**Dibujo de una persona

Descripción generada automáticamente con confianza baja**

SNORT

**CARLOS GONZÁLEZ MARTÍN**

Contenido

[1. Instalamos paquetes 3](#_Toc185420868)

[2. Modificación de archivos de configuración 4](#_Toc185420869)

[3. Comprobación ping 5](#_Toc185420870)

[4. Otros servicios 6](#_Toc185420871)

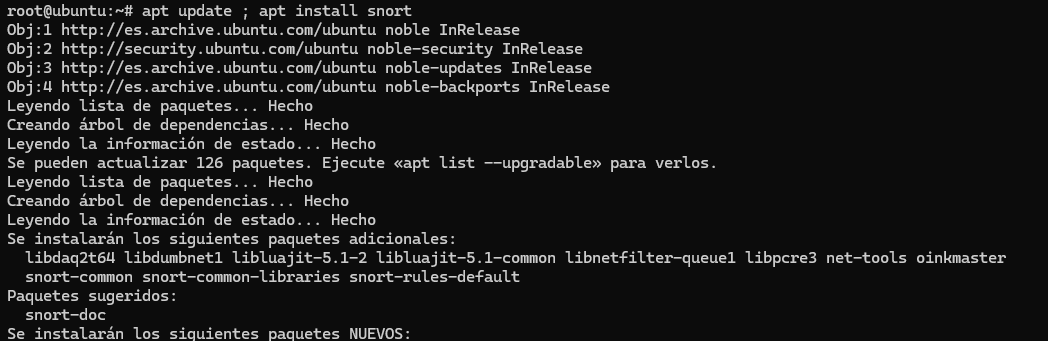
[5. Comprobación 6](#_Toc185420872)

[6. Bot telegram 7](#_Toc185420873)

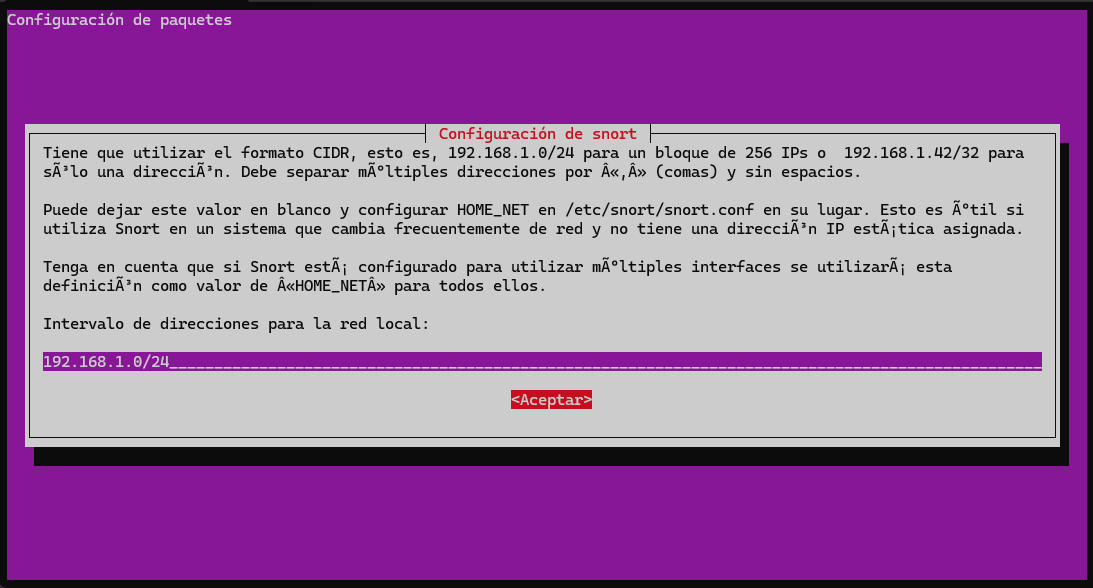
[7. Conclusión 13](#_Toc185420874)

