Dibujo de una persona

Descripción generada automáticamente con confianza baja

Práctica SNORT

Ethan Erwin Sánchez

Víctor Rodríguez Pérez

Índice

[Índice 2](#_Toc184892615)

[Preparación inicial 3](#_Toc184892616)

[Configuración de reglas 4](#_Toc184892617)

[comprobación de las reglas 5](#_Toc184892618)

[Conectar con telegram 6](#_Toc184892619)

[comprobación telegram 8](#_Toc184892620)

[Conclusión 8](#_Toc184892621)

## Preparación inicial

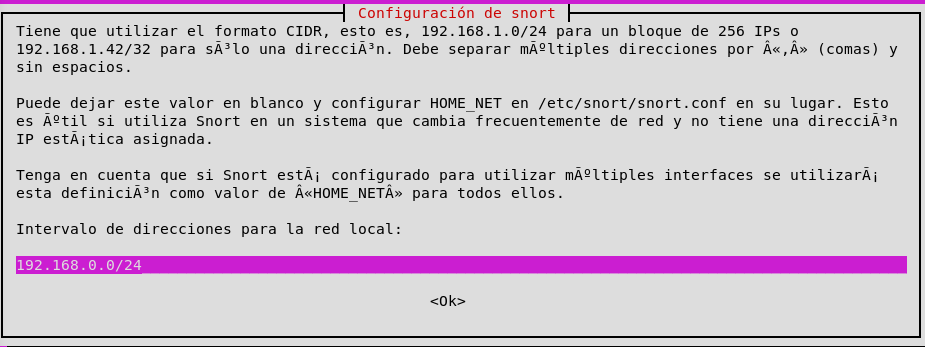
El primer paso es activar el servicio de iptables en el equipo, en nuestro caso no hizo falta ya que venían activadas por defecto.

El siguiente paso es instalar el servicio de snort usando

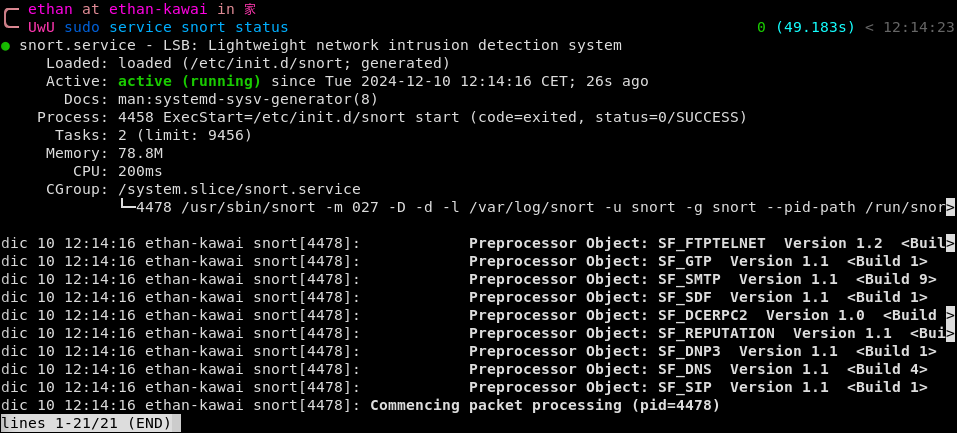
Sudo apt update | sudo apt install snort

Durante la instalación nos pedirá que red queremos proteger, en nuestro caso pusimos la

192.168.0.0/24



Aquí terminaría la configuración inicial de snort, si hacemos un comando para ver el estado veremos que esta activo

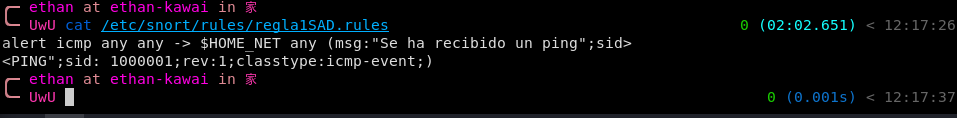


## Configuración de reglas

El propio snort nos facilita un fichero por defecto sin ninguna regla para poder agregar nuestras proprias reglas, pero nosotros por facilidad de organizar y saber que es cada regla crearemos nuestros proio ficheros en el directorio

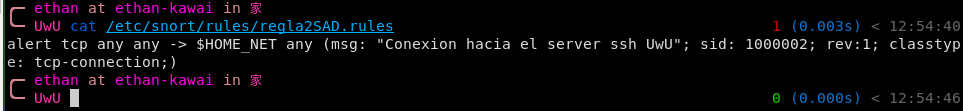
/etc/snort/rules/XXX.rules

La primera regla que crearemos será para detectar los ping que se hagan a nuestra red, crearemos nuestro archivo en /etc/snort/rules/regla1SAD.rules

