

Security Operation: Operazioni Preventive

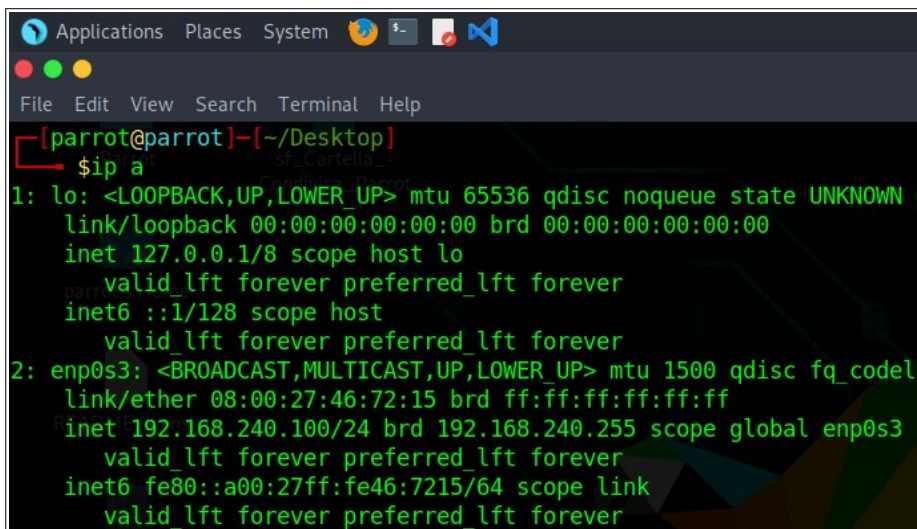
Obiettivo: Osservare in che modo il Firewall impatta sul risultato di una scansione dei servizi esterna.

1) Indirizzi IP

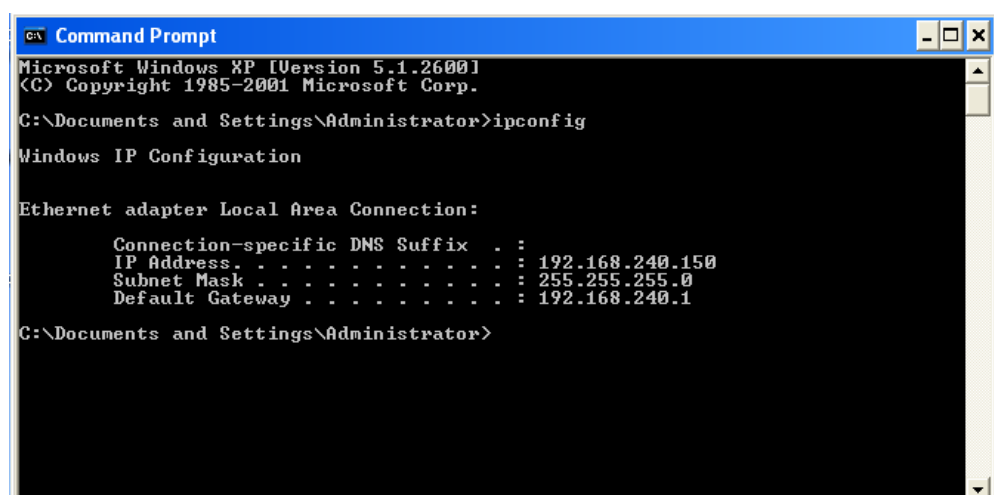
Per cominciare ho modificato gli Indirizzi IP per avere le due macchine nella stessa rete interna:

Parrot 192.168.240.100

Windows XP 192.168.240.150



```
[parrot@parrot]--[~/Desktop]
$ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN g
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
    valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
    valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel
link/ether 08:00:27:46:72:15 brd ff:ff:ff:ff:ff:ff
inet 192.168.240.100/24 brd 192.168.240.255 scope global enp0s3
    valid_lft forever preferred_lft forever
inet6 fe80::a00:27ff:fe46:7215/64 scope link
    valid_lft forever preferred_lft forever
```



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>ipconfig

Windows IP Configuration

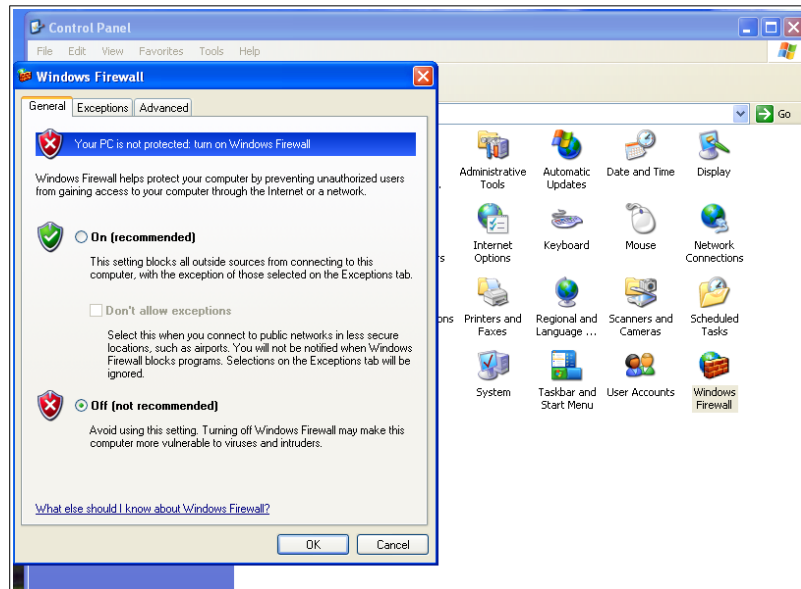
Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.240.150
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.240.1

