



SECURITY OPERATION

Giorno 1



Indice

- Introduzione
- Configurazione Ip
- Disattivazione Firewall
- Primo scanning con Nmap
- Attivazione del Firewall
- Secondo scanning con Nmap
- Conclusi



Introduzione

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

1. Assicuratevi che il Firewall sia disattivato sulla macchina Windows XP
2. Effettuare una scansione con nmap sulla macchina target
3. Abilitare il Firewall sulla macchina Windows XP
4. Effettuare una seconda scansione con nmap
5. Trovare le eventuali differenze e motivarle.

Configurazione Ip

Andiamo a configurare gli indirizzi Ip della macchina Windows XP e della macchina Kali.

```
C:\ Command Prompt
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 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>
```

```
(kali@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.240.100 netmask 255.255.255.0 broadcast 192.168.240.255
    inet6 fe80::a00:27ff:fe21:b1d0 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:21:b1:d0 txqueuelen 1000 (Ethernet)
    RX packets 48 bytes 8586 (8.3 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 17 bytes 2494 (2.4 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.5 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::db46:ef7d:3163:c23d prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:36:82:25 txqueuelen 1000 (Ethernet)
    RX packets 42 bytes 6758 (6.5 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 20 bytes 2882 (2.8 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 240 (240.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Disattivazione Firewall

Come richiesto dall'esercizio andiamo a disattivare il firewall della macchina Windows XP



Primo scanning con Nmap

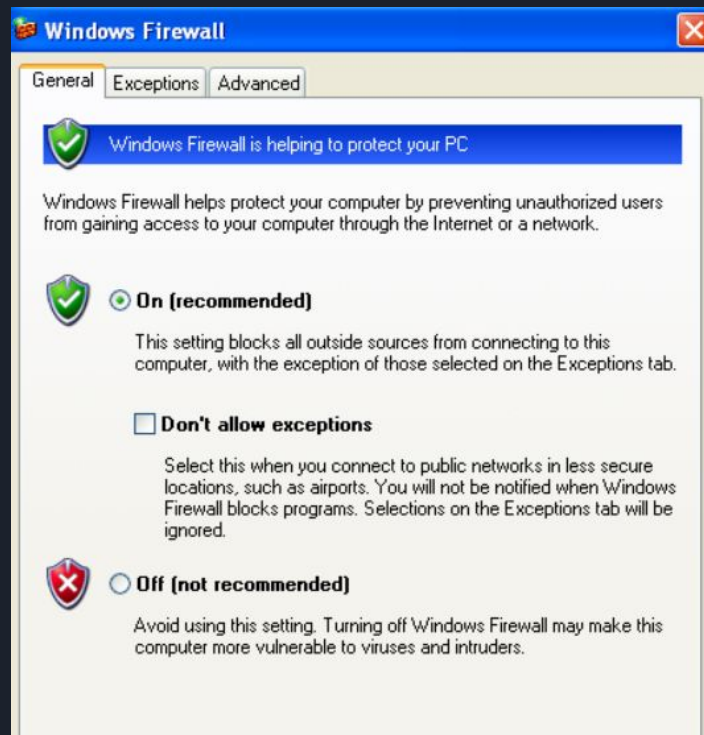
Facciamo il primo scanning con il tool “nmap” già presente sulla macchina di Kali. Possiamo notare che ci sono servizi aperti sulle porte 135, 149, 445, 1032.

```
(kali@kali)-[~/Desktop]
$ nmap -sV 192.168.240.150 -o report.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 07:12 EDT
Nmap scan report for 192.168.240.150
Host is up (0.00054s 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 Vista Embedded microsoft-ds (workgroup: MSHOME)
1032/tcp   open  msrpc        Microsoft Windows RPC
Service Info: Host: GIO; OS: Windows; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_vista

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 55.07 seconds
```

Attivazione del Firewall

Attiviamo il firewall della macchina Windows XP per trovare le differenze.



Secondo scanning con Nmap

Avviamo il secondo scanning e notiamo che è stato bloccato. Disattivando il Ping attraverso il comando “-Pn” notiamo invece che ci da un risultato più accurato.

```
(kali㉿kali)-[~/Desktop]
$ nmap -sV 192.168.240.150 -o report1.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 07:23 EDT
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 3.12 seconds
```

```
(kali㉿kali)-[~/Desktop]
$ nmap -sV 192.168.240.150 -o report1.txt -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 07:24 EDT
Nmap scan report for 192.168.240.150
Host is up (0.00070s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows Vista Embedded microsoft-ds (workgroup: MSHOME)
Service Info: Host: GIO; OS: Windows; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_vista

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.21 seconds
```




Conclusioni

Possiamo dire quindi che utilizzando un firewall possiamo rendere una macchina più sicura perchè va a rendere inaccessibili alcuni servizi. Nel nostro caso i servizi sulle porte 139 e 445 sono ancora accessibili dall'esterno.