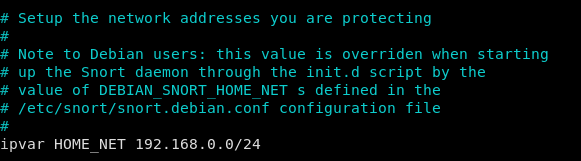


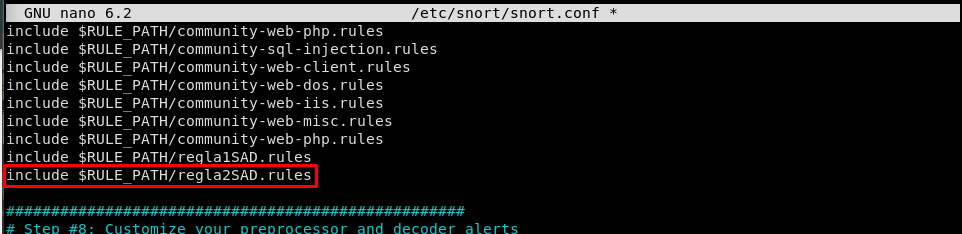
Nuestra segunda regla será para detectar ssh, por lo cual crearemos una regla nueva en

/etc/snort/rules/regla2SAD.rules



Después hay que añadir estas 2 reglas creadas al archivo de configuración y ya que te encuentras en el archivo de configuración hay que cambiar el HOME\_NET de any a la ip especificado en la configuración inicial, que se encuentra en /etc/snort/snort.conf



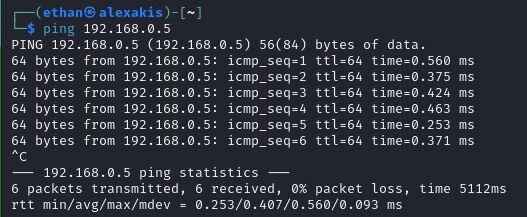


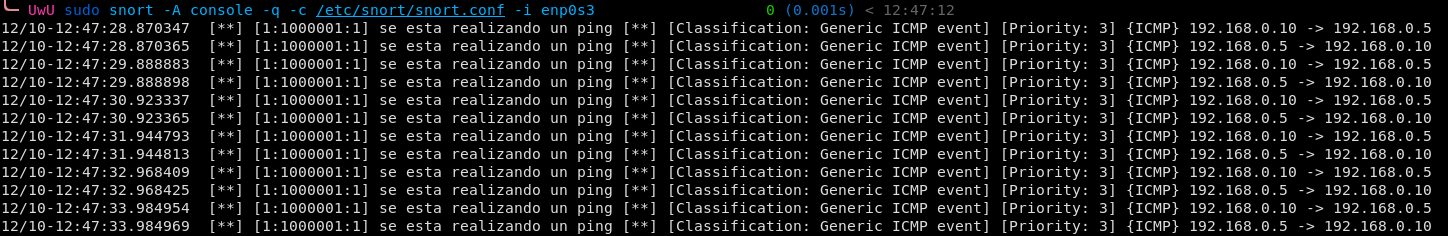
## comprobación de las reglas

Para poner a funcionar el snort hay que usar el siguiente comando:

Sudo snort -A console -q -c /etc/snort/snort.conf -i enp0s3

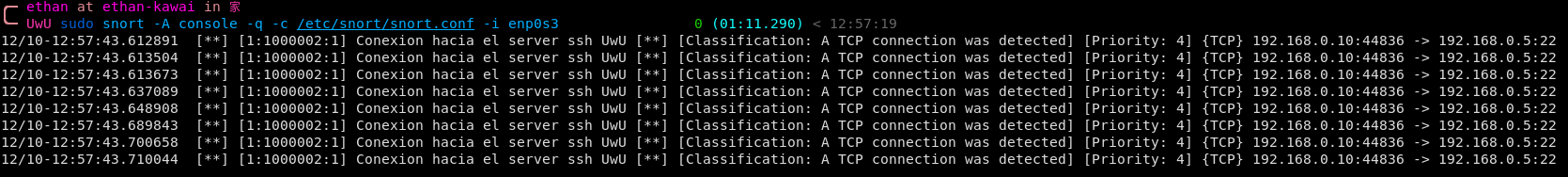
Una vez ejecutado esto si hacemos un ping o una conexión ssh nos saldrá una alerta





