IES Valle Inclán

SNORT

CARLOS GONZÁLEZ MARTÍN

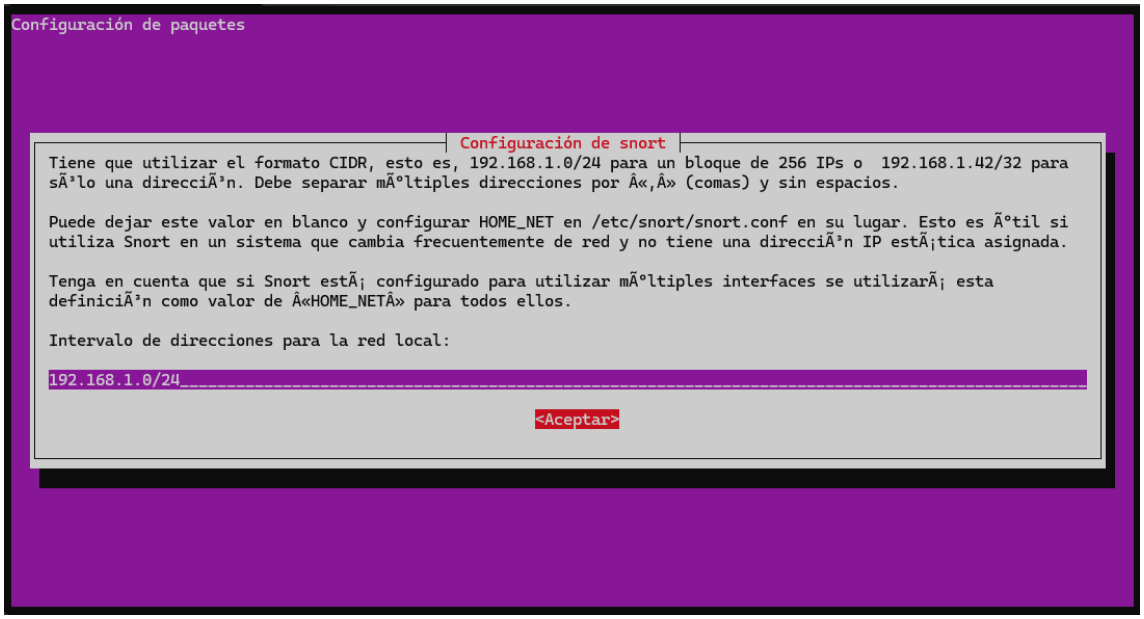
Contenido

1. Instalamos paquetes

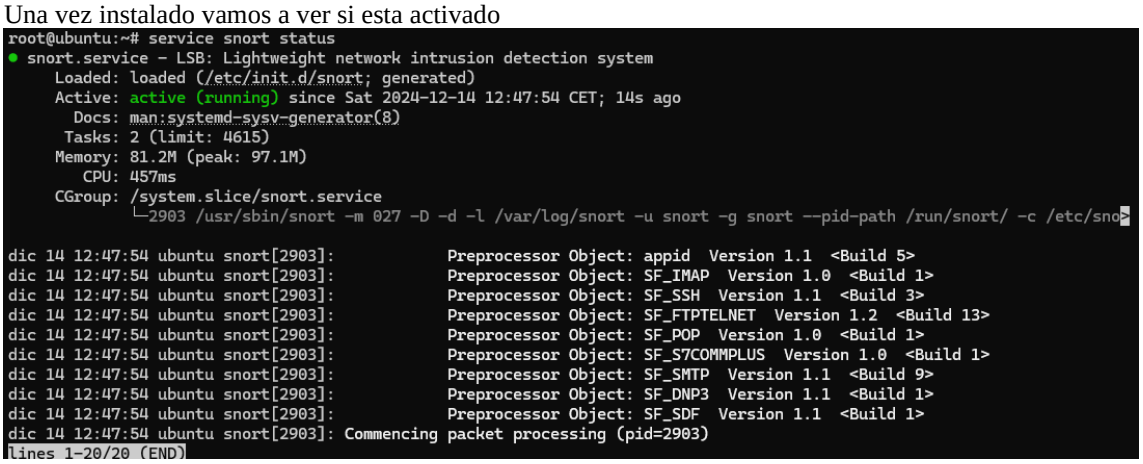
Ahora lo que haremos será instalar los paquetes, en este caso hemos usado Ubuntu, para poder descargándolo mediante el programa de paquetes apt, por que en caso de debían tenemos que usar git clone y luego instalarlo.

```
root@ubuntu:~# apt update ; apt install snort
Obj:1 http://es.archive.ubuntu.com/ubuntu noble InRelease
Obj:2 http://security.ubuntu.com/ubuntu noble-security InRelease
Obj:3 http://es.archive.ubuntu.com/ubuntu noble-updates InRelease
Obj:4 http://es.archive.ubuntu.com/ubuntu noble-backports InRelease
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se pueden actualizar 126 paquetes. Ejecute «apt list --upgradable» para verlos.
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  libdaq2t64 libdumbnet1 libluajit-5.1-2 libluajit-5.1-common libnetfilter-queue1 libpcre3 net-tools oinkmaster
  snort-common snort-common-libraries snort-rules-default
Paquetes sugeridos:
  snort-doc
Se instalarán los siguientes paquetes NUEVOS:
```

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.