# Instalamos paquetes

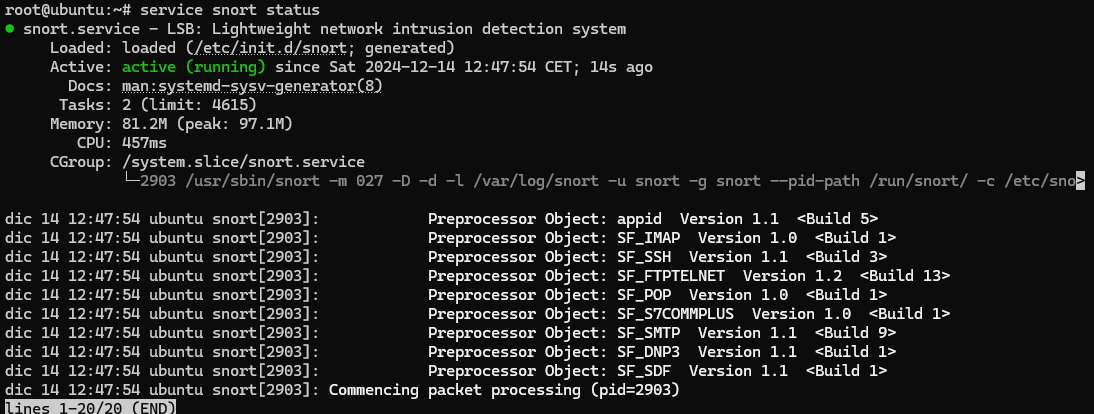
Ahora lo que haremos será instalar los paquetes, en este caso hemos usado Ubuntu, para poder descargándolo mediante el programa de paquetes apt, por que en caso de debían tenemos que usar git clone y luego instalarlo.



Mientras se instala nos saldrá la siguiente ventana, tendremos que indicarle la red donde vamos a estar usando snort, podemos dejarlo en blanco, ya que vamos a modificarlo mas adelante, pero es recomendable modificarlo ahora.



Una vez instalado vamos a ver si esta activado



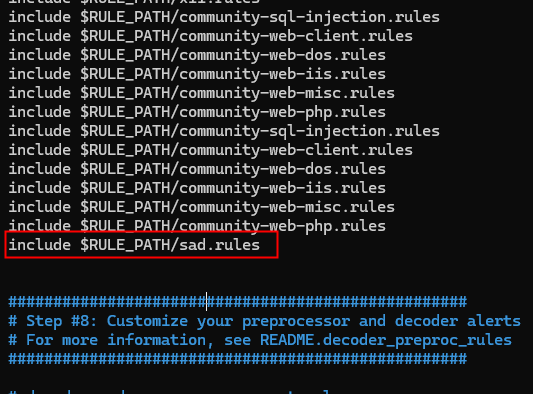
# Modificación de archivos de configuración

Una vez instalado con nano haremos una nueva regla llamada reglaSAD.rules dentro de /etc/snort/rules/reglaSAD.rules



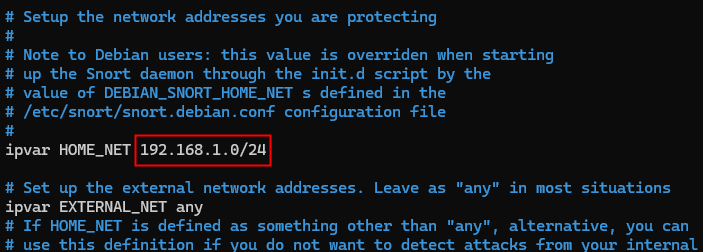
Lo que viene a decir esta regla es que detecte todas las peticiones icmp (ping) que recibe el servidor y que nos avise que se ha detectado un ping.

Una vez guardada la regla nos iremos con nano en /etc/snort/snort.conf para añadir la regla a snort y también modificar la dirección ip donde va a escuchar el equipo.



Añadimos la regla, esta casi al final del documento.

