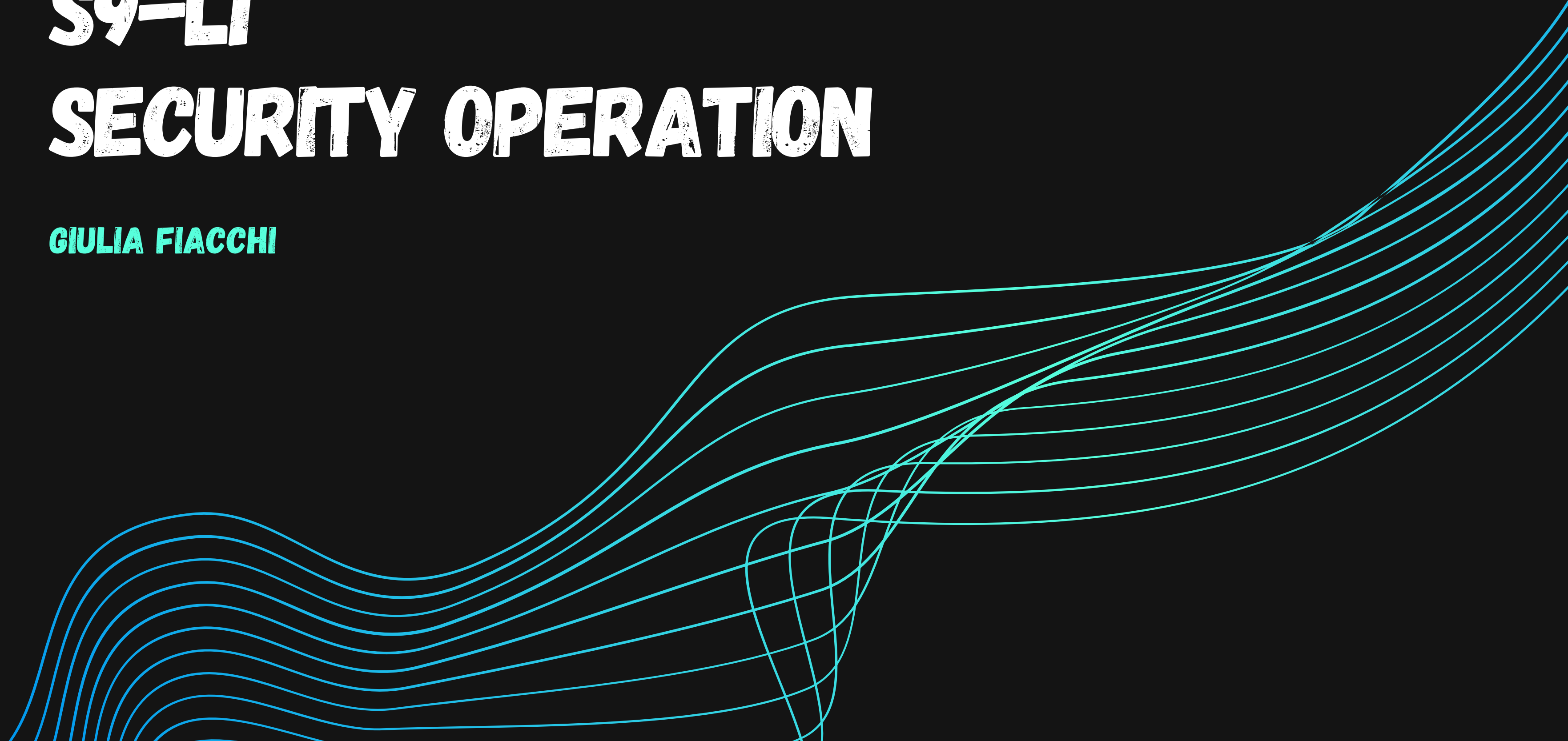


**S9-L1**

# **SECURITY OPERATION**

**GIULIA FIACCHI**



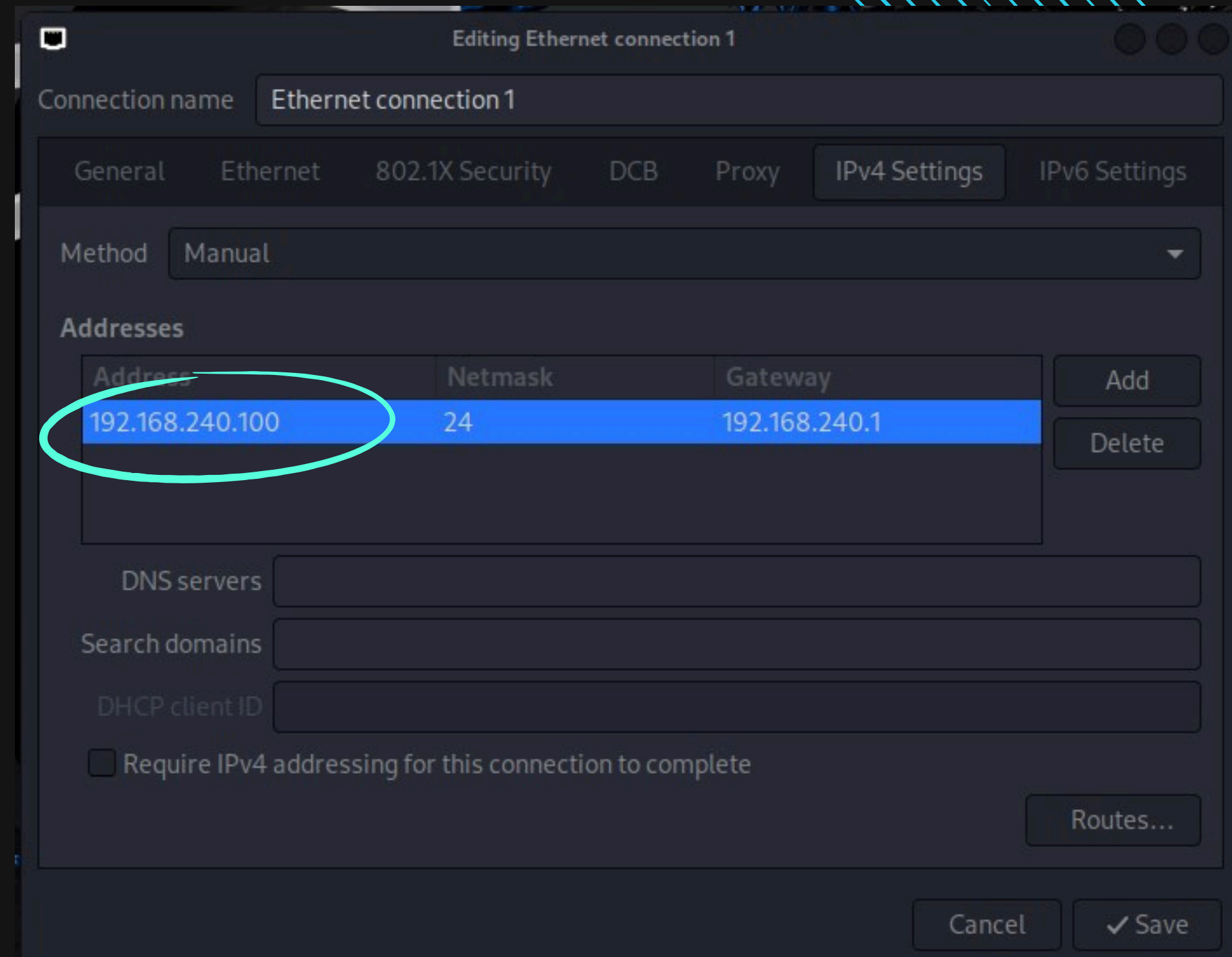
# PARTE 1

## CONFIGURAZIONE IP

192.168.240.100

Per prima cosa apriamo la kali e configuriamo l'IP.