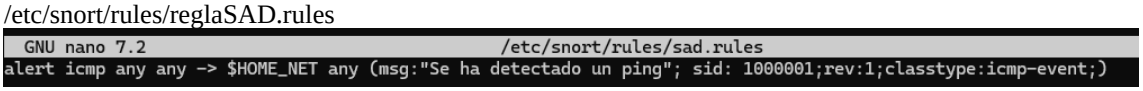


Una vez instalado vamos a ver si esta activado



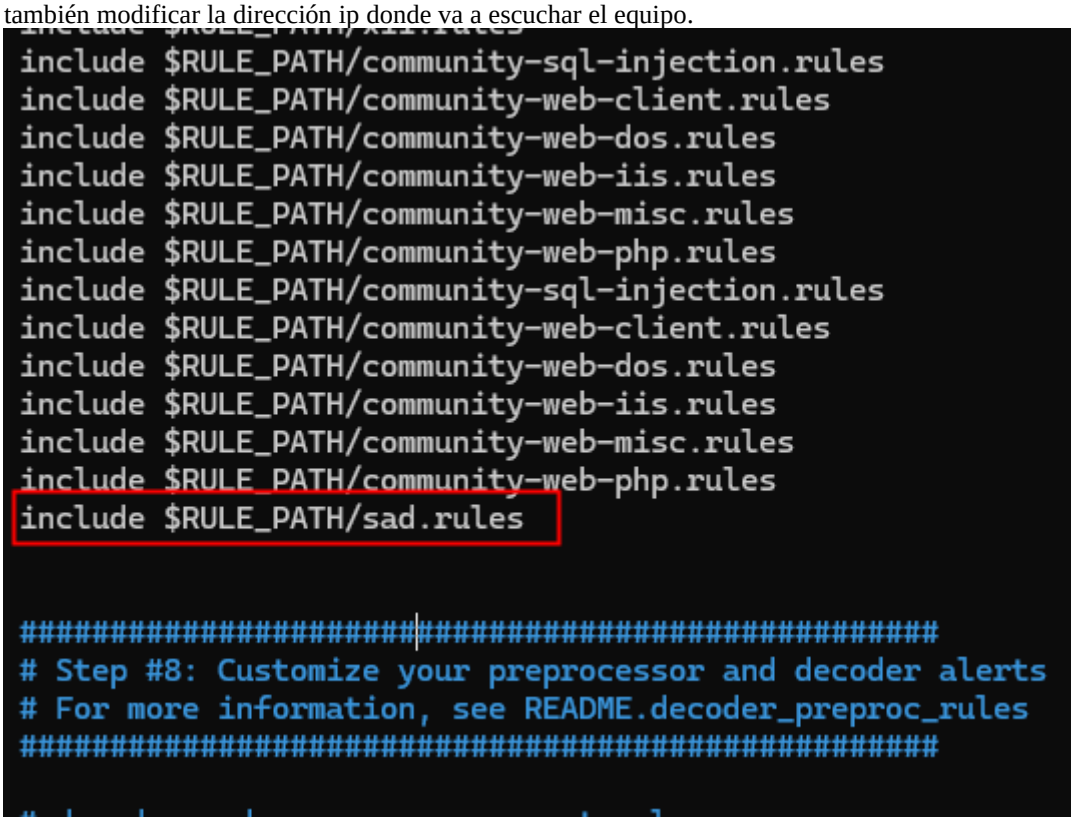
2. Modificación de archivos de configuración

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

```
# Setup the network addresses you are protecting
#
# Note to Debian users: this value is overriden when starting
# up the Snort daemon through the init.d script by the
# value of DEBIAN_SNORT_HOME_NET s defined in the
# /etc/snort/snort.debian.conf configuration file
#
ipvar HOME_NET 192.168.1.0/24

# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET any
# If HOME_NET is defined as something other than "any", alternative, you can
# use this definition if you do not want to detect attacks from your internal
```

3. Comprobación ping

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

```
root@ubuntu:~# snort -A console -q -c /etc/snort/snort.conf -i enp0s3
```

Mediante otro equipo hacemos un ping a la máquina.

```
root@ubuntu:~# snort -A console -q -c /etc/snort/snort.conf -i enp0s3
12/14-13:03:05.323803  [**] [1:1000001:1] Se ha detectado un ping [**] [Classification: Generic ICMP event] [Priority: 3
] {ICMP} 192.168.1.154 -> 192.168.1.145


12/14-13:05:02.384558  [**] [1:1000001:1] Se ha detectado un ping [**] [Classification: Generic ICMP event] [Priority: 3
] {ICMP} 192.168.1.6 -> 192.168.1.154
12/14-13:05:02.384576  [**] [1:1000001:1] Se ha detectado un ping [**] [Classification: Generic ICMP event] [Priority: 3
] {ICMP} 192.168.1.154 -> 192.168.1.6
12/14-13:05:03.394262  [**] [1:1000001:1] Se ha detectado un ping [**] [Classification: Generic ICMP event] [Priority: 3
] {ICMP} 192.168.1.6 -> 192.168.1.154
12/14-13:05:03.394288  [**] [1:1000001:1] Se ha detectado un ping [**] [Classification: Generic ICMP event] [Priority: 3
] {ICMP} 192.168.1.154 -> 192.168.1.6
12/14-13:05:04.416238  [**] [1:1000001:1] Se ha detectado un ping [**] [Classification: Generic ICMP event] [Priority: 3
] {ICMP} 192.168.1.6 -> 192.168.1.154
12/14-13:05:04.416264  [**] [1:1000001:1] Se ha detectado un ping [**] [Classification: Generic ICMP event] [Priority: 3
] {ICMP} 192.168.1.154 -> 192.168.1.6
12/14-13:05:05.438953  [**] [1:1000001:1] Se ha detectado un ping [**] [Classification: Generic ICMP event] [Priority: 3
] {ICMP} 192.168.1.6 -> 192.168.1.154
12/14-13:05:05.438977  [**] [1:1000001:1] Se ha detectado un ping [**] [Classification: Generic ICMP event] [Priority: 3
] {ICMP} 192.168.1.154 -> 192.168.1.6
```