Ahora nos iremos al principio del documento y modificamos la línea de $HOME\_NET y en vez de dejarlo en any ponemos la ip donde tenemos la maquina

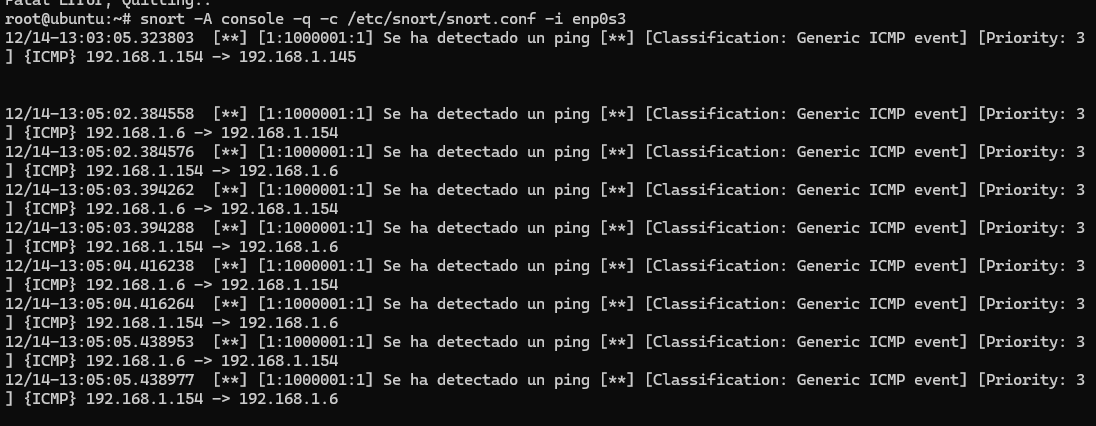


# Comprobación ping

Guardamos el archivo y pondremos el siguiente comando para ponernos en modo escucha.

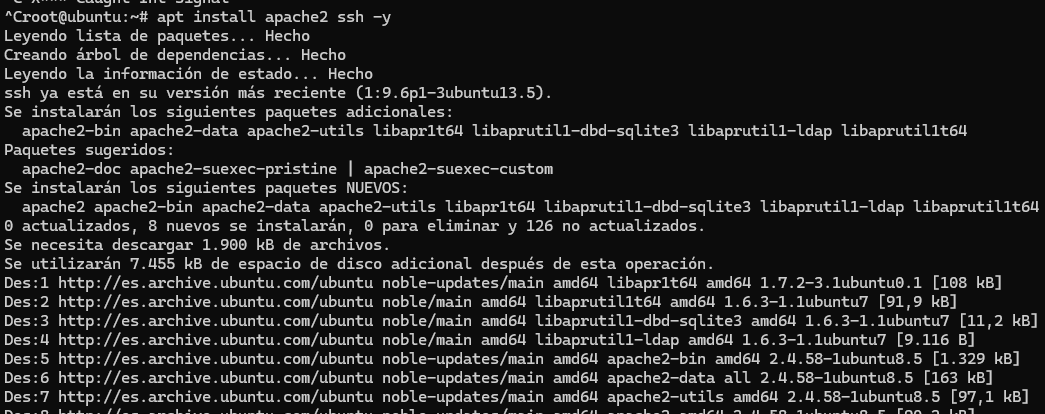


Mediante otro equipo hacemos un ping a la máquina.



# Otros servicios

Vemos que nos lo detecta, vamos a probar con otros servicios y configurar las reglas.



Copiaremos la regla que hemos hecho anteriormente y la modificaremos para que cuando solicitemos una pagina web del servidor nos avise.

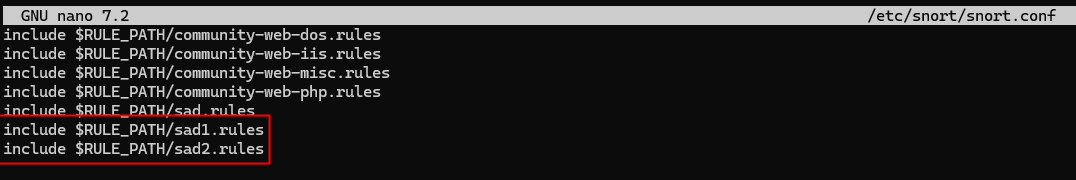


Ahora hacemos la regla para ssh





Sincronizamos las reglas en el archivo de configuración de snort para que pueda escuchar una petición http o ssh.