Poi con "ip a" verifichiamo che sia andato a buon fine



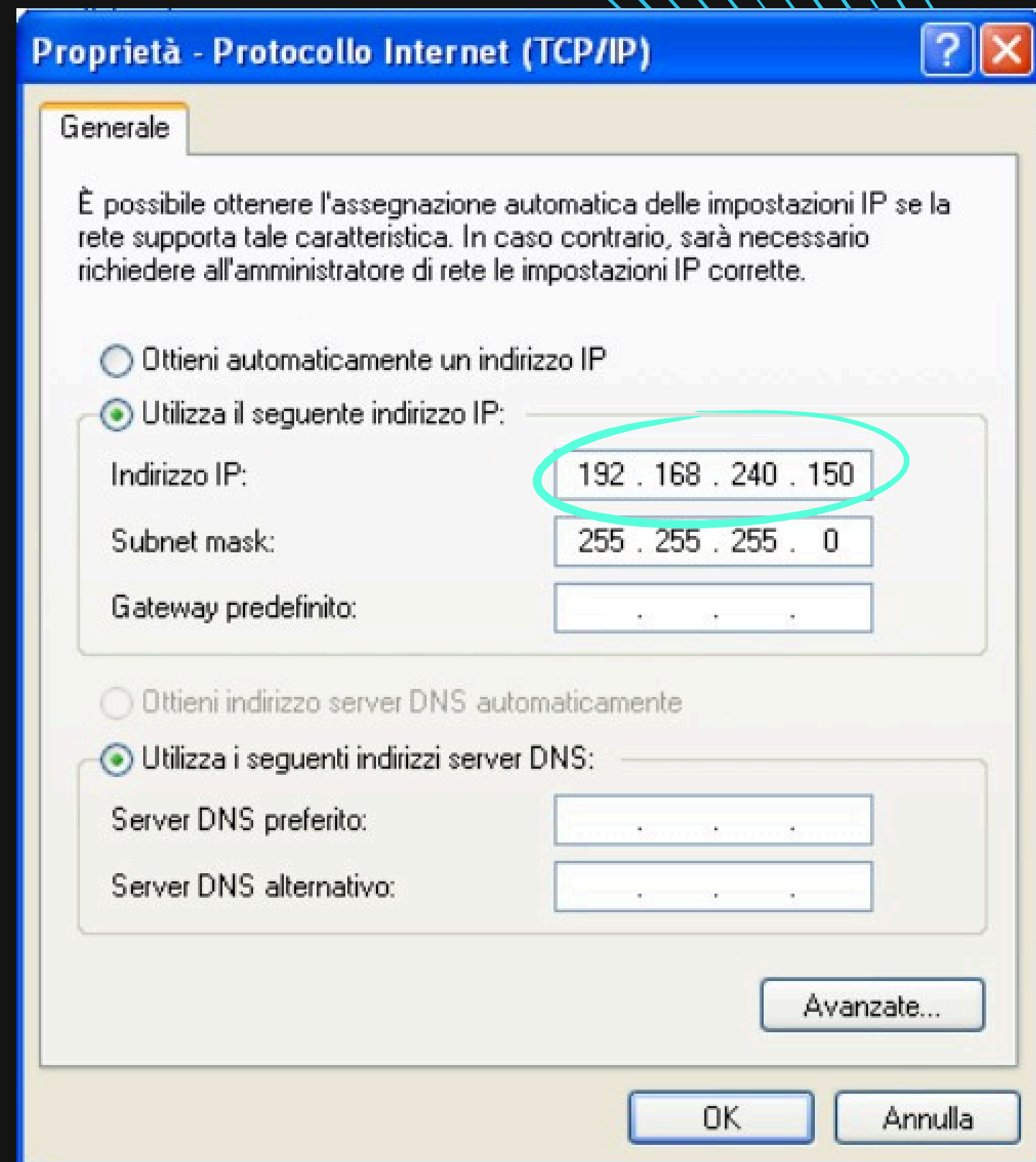
# PARTE 1

## CONFIGURAZIONE IP

192.168.240.150

Poi ci spostiamo su windows XP e anche qui modifichiamo l'IP.

Poi verifichiamo con il comando "ipconfig".



