18 MARZO 2024

REPORT - EPICODE

S9L1- CS0124

PRESENTED BY

Alessandro Marasca

TRACCIA

Durante la lezione teorica, abbiamo studiato le azioni preventive per ridurre la possibilità di attacchi provenienti dall'esterno.
Abbiamo visto che a livello di rete, possiamo attivare / configurare Firewall e regole per fare in modo che un determinato traffico, potenzialmente dannoso, venga bloccato. La macchina Windows XP che abbiamo utilizzato ha di default il Firewall disabilitato.

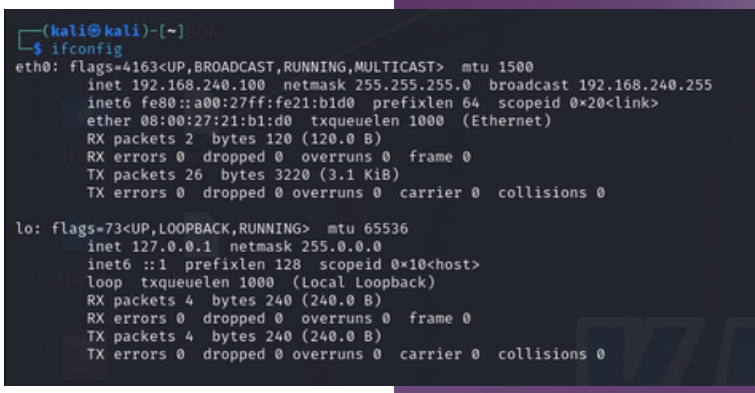
L'esercizio di oggi è verificare in che modo l'attivazione del Firewall impatta il risultato di una scansione dei servizi dall'esterno. Per questo motivo:

1. Assicuratevi che il Firewall sia disattivato sulla macchina Windows XP
2. Effettuate una scansione con nmap sulla macchina target (utilizzate lo switch–sV, per la service detection e -o nomefilereport per salvare in un file l'output)
3. Abilitare il Firewall sulla macchina Windows XP
4. Effettuate una seconda scansione con nmap, utilizzando ancora una volta lo switch –sV.
5. Trovare le eventuali differenze e motivarle.

Che differenze notate? E quale può essere la causa del risultato diverso?
Requisiti:
Configurate l'indirizzo di *Windows XP* come di seguito: 192.168.240.150
Configurate l'indirizzo della macchina *Kali* come di seguito: 192.168.240.100

CONFIGURAZIONI IP

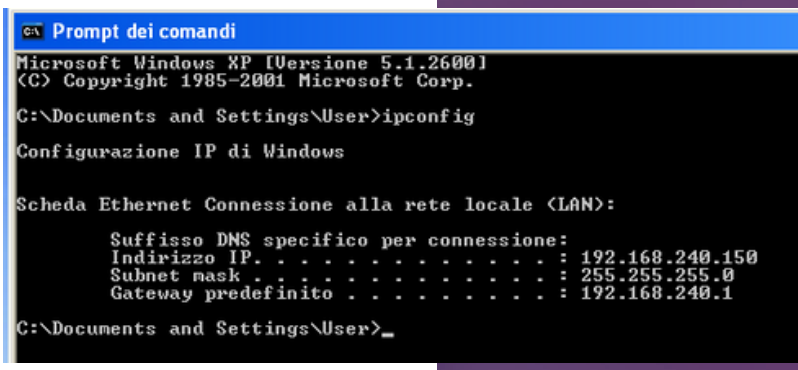
KALI



Impostiamo l'IP delle **MV Kali** e **Windows XP**.