4. Otros servicios

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

```
^Croot@ubuntu:~# apt install apache2 ssh -y
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
ssh ya está en su versión más reciente (1:9.6p1-3ubuntu13.5).
Se instalarán los siguientes paquetes adicionales:
  apache2-bin apache2-data apache2-utils libapr1t64 libaprutil1-dbd-sqlite3 libaprutil1-ldap libaprutil1t64
Paquetes sugeridos:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom
Se instalarán los siguientes paquetes NUEVOS:
  apache2 apache2-bin apache2-data apache2-utils libapr1t64 libaprutil1-dbd-sqlite3 libaprutil1-ldap libaprutil1t64
0 actualizados, 8 nuevos se instalarán, 0 para eliminar y 126 no actualizados.
Se necesita descargar 1.900 kB de archivos.
Se utilizarán 7.455 kB de espacio de disco adicional después de esta operación.
Des:1 http://es.archive.ubuntu.com/ubuntu noble-updates/main amd64 libapr1t64 amd64 1.7.2-3.1ubuntu0.1 [108 kB]
Des:2 http://es.archive.ubuntu.com/ubuntu noble/main amd64 libaprutil1t64 amd64 1.6.3-1.1ubuntu7 [91,9 kB]
Des:3 http://es.archive.ubuntu.com/ubuntu noble/main amd64 libaprutil1-dbd-sqlite3 amd64 1.6.3-1.1ubuntu7 [11,2 kB]
Des:4 http://es.archive.ubuntu.com/ubuntu noble/main amd64 libaprutil1-ldap amd64 1.6.3-1.1ubuntu7 [9.116 B]
Des:5 http://es.archive.ubuntu.com/ubuntu noble-updates/main amd64 apache2-bin amd64 2.4.58-1ubuntu8.5 [1.329 kB]
Des:6 http://es.archive.ubuntu.com/ubuntu noble-updates/main amd64 apache2-data all 2.4.58-1ubuntu8.5 [163 kB]
Des:7 http://es.archive.ubuntu.com/ubuntu noble-updates/main amd64 apache2-utils amd64 2.4.58-1ubuntu8.5 [97,1 kB]
```

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

```
  GNU nano 7.2                                                    /etc/snort/rules/sad1.rules
alert tcp any any -> $HOME_NET 80 (msg:"Se ha detectado una sesion de http"; sid: 1000002;rev:1;classtype:tcp-connection;)
```

Ahora hacemos la regla para ssh

```
root@ubuntu:~# cp /etc/snort/rules/sad1.rules /etc/snort/rules/sad2.rules
root@ubuntu:~# nano /etc/snort/rules/sad2.rules
```

```
  GNU nano 7.2                                                    /etc/snort/rules/sad2.rules
alert icmp any any -> $HOME_NET 22 (msg:"Se ha detectado una sesion por ssh"; sid: 1000001;rev:1;classtype:tcp-connection;)
```

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

```
  GNU nano 7.2                                                    /etc/snort/snort.conf
include $RULE_PATH/community-web-dos.rules
include $RULE_PATH/community-web-iis.rules
include $RULE_PATH/community-web-misc.rules
include $RULE_PATH/community-web-php.rules
include $RULE_PATH/sad.rules
include $RULE_PATH/sad1.rules
include $RULE_PATH/sad2.rules
```

5. Comprobación

Nos ponemos en modo escucha.

```
root@ubuntu:~# snort -A console -q -c /etc/snort/snort.conf -i enp0s3
```

Con otro cliente hacemos una conexión por ssh.

```
PS C:\Users\carlo> ssh usuario@192.168.1.154
usuario@192.168.1.154's password:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-50-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

El mantenimiento de seguridad expandido para Applications está desactivado

Se pueden aplicar 124 actualizaciones de forma inmediata.
Para ver estas actualizaciones adicionales, ejecute: apt list --upgradable

Active ESM Apps para recibir futuras actualizaciones de seguridad adicionales.
Vea https://ubuntu.com/esm o ejecute «sudo pro status»

Last login: Sat Dec 14 13:26:57 2024 from 192.168.1.6
usuario@ubuntu:~$ exi
Orden «exi» no encontrada, pero hay 16 similares.
usuario@ubuntu:~$ exit
cerrar sesión
Connection to 192.168.1.154 closed.
```