# PARTE 2

## PING TRA MACCHINE

Per verificare che la macchine comunicassero tra di loro abbiamo poi eseguito il comando:

**ping -c4 192.168.240.150 da Kali**

**ping 192.168.240.100 da Windows**

```
(kali㉿kali)-[~]  
$ ping -c4 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=2.55 ms  
64 bytes from 192.168.240.150: icmp_seq=2 ttl=128 time=2.33 ms  
64 bytes from 192.168.240.150: icmp_seq=3 ttl=128 time=1.15 ms  
64 bytes from 192.168.240.150: icmp_seq=4 ttl=128 time=2.04 ms  
  
— 192.168.240.150 ping statistics —  
4 packets transmitted, 4 received, 0% packet loss, time 3045ms  
rtt min/avg/max/mdev = 1.152/2.017/2.551/0.532 ms
```

```
C:\Documents and Settings\Administrator>ping 192.168.240.100  
Esecuzione di Ping 192.168.240.100 con 32 byte di dati:  
Risposta da 192.168.240.100: byte=32 durata=1ms TTL=64  
Risposta da 192.168.240.100: byte=32 durata=1ms TTL=64  
Risposta da 192.168.240.100: byte=32 durata=1ms TTL=64  
Risposta da 192.168.240.100: byte=32 durata<1ms TTL=64  
  
Statistiche Ping per 192.168.240.100:  
Pacchetti: Trasmessi = 4, Ricevuti = 4, Persi = 0 (0% persi),  
Tempo approssimativo percorsi andata/ritorno in millisecondi:  
Minimo = 0ms, Massimo = 1ms, Medio = 0ms
```

# PARTE 3

## CREAZIONE DI UN FILE REPORT

Come richiesto dalla traccia sarà necessario creare un file report.txt e perciò eseguiamo il comando:

**nano report.txt**

e poi salviamo.



```
(kali@kali)~  
$ nano report.txt
```



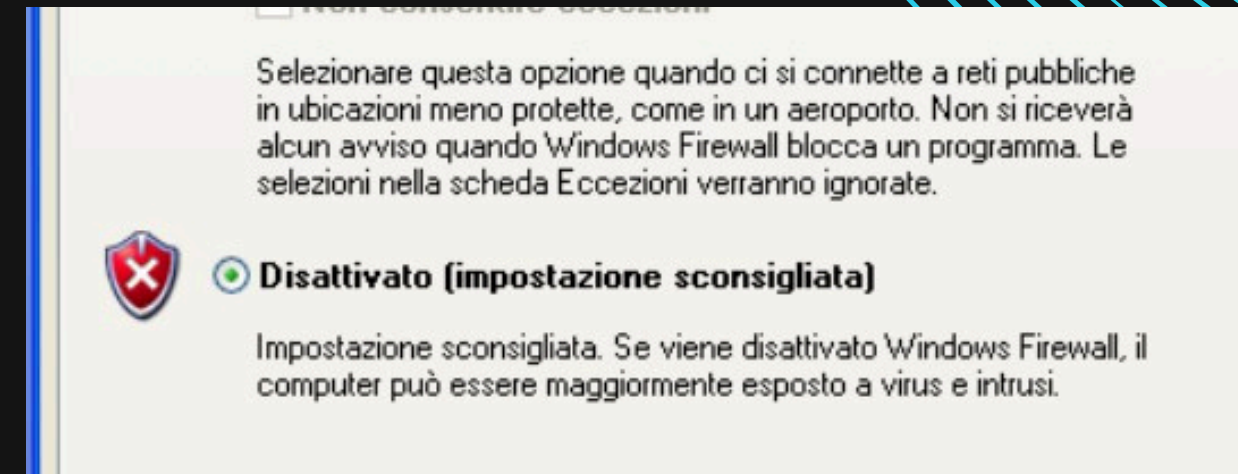
# PARTE 4

## SCANSIONE NMAP – FIREWALL DISATTIVATO

Ora procediamo con le scansioni ma, prima ci assicuriamo che il firewall sia disattivato su Windows XP.

Eseguiamo la scansione con il comando:

**nmap -sV -o report.txt 192.168.240.150**



```
(kali@kali)-[~]
$ nmap -sV -o report.txt 192.168.240.150

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 08:11 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using
--system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.240.150
Host is up (0.0027s 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 7.17 seconds
```

