SECURITY OPERATION

Giorno 1

Indice

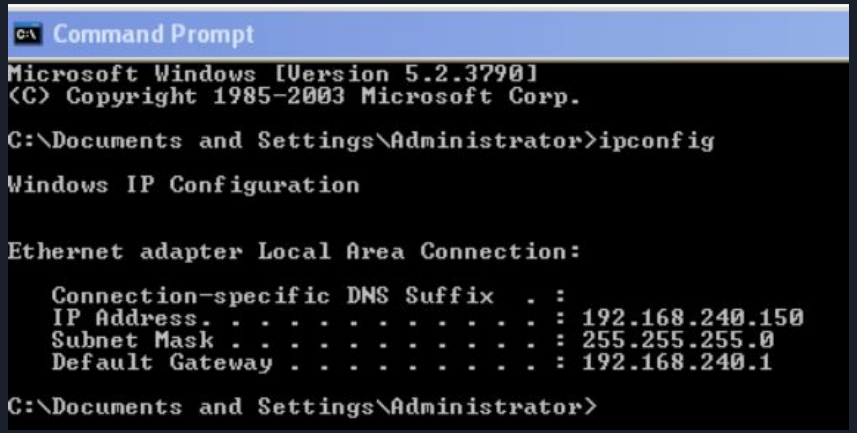
Introduzione

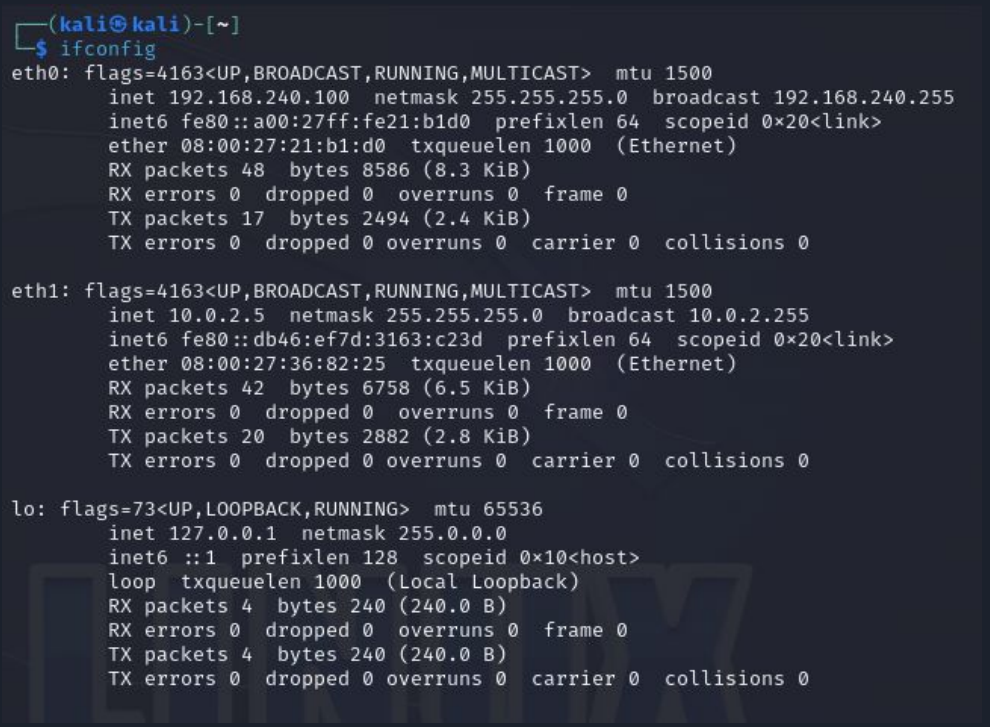
L’esercizio di oggi è di verificare in che modo l’attivazione del Firewall impatta il risultato di una scansione dei servizi dall’esterno. Per questo motivo:

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.





Disattivazione Firewall

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

Primo scanning con Nmap

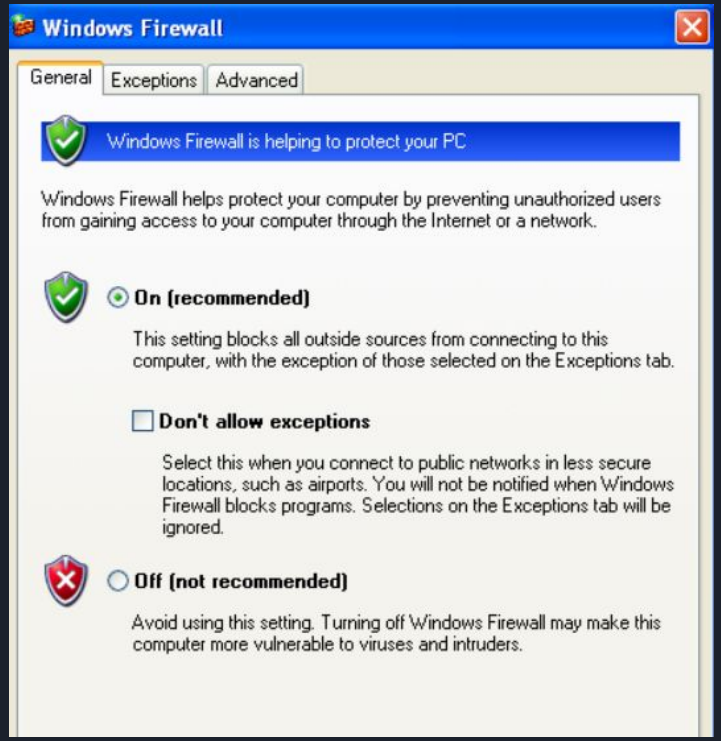
Facciamo il primo scanning con il tool “nmap” già presente sulla macchina di Kali. Possiamo notare che ci sono servizi aperti sulle porte 135, 149, 445, 1032.

```
┌──(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.