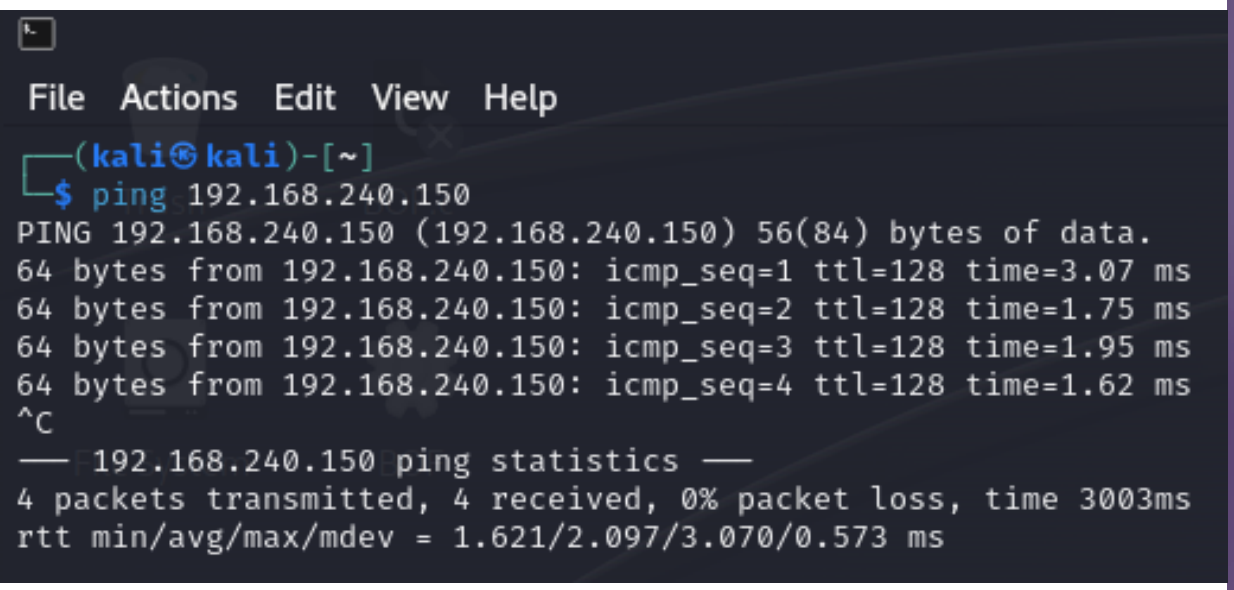
KALI: impostiamo l'IP attraverso il comando **sudo nano /etc/network/interfaces**

WINDOWS XP



Windows XP: simpostiamo l'IP dalle risorse di rete e modificando direttamente il parametro TCP/IP con l'indirizzo corretto

Verifichiamo che le MV comunichino attraverso il ping e procediamo.



SCANSIONE NMAP

Effettuiamo la scansione **NMAP** col comando **-sV** per vedere lo stato e la versione delle porte di **Windows XP** mentre il firewall è **spento.** Salviamo in output il risultato della scansione nel file "**S9L1.txt**" col comando **-oN.** Osserviamo la presenza di 3 porte aperte.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -sV 192.168.240.150 -Pn -oN S9L1.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 07:20 EDT
Nmap scan report for 192.168.240.150
Host is up (0.0020s 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 20.59 seconds
```

```
File  Edit  Search  View  Document  Help

1 # Nmap 7.94SVN scan initiated Mon Mar 18 07:20:11 2024 as: nmap -sV -Pn -oN S9L1.txt 192.168.240.150
2 Nmap scan report for 192.168.240.150
3 Host is up (0.0020s latency).
4 Not shown: 997 closed tcp ports (conn-refused)
5 PORT    STATE SERVICE      VERSION
6 135/tcp open  msrpc        Microsoft Windows RPC
7 139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
8 445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds
9 Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp
10
11 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
12 # Nmap done at Mon Mar 18 07:20:31 2024 -- 1 IP address (1 host up) scanned in 20.59 seconds
13
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 07:06 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 3.09 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.240.150 -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 07:07 EDT
Nmap scan report for 192.168.240.150
Host is up (0.0016s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE  SERVICE VERSION
2869/tcp closed icslap

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 159.52 seconds
```

Passiamo alla scansione NMAP col firewall **ON** e notiamo come risulti tracciabile soltanto una porta, chiusa, corrispondete al Microsoft Internet Connection Firewall (ICF), Internet Connection Sharing (ICS), SSDP Discover Service, Microsoft Universal Plug and Play (UPnP), Microsoft Event Notification

Alessandro Marasca

Epicode

S9L1 - CS0124

14 MARZO 2024