Ahora nos iremos al server.

```
root@ubuntu:~# snort -A console -q -c /etc/snort/snort.conf -i enp0s3
12/16-20:58:00.441290  [**] [1:1000003:3] Se ha detectado una sesion por ssh [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.1.158:50855 -> 192.168.1.154:22
12/16-20:58:00.470816  [**] [1:1000003:3] Se ha detectado una sesion por ssh [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.1.158:50855 -> 192.168.1.154:22
12/16-20:58:00.503591  [**] [1:1000003:3] Se ha detectado una sesion por ssh [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.1.158:50855 -> 192.168.1.154:22
12/16-20:58:00.535891  [**] [1:1000003:3] Se ha detectado una sesion por ssh [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.1.158:50855 -> 192.168.1.154:22
12/16-20:58:00.568266  [**] [1:1000003:3] Se ha detectado una sesion por ssh [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.1.158:50855 -> 192.168.1.154:22
12/16-20:58:00.595557  [**] [1:1000003:3] Se ha detectado una sesion por ssh [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.1.158:50855 -> 192.168.1.154:22
12/16-20:58:00.627984  [**] [1:1000003:3] Se ha detectado una sesion por ssh [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.1.158:50855 -> 192.168.1.154:22
12/16-20:58:00.660487  [**] [1:1000003:3] Se ha detectado una sesion por ssh [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.1.158:50855 -> 192.168.1.154:22
12/16-20:58:00.689709  [**] [1:1000003:3] Se ha detectado una sesion por ssh [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.1.158:50855 -> 192.168.1.154:22
12/16-20:58:00.723269  [**] [1:1000003:3] Se ha detectado una sesion por ssh [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.1.158:50855 -> 192.168.1.154:22
```

Ahora en el buscador escribiremos la IP.

```
root@ubuntu:~# snort -A console -q -c /etc/snort/snort.conf -i enp0s3
12/16-20:51:19.761716  [**] [1:1000002:1] Se ha detectado una sesion de http [**] [Classification: A TCP connection was detected] [Priority: 4] {TCP} 192.168.1.6:54643 -> 192.168.1.154:80
12/16-20:51:28.443592  [**] [1:1000001:1] Se ha detectado un ping [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.1.154 -> 192.168.1.145
```

6. Bot telegram

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

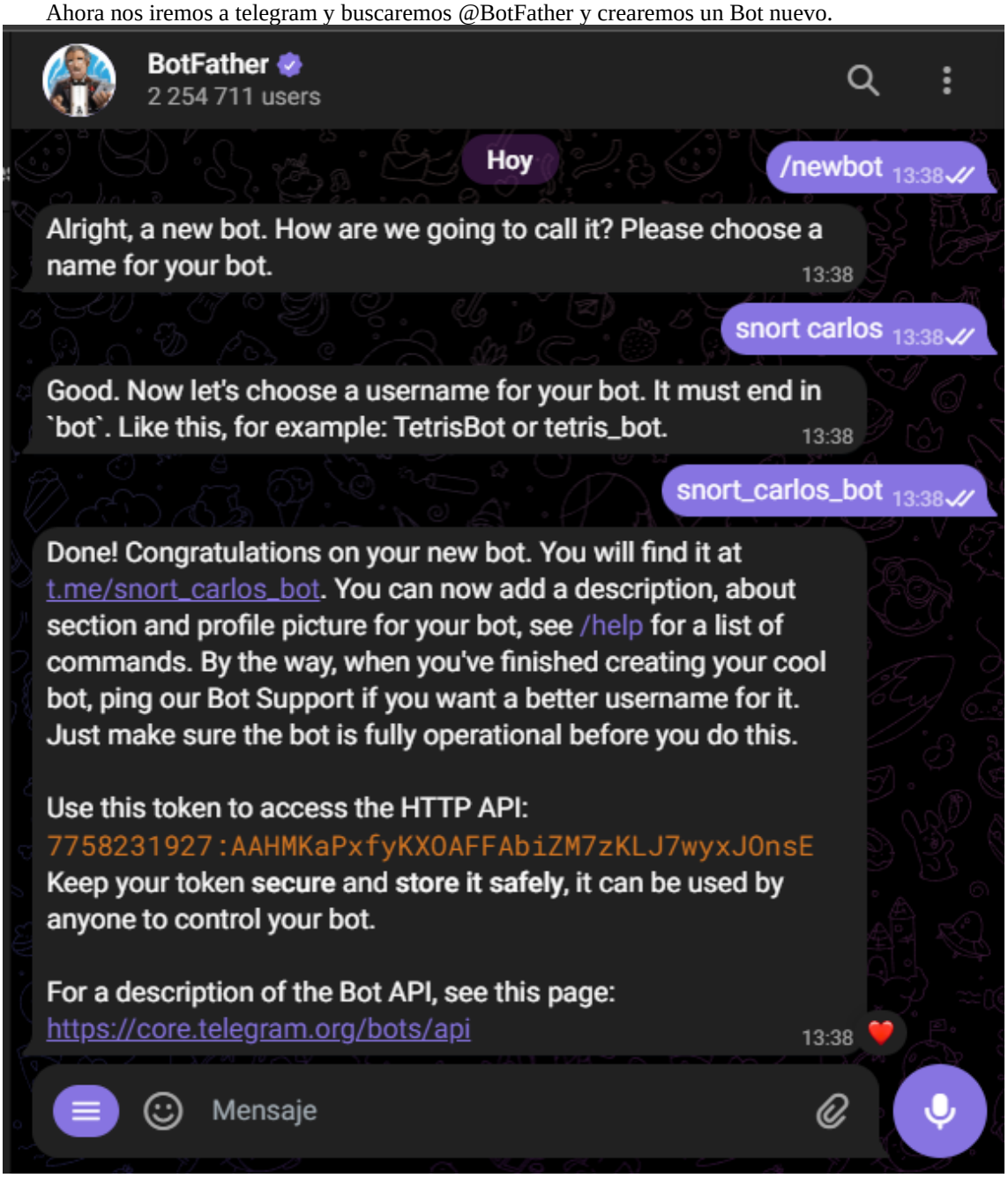
Lo primero será instalar git.

```
root@ubuntu:~# apt install git
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  git-man liberror-perl
Paquetes sugeridos:
  git-daemon-run | git-daemon-sysvinit git-doc git-email git-gui gitk gitweb git-cvs git-mediawiki git-svn
Se instalarán los siguientes paquetes NUEVOS:
  git git-man liberror-perl
0 actualizados, 3 nuevos se instalarán, 0 para eliminar y 126 no actualizados.
Se necesita descargar 4.804 kB de archivos.
Se utilizarán 24,5 MB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] s
Des:1 http://es.archive.ubuntu.com/ubuntu noble/main amd64 liberror-perl all 0.17029-2 [25,6 kB]
Des:2 http://es.archive.ubuntu.com/ubuntu noble-updates/main amd64 git-man all 1:2.43.0-1ubuntu7.1 [1.100 kB]
Des:3 http://es.archive.ubuntu.com/ubuntu noble-updates/main amd64 git amd64 1:2.43.0-1ubuntu7.1 [3.679 kB]
Descargados 4.804 kB en 1s (4.088 kB/s)
Seleccionando el paquete liberror-perl previamente no seleccionado.
(Leyendo la base de datos ... 152619 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar .../liberror-perl_0.17029-2_all.deb ...
```