# PARTE 5

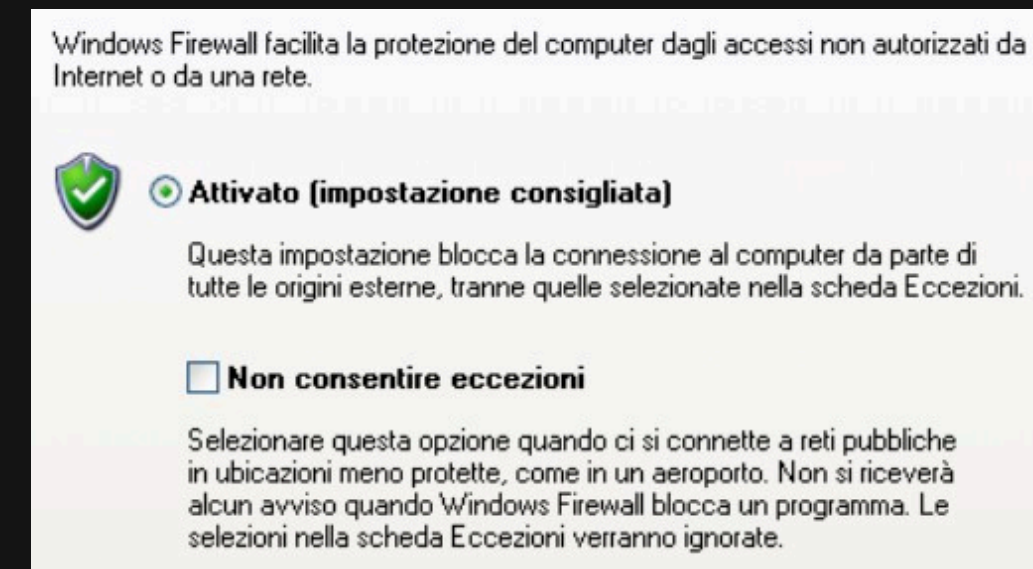
## SCANSIONE NMAP – FIREWALL ATTIVATO

Andiamo quindi ad eseguire la seconda scansione ma, con il firewall attivo.

E sempre con il comando:

```
nmap -sV -o report.txt 192.168.240.150
```

avviamo la scansione ma, non va a buon fine.



```
(kali@kali)-[~]  
$ nmap -sV -o report.txt 192.168.240.150  
  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 08:12 EDT  
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using  
--system-dns or specify valid servers with --dns-servers  
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 3.34 seconds
```



# PARTE 5

## SCANSIONE NMAP – FIREWALL ATTIVATO (ALTERNATIVA)

Provando però con il comando

**nmap -Pn -sV -o report.txt 192.168.240.150**

avviamo la scansione e osserviamo che riesce a scansionare andando a disabilitare il ping per verificare se l'host è attivo; possiamo notare che ci darà solo due porte e non anche la 135 .

```
(kali㉿kali)-[~]  
$ nmap -Pn -sV -o report.txt 192.168.240.150  
  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 08:14 EDT  
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using  
--system-dns or specify valid servers with --dns-servers  
Nmap scan report for 192.168.240.150  
Host is up (0.0063s latency).  
Not shown: 998 filtered tcp ports (no-response)  
PORT      STATE SERVICE      VERSION  
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/submi  
t/ .  
Nmap done: 1 IP address (1 host up) scanned in 13.31 seconds
```



# PARTE 6

*Che differenze notate? E quale può essere la causa del risultato diverso?*

## DIFFERENZE E CONSIDERAZIONI

Confrontando i risultati ottenuti, notiamo che con il firewall disattivato abbiamo accesso a tutte le porte, in particolare a **135 - 139 - 445**, mentre con il firewall attivo molte delle porte che erano visibili con il Firewall disattivato potrebbero non apparire nella scansione, poiché il Firewall blocca l'accesso a queste porte.

Il risultato diverso è dovuto al Firewall che blocca il traffico in entrata su molte porte, filtra i pacchetti sospetti o non autorizzati, rispondendo con pacchetti di reset (RST) o semplicemente ignorando le richieste e che le regole di sicurezza del Firewall possono essere configurate per permettere solo determinati tipi di traffico

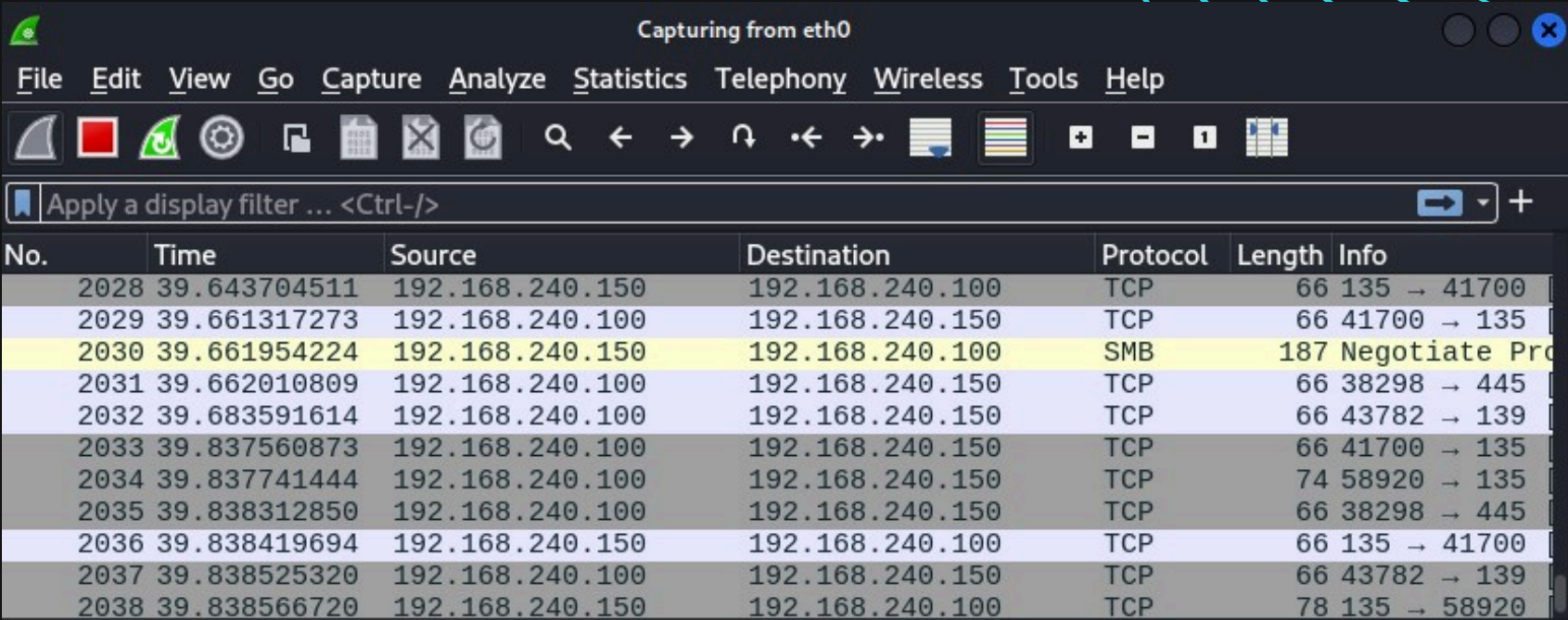
# PARTE 7

## WIRESHARK

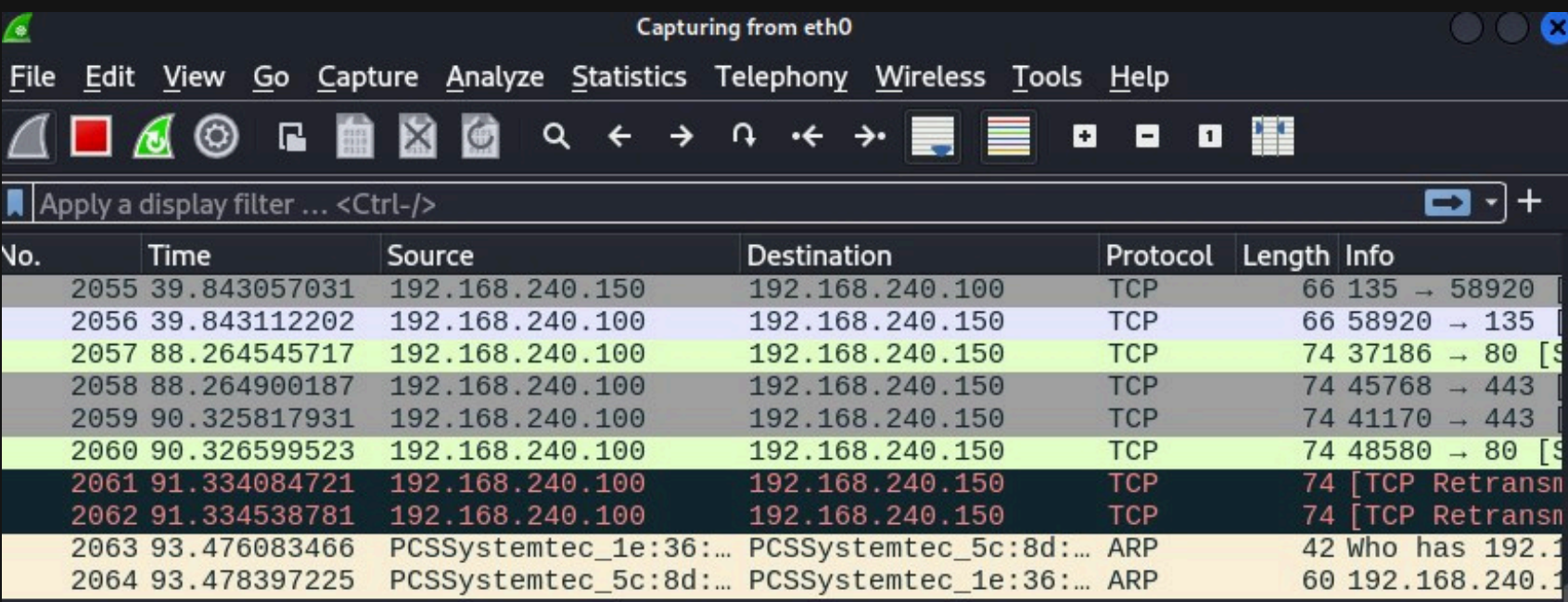
Adesso proviamo ad osservare l'andamento delle scansioni con Wireshark e quindi mettiamo in ascolto il servizio con il comando: **nc -lvp 192.168.240.150**

Poi avviamo le scansioni con gli stessi comandi di prima e lo facciamo sia con il firewall attivo che disattivo.

```
(kali@kali)-[~]  
$ nc -lvp 192.168.240.150  
listening on [any] 192 ...  
[ ]
```



No.	Time	Source	Destination	Protocol	Length	Info
2028	39.643704511	192.168.240.150	192.168.240.100	TCP	66	135 → 41700
2029	39.661317273	192.168.240.100	192.168.240.150	TCP	66	41700 → 135
2030	39.661954224	192.168.240.150	192.168.240.100	SMB	187	Negotiate Pro
2031	39.662010809	192.168.240.100	192.168.240.150	TCP	66	38298 → 445
2032	39.683591614	192.168.240.100	192.168.240.150	TCP	66	43782 → 139
2033	39.837560873	192.168.240.100	192.168.240.150	TCP	66	41700 → 135
2034	39.837741444	192.168.240.100	192.168.240.150	TCP	74	58920 → 135