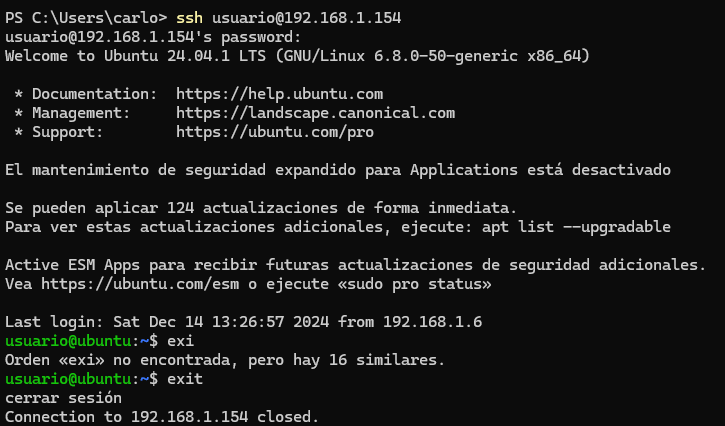


# Comprobación

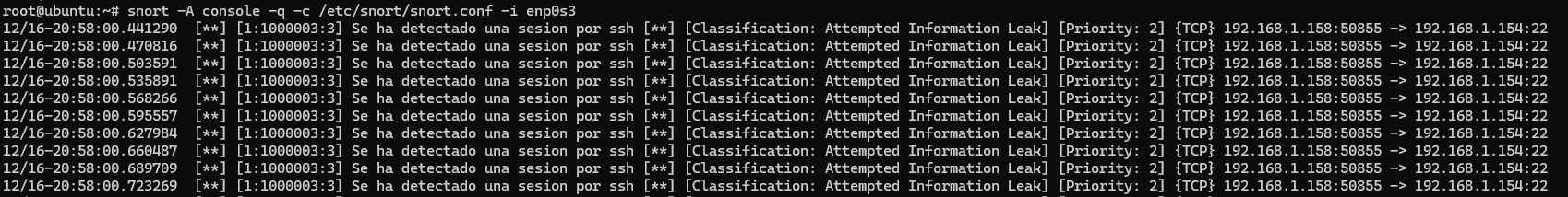
Nos ponemos en modo escucha.



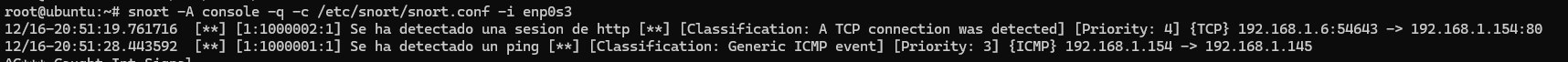
Con otro cliente hacemos una conexión por ssh.



Ahora nos iremos al server.



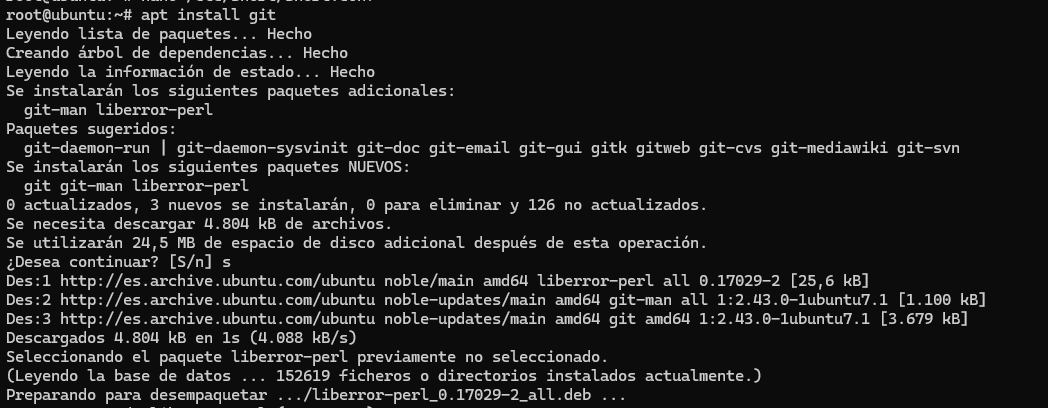
Ahora en el buscador escribiremos la IP.