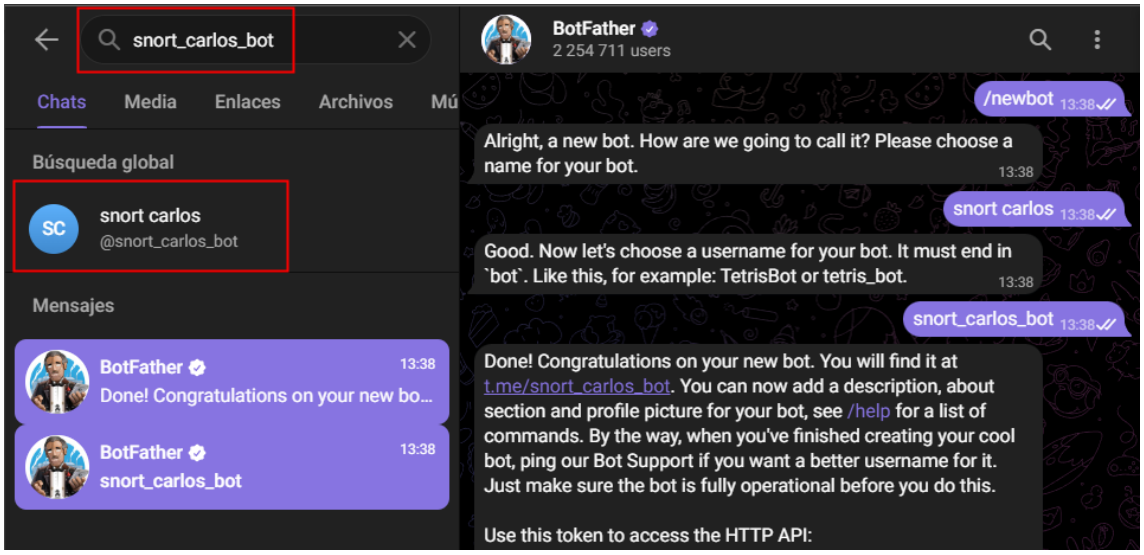
Y ahora nos descargaremos la herramienta.

```
root@ubuntu:~# git clone https://github.com/gagaltotal/Snort-Bot-Telegram-Shell
Clonando en 'Snort-Bot-Telegram-Shell'...
remote: Enumerating objects: 101, done.
remote: Counting objects: 100% (13/13), done.
remote: Compressing objects: 100% (13/13), done.
remote: Total 101 (delta 4), reused 0 (delta 0), pack-reused 88 (from 1)
Recibiendo objetos: 100% (101/101), 556.37 KiB | 3.71 MiB/s, listo.
Resolviendo deltas: 100% (46/46), listo.
root@ubuntu:~#
```

