Nov 16 07:26:01 2023 -- 1 IP address (1 host up) scanned in 8.31 seconds
```

Si nota che la scansione dà come risultato la versione di ogni servizio presente sulle porte aperte e il sistema operativo.



Tiro su il firewall e riprovo la scansione

```
(kali㉿kali)-[~]  
└─$ sudo nmap -sV 192.168.240.150  
[sudo] password for kali:  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-16 07:29 CET  
Nmap scan report for 192.168.240.150  
Host is up (0.0028s latency).  
All 1000 scanned ports on 192.168.240.150 are in ignored states.  
Not shown: 1000 filtered tcp ports (no-response)  
MAC Address: 08:00:27:B4:3F:C7 (Oracle VirtualBox virtual NIC)  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 25.95 seconds
```

Dalla scansione effettuata con il firewall su si può notare che nmap ci dice che l'host è attivo quindi lo ha visto ma ci non ci mostra nessuna porta perché le vede come filtrate.