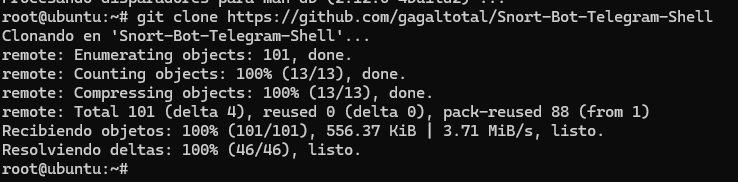
# Bot telegram

Ahora vamos a crear un Bot de telegram para que nos avise cada vez que hacen un ping, página web o ssh.

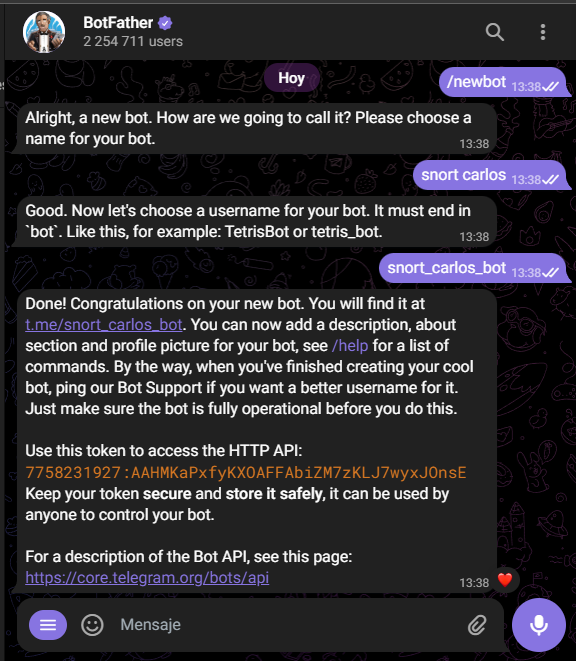
Lo primero será instalar git.



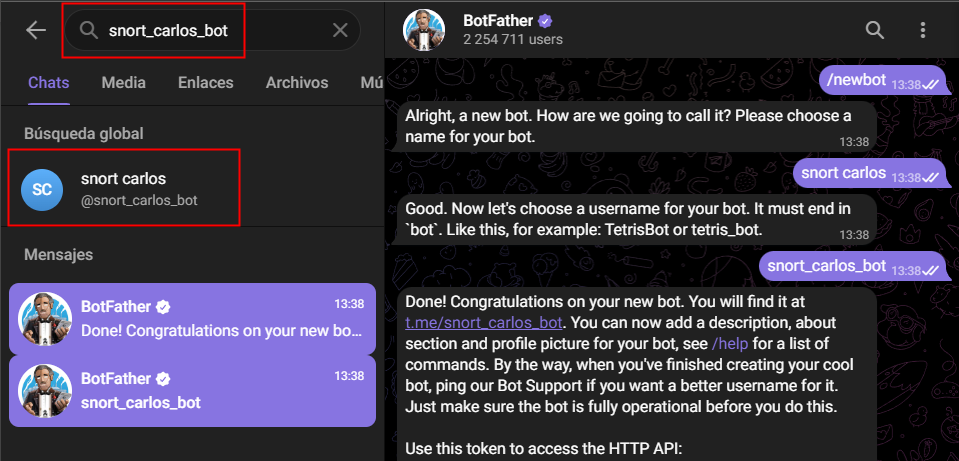
Y ahora nos descargaremos la herramienta.