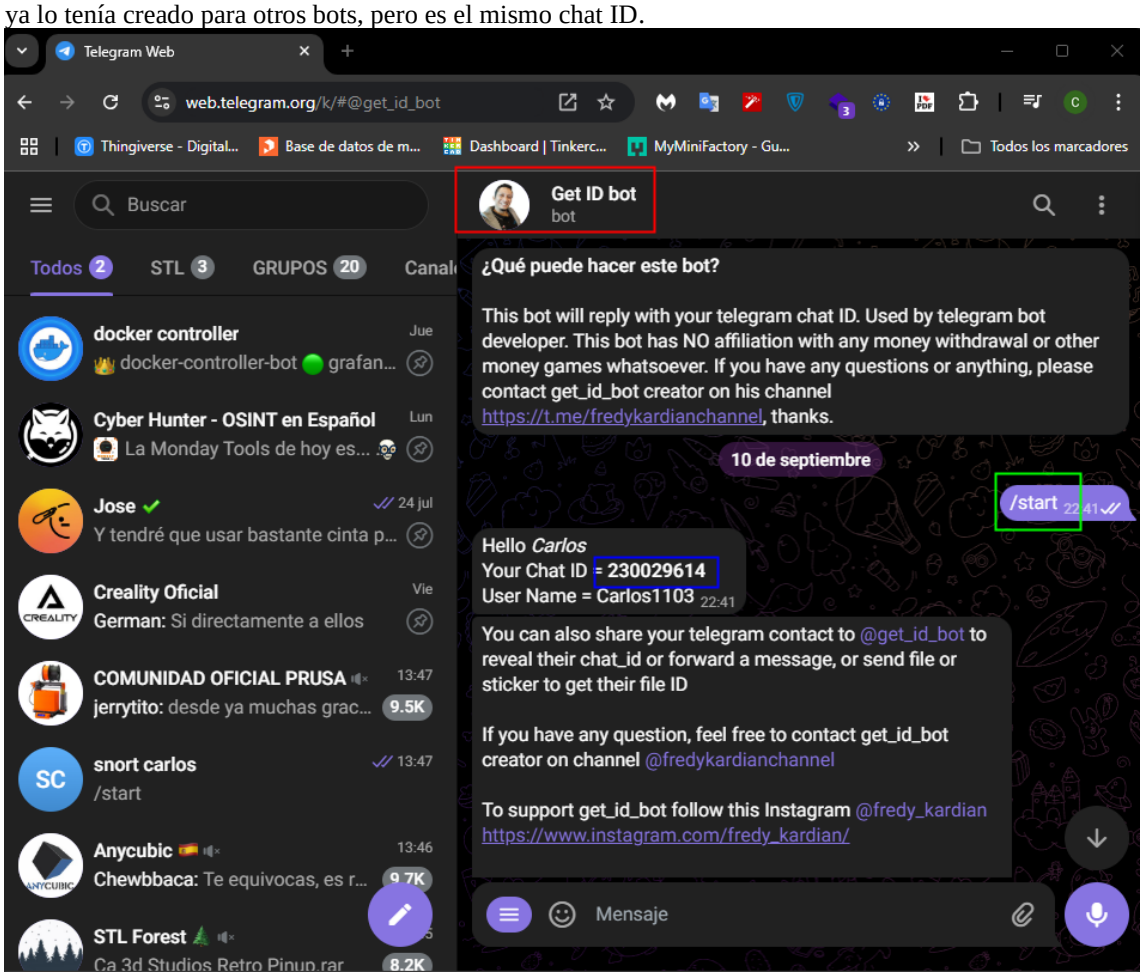
Ahora nos iremos a telegram y buscaremos @BotFather y crearemos un Bot nuevo.



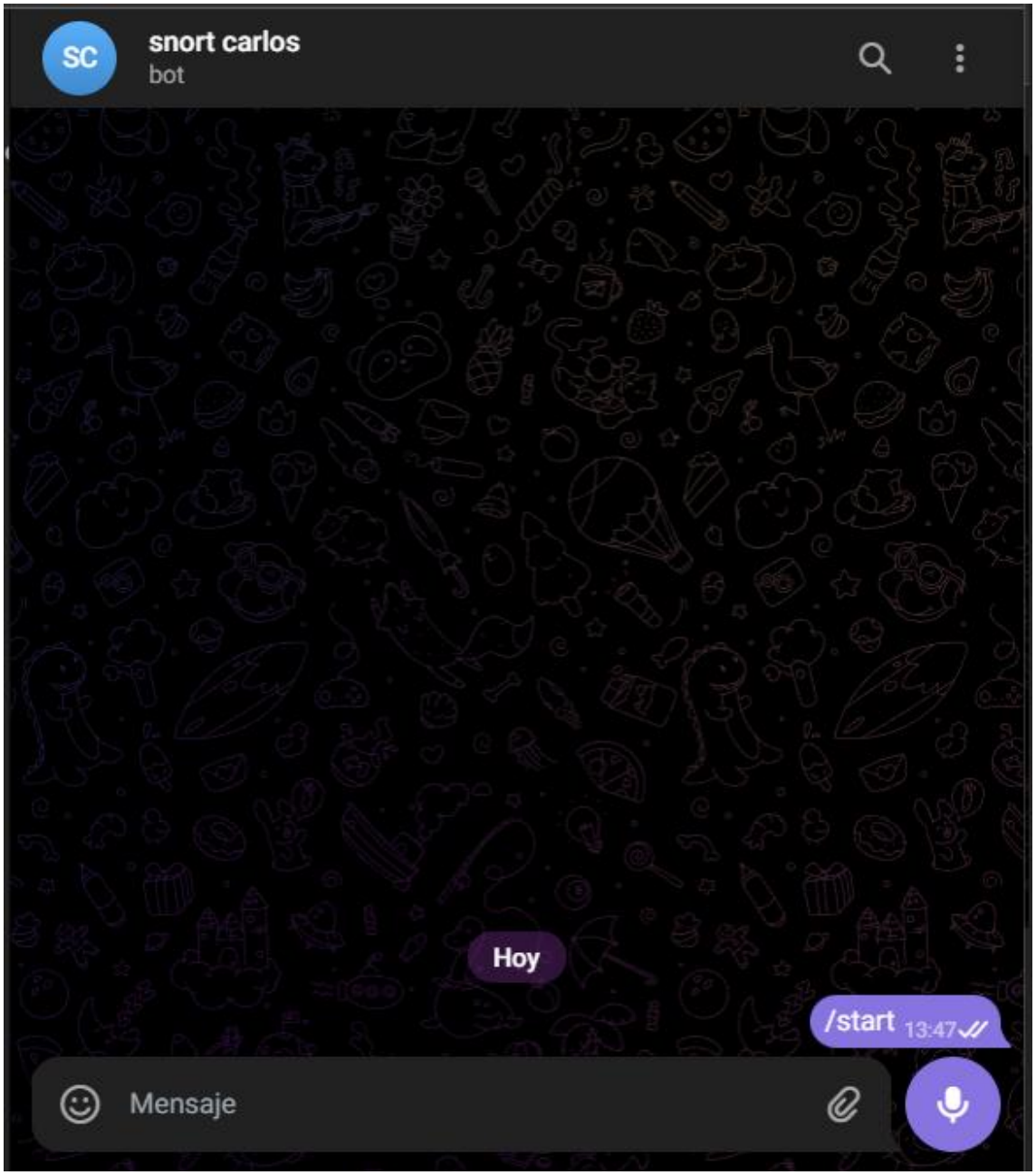
Ahora buscaremos el Bot en el buscador.



