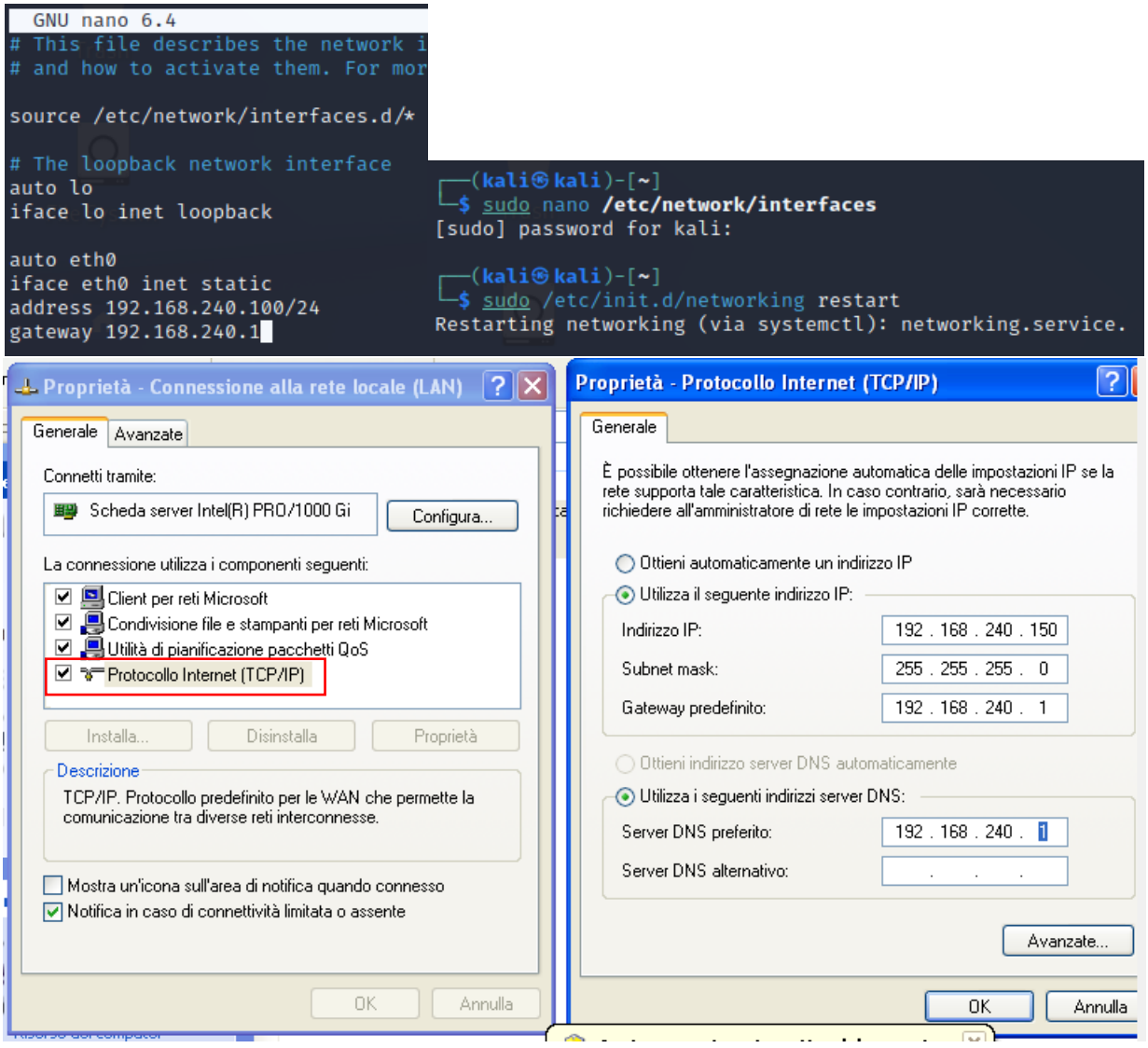
SCANSIONE NMAP CON FIREWALL ATTIVATO/DISATTIVATO

L’esercizio di oggi richiede di effettuare 2 diverse scansioni con Nmap dalla macchina Kali verso Windows XP, prima con firewall disattivato poi con filtro attivo.

