S9L1,

BENVENUTI LUIGI

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:

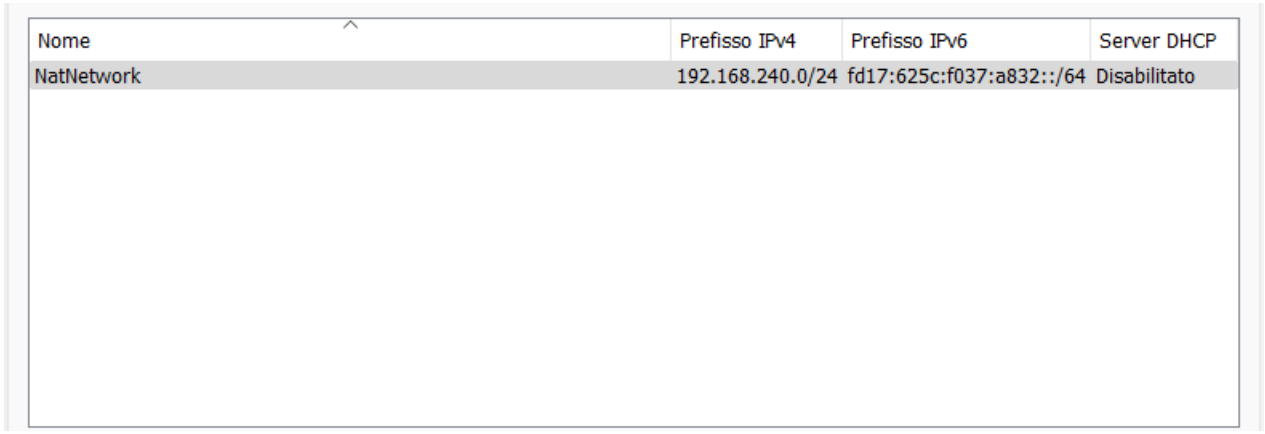
1. Assicuratevi che il Firewall sia disattivato sulla macchina Windows XP

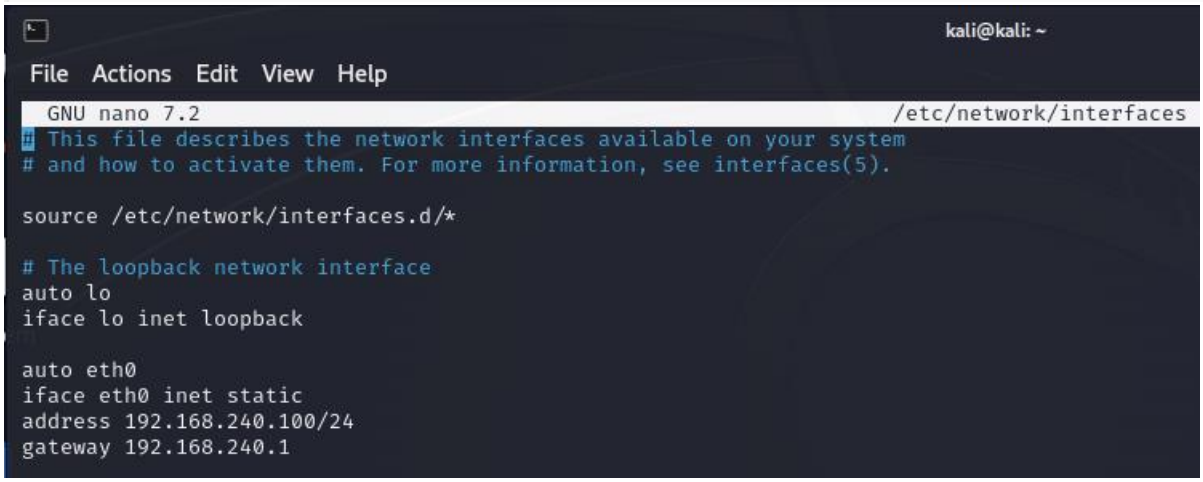
2.Effettuate una scansione con nmapsulla macchina target (utilizzate lo switch–sV, per la service detectione -o nomefilereportper salvare in un file l'output)

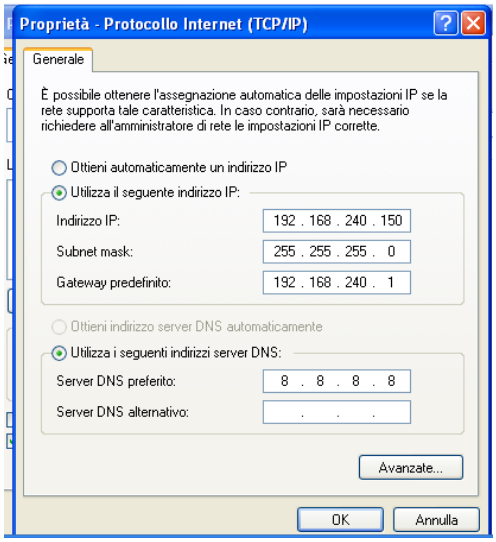
3.Abilitare il Firewall sulla macchina Windows XP

4.Effettuate una seconda scansione con nmap, utilizzando ancora una volta lo switch–sV.

Configurazione di rete:







Nmap (no firewall):

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.240.150 -o report.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 07:16 EDT
Nmap scan report for 192.168.240.150
Host is up (0.0037s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 0.59 seconds
```

Nmap (firewall):

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.240.150 -sV -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 10:41 EDT
Stats: 0:01:18 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 37.00% done; ETC: 10:45 (0:02:13 remaining)
Stats: 0:01:53 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 53.50% done; ETC: 10:45 (0:01:38 remaining)
Stats: 0:02:45 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 78.00% done; ETC: 10:45 (0:00:47 remaining)
Stats: 0:02:47 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 79.00% done; ETC: 10:45 (0:00:44 remaining)
Nmap scan report for 192.168.240.150
Host is up.
All 1000 scanned ports on 192.168.240.150 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 210.63 seconds
```