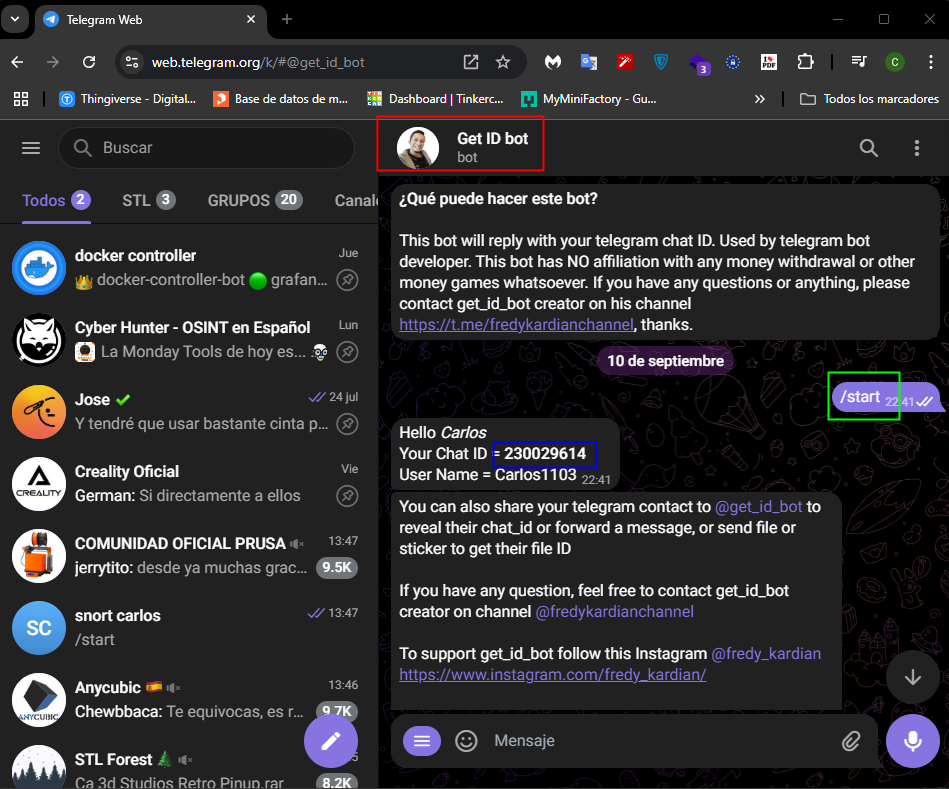
Ahora nos iremos a telegram y buscaremos @BotFather y crearemos un Bot nuevo.



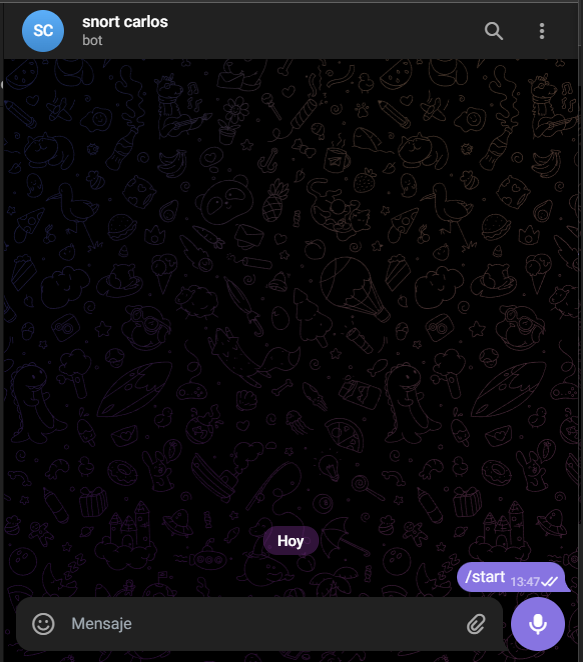
Ahora buscaremos el Bot en el buscador.



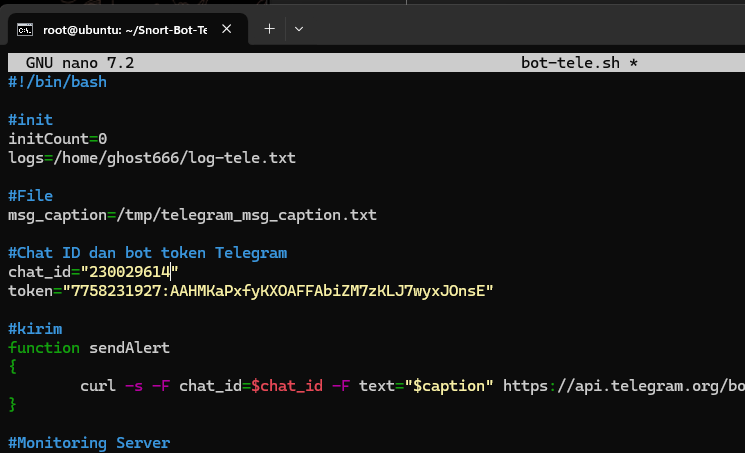
Una vez que tenemos el token https nos iremos al Bot @get\_id\_bot y nos dirá el ID del chat, en mi caso ya lo tenía creado para otros bots, pero es el mismo chat ID.



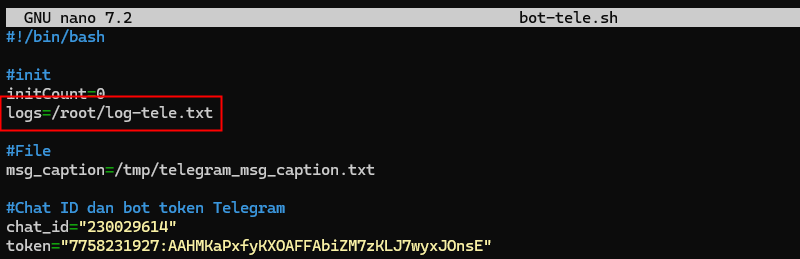
Ahora iniciaremos el Bot con el comando /start.

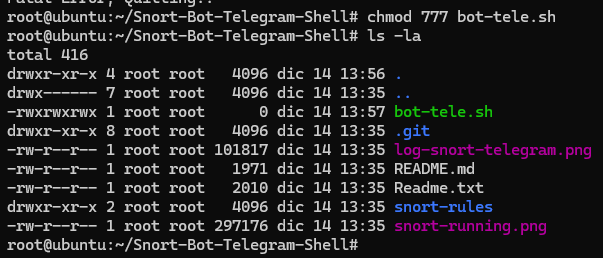


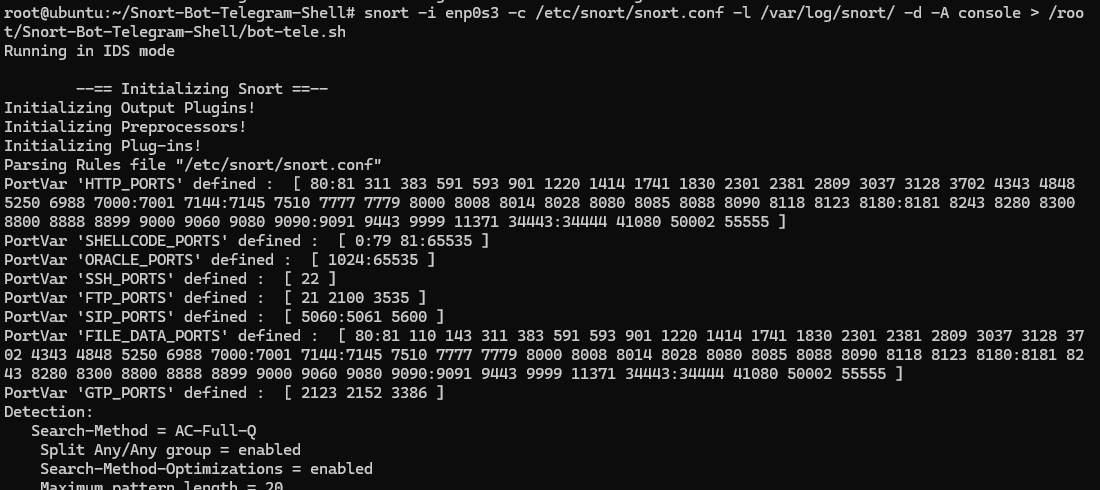
Y ahora copiaremos los valores que nos han ofrecido los bots en la configuración de bot-tele.sh



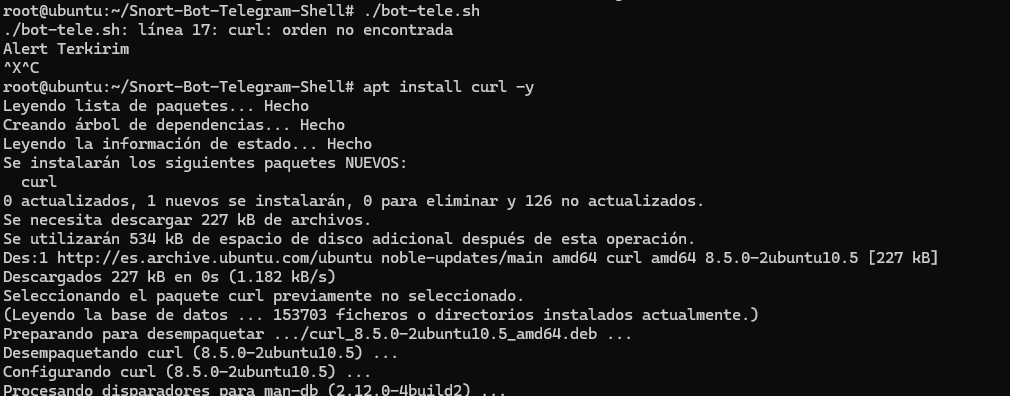
Por último, hay que indicarle donde guardara lo logs.



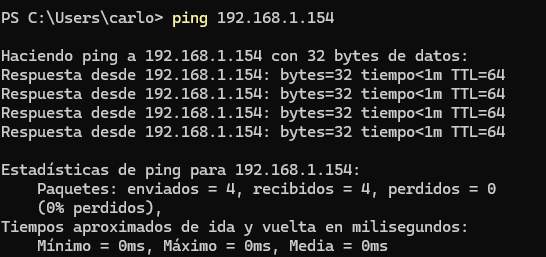


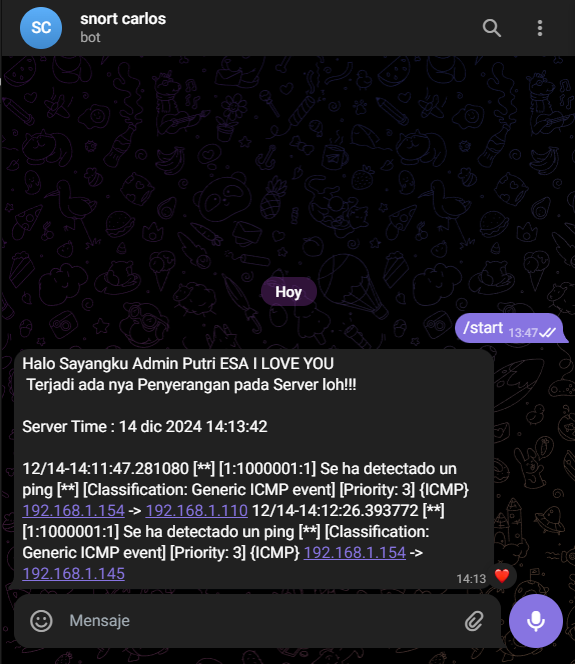


Ahora instalaremos curl por un fallo en la linea del script.



Haremos un ping en otro equipo y nos tiene que mandar un mensaje.





# Conclusión

La práctica con Snort permitió comprender su funcionamiento como IDS basado en análisis de paquetes y detección por firmas. Se configuraron reglas personalizadas y se evaluó su capacidad para identificar y registrar actividades maliciosas en tiempo real.

Snort demostró ser eficiente y flexible, aunque su eficacia depende de reglas bien definidas y de la minimización de falsos positivos. Esta experiencia resaltó la importancia de su integración en un entorno de seguridad para una detección temprana de intrusiones.