Per prima cosa cambiamo gli indirizzi IP delle 2 macchine come richiesto:

KALI 192.168.240.100

WINDOWS XP 192.168.240.150

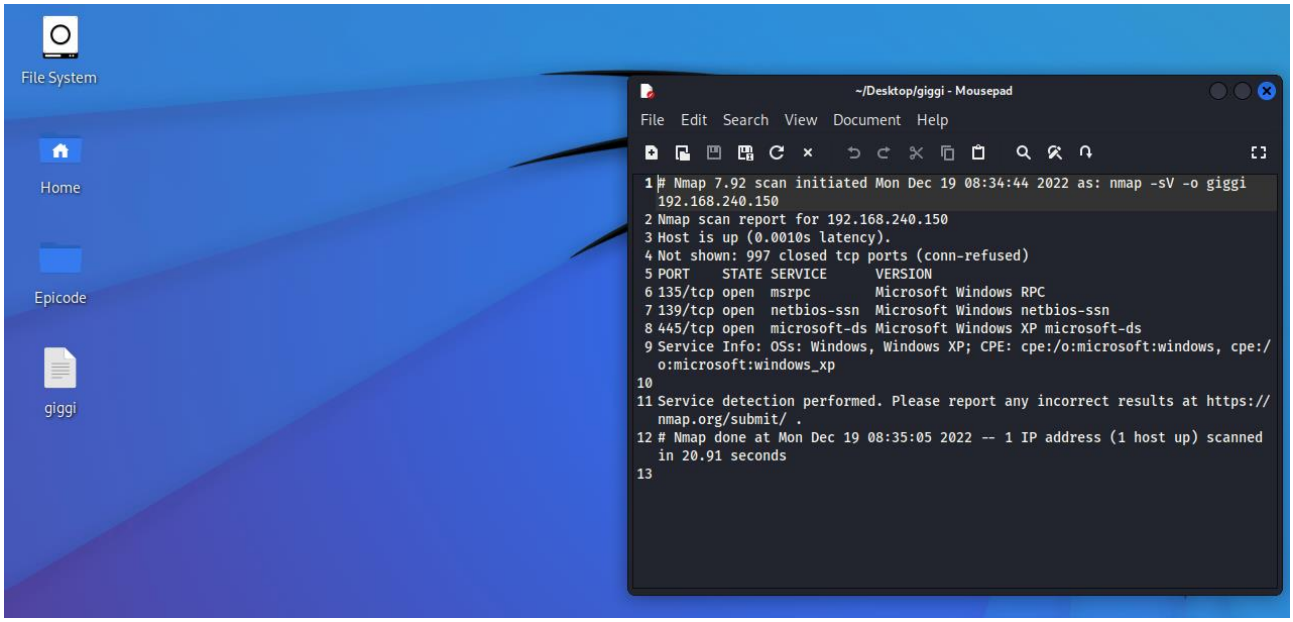


Da Kali, con il comando nmap –sV 192.168.240.150 –o giggi, andiamo ad effettuare la prima scansione con firewall non attivo che ci darà come risultato le porte aperte e le versioni dei servizi attivi:

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -sV 192.168.240.150 -o giggi
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-19 08:34 EST
Nmap scan report for 192.168.240.150
Host is up (0.0010s 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 20.91 seconds
```

Con –o creiamo un file con i risultati della scansione:



Attiviamo ora il firewall e riproviamo lo scan sempre con lo stesso comando:

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -sV 192.168.240.150 -o giggi2
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-19 08:44 EST
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 3.68 seconds
```

Come possiamo vedere dall'immagine, Nmap non è riuscito a stabilire una connessione con la macchina XP in quanto il firewall, una volta attivo, blocca il traffico di pacchetti a meno che non ci sia una regola che dica il contrario.

Vediamo anche dal file di log come vicino al tipo di pacchetto, in questo caso TCP, ci sia la scritta DROP che significa che il firewall ha scartato i pacchetti provenienti dall' IP 192.168.240.100: