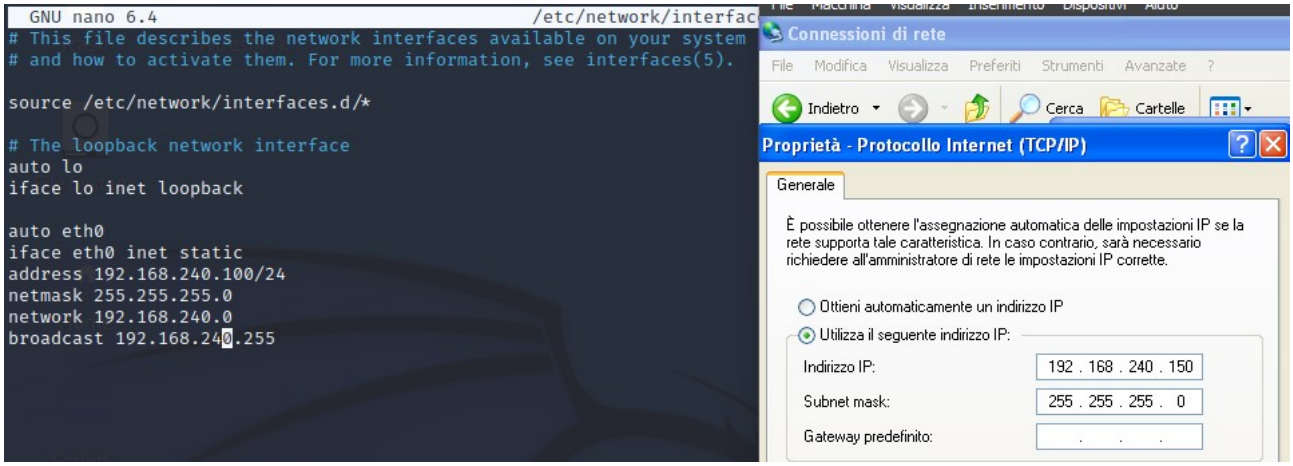
Alaimo Alessandro
19/12/2022

Security Operation

Come richiesto dall'esercizio, andiamo a cambiare gli indirizzi IP delle macchine Kali e Windows XP come di seguito:



Fatto ciò, verifichiamo che il firewall non sia attivo e che le due macchine comunichino tra loro:

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.240.150
PING 192.168.240.150 (192.168.240.150) 56(84) bytes of data.
64 bytes from 192.168.240.150: icmp_seq=1 ttl=128 time=0.206 ms
64 bytes from 192.168.240.150: icmp_seq=2 ttl=128 time=0.227 ms
64 bytes from 192.168.240.150: icmp_seq=3 ttl=128 time=0.223 ms
64 bytes from 192.168.240.150: icmp_seq=4 ttl=128 time=0.251 ms
^C
── 192.168.240.150 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3050ms
rtt min/avg/max/mdev = 0.206/0.226/0.251/0.016 ms
```

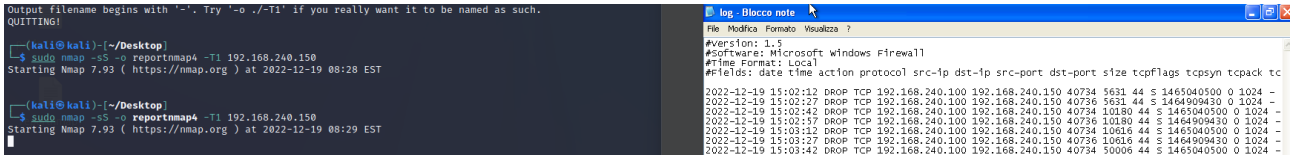
Fatto ciò andiamo ad eseguire un NMAP con lo switch -sV per la service detection e lo switch -o per salvare in un file l'output dato dal tool.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -sV -o reportnmap1 192.168.240.150
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-19 08:21 EST
Nmap scan report for 192.168.240.150
Host is up (0.00042s 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 20.93 seconds
```

Ora vediamo che risultato ci darà la scansione nel caso in cui il firewall sia attivo:

Ora andiamo a salvarci un file chiamandolo log, dalle opzioni avanzate del firewall e possiamo notare che fintanto il firewall è attivo, il file che abbiamo chiamato log si aggiornerà ad ogni apertura di esso:



Come possiamo notare, il firewall blocca a priori qualsiasi pacchetto proveniente dalla macchina Kali. Se invece il firewall è disattivato, non otterremo nessun log.