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

```
root@ubuntu: ~/Snort-Bot-Te
 GNU nano 7.2                                          bot-tele.sh *
#!/bin/bash

#init
initCount=0
logs=/home/ghost666/log-tele.txt

#File
msg_caption=/tmp/telegram_msg_caption.txt

#Chat ID dan bot token Telegram
chat_id="230029614"
token="7758231927:AAHMKaPxfyKXOAFFAbiZM7zKLJ7wyxJOnsE"

#kirim
function sendAlert
{
        curl -s -F chat_id=$chat_id -F text="$caption" https://api.telegram.org/bo
}

#Monitoring Server
```

Por último, hay que indicarle donde guardara lo logs.

```
 GNU nano 7.2                                          bot-tele.sh
#!/bin/bash

#init
initCount=0
logs=/root/log-tele.txt

#File
msg_caption=/tmp/telegram_msg_caption.txt

#Chat ID dan bot token Telegram
chat_id="230029614"
token="7758231927:AAHMKaPxfyKXOAFFAbiZM7zKLJ7wyxJOnsE"
```

```
root@ubuntu:~/Snort-Bot-Telegram-Shell# chmod 777 bot-tele.sh
root@ubuntu:~/Snort-Bot-Telegram-Shell# ls -la
total 416
drwxr-xr-x 4 root root   4096 dic 14 13:56 .
drwx------ 7 root root   4096 dic 14 13:35 ..
-rwxrwxrwx 1 root root      0 dic 14 13:57 bot-tele.sh
drwxr-xr-x 8 root root   4096 dic 14 13:35 .git
-rw-r--r-- 1 root root 101817 dic 14 13:35 log-snort-telegram.png
-rw-r--r-- 1 root root   1971 dic 14 13:35 README.md
-rw-r--r-- 1 root root   2010 dic 14 13:35 Readme.txt
drwxr-xr-x 2 root root   4096 dic 14 13:35 snort-rules
-rw-r--r-- 1 root root 297176 dic 14 13:35 snort-running.png
root@ubuntu:~/Snort-Bot-Telegram-Shell#
```

```
root@ubuntu:~/Snort-Bot-Telegram-Shell# snort -i enp0s3 -c /etc/snort/snort.conf -l /var/log/snort/ -d -A console > /roo
t/Snort-Bot-Telegram-Shell/bot-tele.sh
Running in IDS mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/snort.conf"
PortVar 'HTTP_PORTS' defined :  [ 80:81 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848
5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300
8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ]
PortVar 'SHELLCODE_PORTS' defined :  [ 0:79 81:65535 ]
PortVar 'ORACLE_PORTS' defined :  [ 1024:65535 ]
PortVar 'SSH_PORTS' defined :  [ 22 ]
PortVar 'FTP_PORTS' defined :  [ 21 2100 3535 ]
PortVar 'SIP_PORTS' defined :  [ 5060:5061 5600 ]
PortVar 'FILE_DATA_PORTS' defined :  [ 80:81 110 143 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 37
02 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 82
43 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ]
PortVar 'GTP_PORTS' defined :  [ 2123 2152 3386 ]
Detection:
   Search-Method = AC-Full-Q
    Split Any/Any group = enabled
    Search-Method-Optimizations = enabled
    Maximum pattern length = 20
```

