

## S9/L1

Il lavoro di quest'oggi prevede di effettuare 2 scansioni su Windows XP con il tool **nmap**.

La prima verrà eseguita con il firewall disattivato e la seconda , invece, quando è attivo.

Seguiamo i passaggi dati dalla 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.

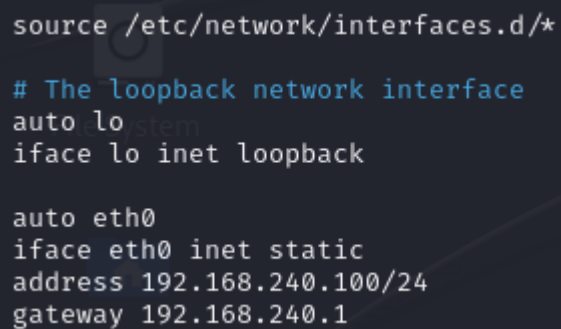
La macchina Windows XP che abbiamo utilizzato ha di default il Firewall disabilitato.

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 -o nomefile report 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.

Prima di iniziare, cambiamo gli indirizzi IP di **Kali** e **Windows** rispettivamente in **192.168.240.100** e **192.168.240.150**

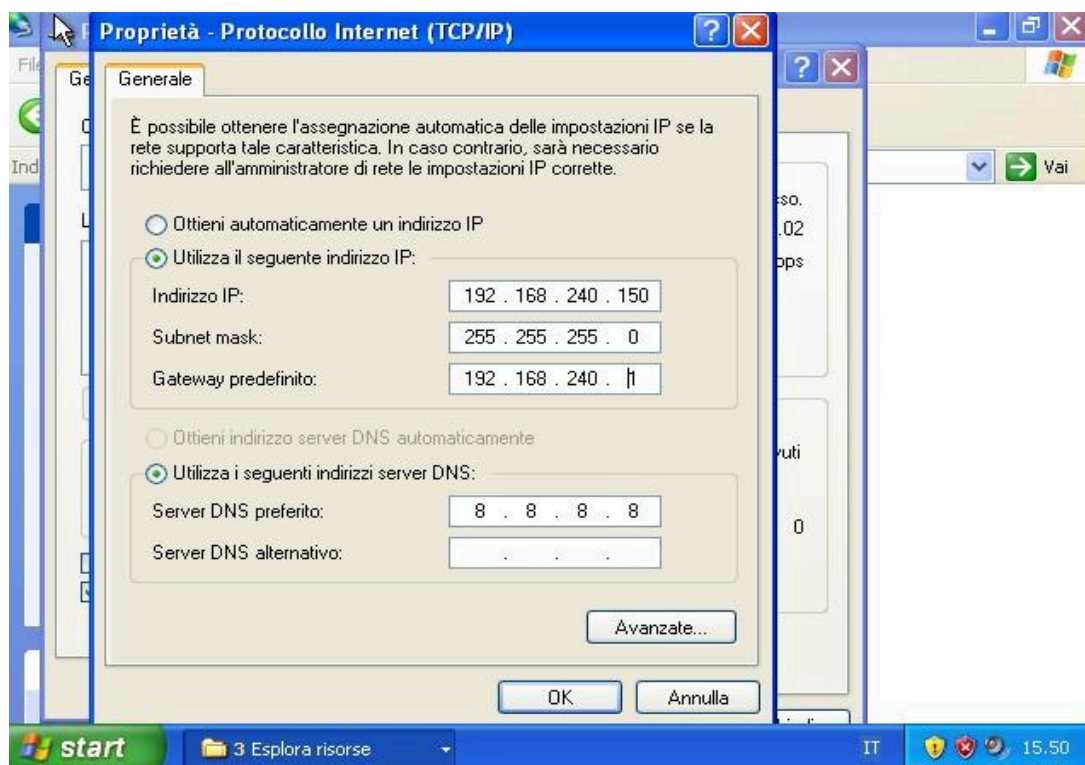
Per Kali sul terminale digitiamo 'sudo nano /etc/network/interfaces' e lo impostiamo come nell'immagine. Premere successivamente CTRL + O , CTRL + X per tornare sul terminale. Riavviare la macchina con il comando 'sudo reboot'.



```
source /etc/network/interfaces.d/*  
  
# The loopback network interface  
auto lo  
iface lo inet loopback  
  
auto eth0  
iface eth0 inet static  
address 192.168.240.100/24  
gateway 192.168.240.1
```

Per cambiare indirizzo IP di Windows XP si seguono i seguenti passaggi:

- 1- Premere Start
- 2- Pannello di controllo
- 3- Connessione di rete (nel mio caso lan) e premere su di essa.
- 4- Cliccare su proprietà e sulla voce "La connessione utilizza i componenti seguenti" cliccare su protocollo TCP/IP
- 5- Modificare l'IP come nell'immagine



Una volta configurato, premere OK e tornare alla schermata principale. Riavviare la macchina direttamente da START.

La prima scansione è stata effettuata con il firewall disattivato e sono risultate aperte alcune porte come si può vedere. Abbiamo utilizzato nmap -sV per visualizzare le porte e le loro versioni.

```
(kali@kali)-[~]
$ nmap -sV 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 12:05 EDT
Nmap scan report for 192.168.240.150
Host is up (0.00015s 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 20.71 seconds
```

Utilizziamo “nmap -O” per l’OS Detection.

```
(root@kali)-[/home/kali]
# nmap -O 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 12:06 EDT
Nmap scan report for 192.168.240.150
Host is up (0.00097s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 08:00:27:C0:8C:57 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows XP|2003
OS CPE: cpe:/o:microsoft:windows_xp cpe:/o:microsoft:windows_server_2003
OS details: Microsoft Windows XP SP2 or SP3, or Windows Server 2003
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.93 seconds
```

Al contrario , la seconda scansione verrà effettuata con il firewall attivo.

```
(root@kali)-[/home/kali]
# nmap -sV 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 12:09 EDT
Nmap scan report for 192.168.240.150
Host is up (0.00036s 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:C0:8C:57 (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 39.43 seconds
```

Con una protezione attiva (firewall) nmap non riesce a trovare alcuna porta aperta perciò non potremmo sfruttare delle vulnerabilità che , invece, con il firewall disattivato ne avremmo potuto approfittare.