C:\Documents and Settings\Administrator>
```

2) Scansione dei Servizi con Nmap - Windows Firewall Off

La traccia chiedeva di disattivare il *Firewall* di **Windows XP** prima di avviare ogni scansione ma dato che negli scorsi esercizi abbiamo eseguito altri tipi di scansione era già disattivato.



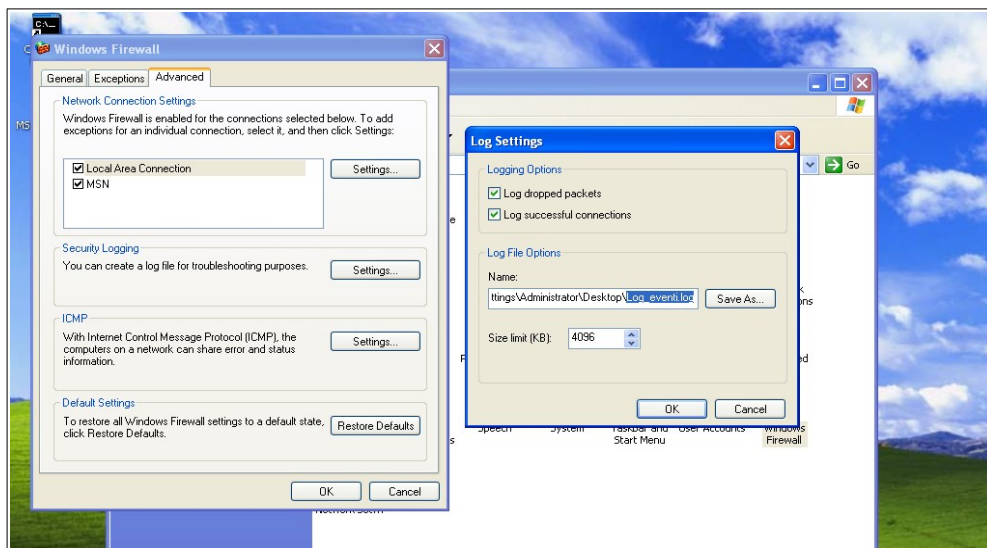
```
Applications Places System
File Edit View Search Terminal Help
[parrot@parrot]~/Desktop
$ nmap -sV 192.168.240.150 > nmap_sV_No_Firewall.txt
[parrot@parrot]~/Desktop
$ cat nmap_sV_No_Firewall.txt
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-26 14:29 BST
Nmap scan report for 192.168.240.150
Host is up (0.0049s latency).
Not shown: 996 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
3389/tcp   open  ms-wbt-server  Microsoft Terminal Services
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 21.75 seconds
```

Dopo aver controllato ho avviato la *Scansione dei Servizi (-sV)* all'indirizzo della macchina **Windows**. Il risultato ci mostra quattro porte aperte con le relative versioni dei servizi attivi.

NB: Ho salvato su un *file .txt* il risultato delle scansioni leggendole poi con *cat*.

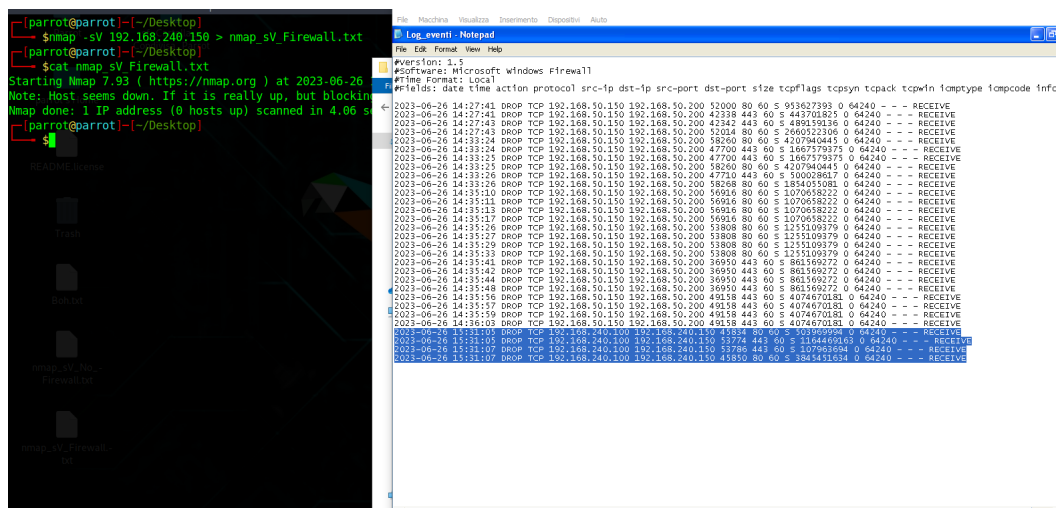
3) Scansione dei Servizi con Nmap - Windows Firewall On

Successivamente come richiesto dalla traccia ho attivato il *Firewall*. Per comodità ho salvato il file di **Log** sul Desktop abilitando le spunte per salvare anche i pacchetti “droppati” e le connessioni eventualmente riuscite.



Avviando la Scansione con **Nmap** (sempre **-sV**) e leggendone il risultato si può evincere che la scansione non ha avuto esito positivo per il blocco del *Firewall* che non ha permesso lo scambio di pacchetti con una fonte esterna.

```
Applications Places System
File Edit View Search Terminal Help
[parrot@parrot]~[~/Desktop]
$ nmap -sV 192.168.240.150 > nmap_sV_Firewall.txt
[parrot@parrot]~[~/Desktop]
$ cat nmap_sV_Firewall.txt
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-26 14:31 BST
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 4.06 seconds
```



4) Scansione Aggressiva – Windows Firewall ON

Il risultato è lo stesso anche con una scansione dei Servizi o con *Timing* o.