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

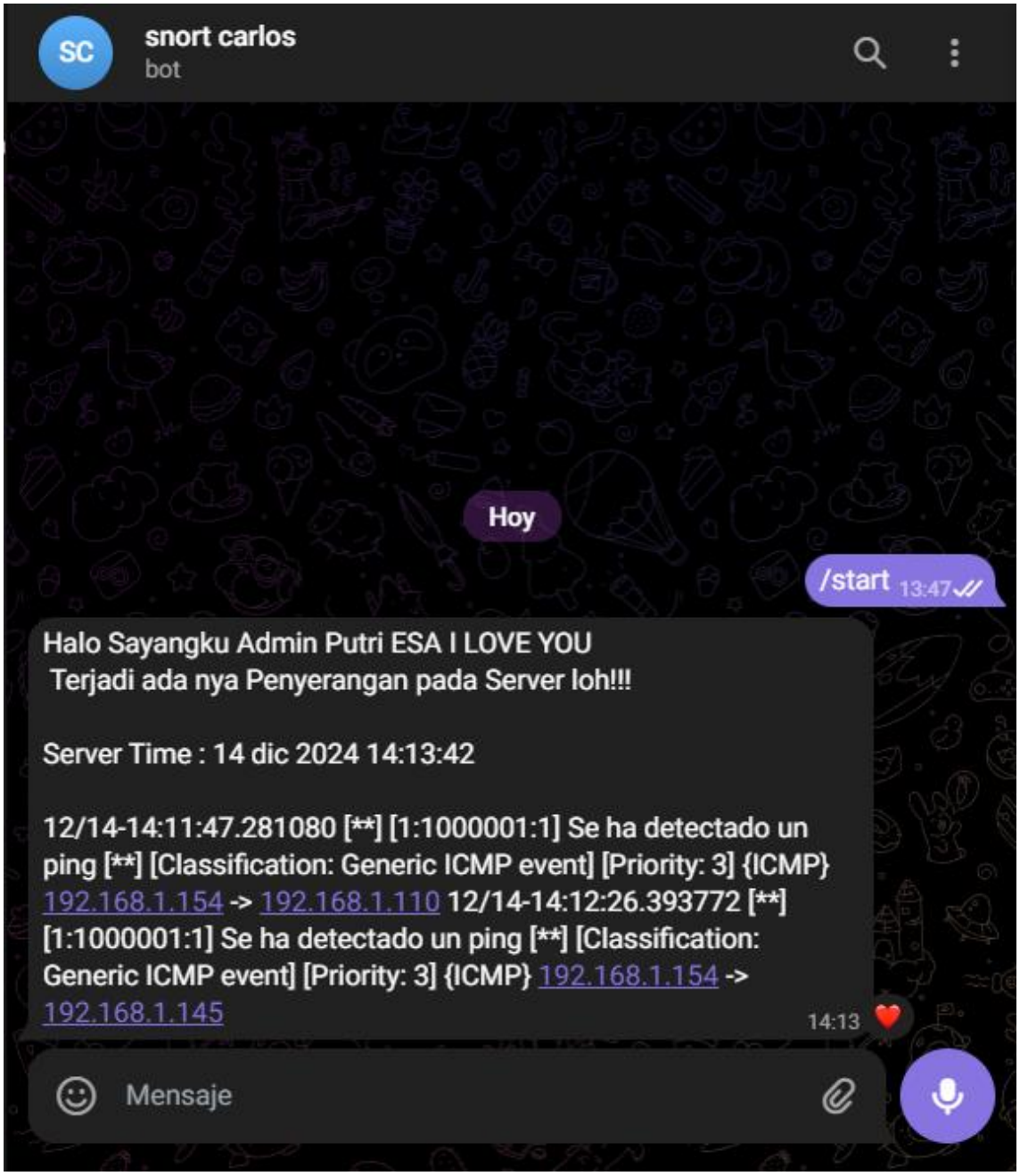
```
root@ubuntu:~/Snort-Bot-Telegram-Shell# ./bot-tele.sh
./bot-tele.sh: línea 17: curl: orden no encontrada
Alert Terkirim
^X^C
root@ubuntu:~/Snort-Bot-Telegram-Shell# apt install curl -y
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes NUEVOS:
  curl
0 actualizados, 1 nuevos se instalarán, 0 para eliminar y 126 no actualizados.
Se necesita descargar 227 kB de archivos.
Se utilizarán 534 kB de espacio de disco adicional después de esta operación.
Des:1 http://es.archive.ubuntu.com/ubuntu noble-updates/main amd64 curl amd64 8.5.0-2ubuntu10.5 [227 kB]
Descargados 227 kB en 0s (1.182 kB/s)
Seleccionando el paquete curl previamente no seleccionado.
(Leyendo la base de datos ... 153703 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar .../curl_8.5.0-2ubuntu10.5_amd64.deb ...
Desempaquetando curl (8.5.0-2ubuntu10.5) ...
Configurando curl (8.5.0-2ubuntu10.5) ...
Procesando disparadores para man-db (2.12.0-4build2) ...
```

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

```
PS C:\Users\carlo> ping 192.168.1.154

Haciendo ping a 192.168.1.154 con 32 bytes de datos:
Respuesta desde 192.168.1.154: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.1.154: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.1.154: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.1.154: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 192.168.1.154:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```



7. 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.