2035	39.838312850	192.168.240.100	192.168.240.150	TCP	66	38298 → 445
2036	39.838419694	192.168.240.150	192.168.240.100	TCP	66	135 → 41700
2037	39.838525320	192.168.240.100	192.168.240.150	TCP	66	43782 → 139
2038	39.838566720	192.168.240.150	192.168.240.100	TCP	78	135 → 58920



No.	Time	Source	Destination	Protocol	Length	Info
2055	39.843057031	192.168.240.150	192.168.240.100	TCP	66	135 → 58920
2056	39.843112202	192.168.240.100	192.168.240.150	TCP	66	58920 → 135
2057	88.264545717	192.168.240.100	192.168.240.150	TCP	74	37186 → 80 [S
2058	88.264900187	192.168.240.100	192.168.240.150	TCP	74	45768 → 443
2059	90.325817931	192.168.240.100	192.168.240.150	TCP	74	41170 → 443
2060	90.326599523	192.168.240.100	192.168.240.150	TCP	74	48580 → 80 [S
2061	91.334084721	192.168.240.100	192.168.240.150	TCP	74	[TCP Retransn
2062	91.334538781	192.168.240.100	192.168.240.150	TCP	74	[TCP Retransn
2063	93.476083466	PCSSystemtec_1e:36:...	PCSSystemtec_5c:8d:...	ARP	42	Who has 192.1
2064	93.478397225	PCSSystemtec_5c:8d:...	PCSSystemtec_1e:36:...	ARP	60	192.168.240.1