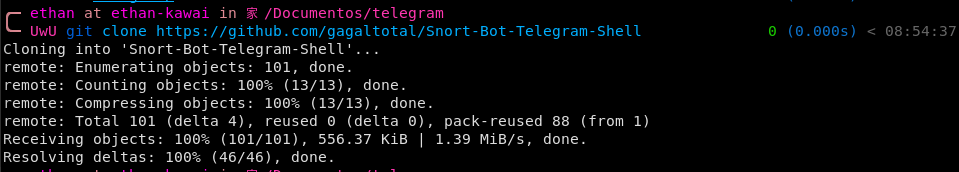
Ahora comprobaremos el ssh



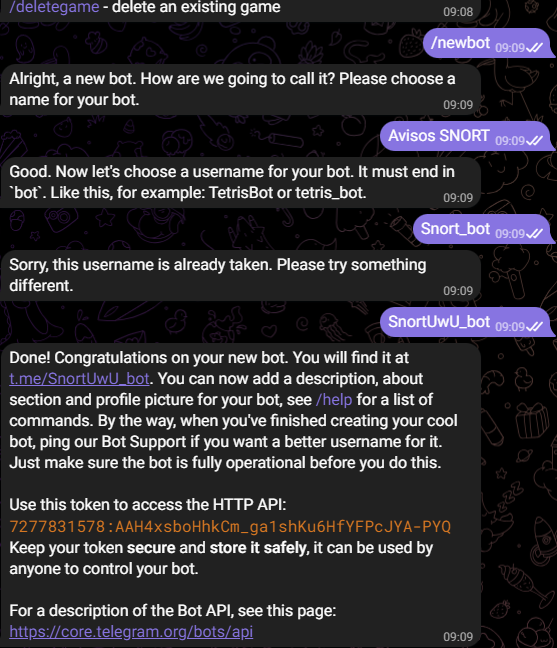


## Conectar con telegram

Ahora para que las alertas se puedan ver sin tener que estar delante de la pantalla configuraremos un bot de telegram para que nos envíen las alertas, para ellos clonaremos un repositorio de git que nos viene todo lo necesario



También tendremos que crear un bot nuevo con BotFather en telegram, asique en el buscador de telegram pondremos @botfather y hablaremos con la cuenta que esta verificada



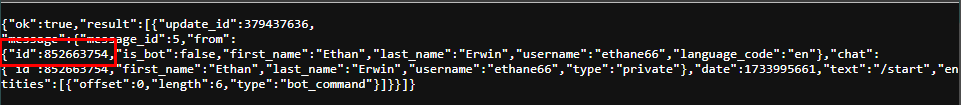
Una vez hayamos clonado el repositorio git y creado el nuevo bot hay que configurar el archivo que se encuentra dentro de donde hayamos clonado el repositorio de git llamado

Bot-tele.sh

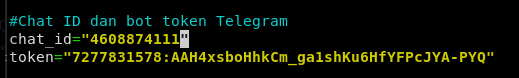
Dentro de ese archivo hay que poner el token y chat-id que sacaremos de telegram, pero para ello hay que hacer una configuración previa.

Para saber el token nos lo dice botfather al crear el bot y con ese token podremos sacar el chat\_id, para ello iremos al buscador del navegador y pondremos

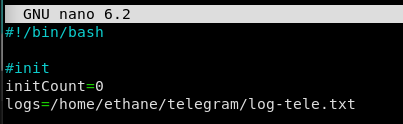
Api.telegram.org/”token de nuestro bot” y si nunca hemos interactuado con nuestro bot nos saldrá en blanco, asique iremos al chat del bot con el enlace que nos da botfather y pondremos /start, después refrescamos la pagina y nos saldrá mas información relacionado con el bot y también el chat\_id



Con esto y el token del bot podremos configurar el archivo bot-tele.sh



Por ultimo hay que crear e indicar donde pondremos los logs de telegram, por comodidad he creado el archivo logs en el mismo directorio donde esta el bot-tele.sh y indicaremos el archivo en de configuración la ruta de los logs

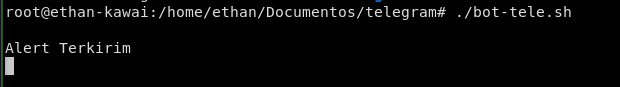


## comprobación telegram

Para poder comprobar que funciona el bot de telegram iniciaremos snort con unos parámetros distintos

Sudo snort -i enp0s3 -c /etc/snort/snort.conf -l /var/logs/snort/ -d -A console > /home/Ethan/documentos/telegram/log-tele.sh

En otra terminal cambiaremos los permisos del archivo bot-tele.sh para que pueda tener permisos de ejecución y después lo ejecutaremos con sudo, una vez tengamos el snort y el archivo sh ejecutados haremos un ssh a la maquina y nos saldrá esta alerta



(Debido a que la red de clase bloquea telegram no puedo adjuntar una imagen del mensaje recibido en telegram, pero esta captura indica que se envió el mensaje)

## Conclusión

En esta practica hemos visto que un programa simple como snort nos puede ayudar a detectar intentos de ataques a nuestra red, ya que viene con un montón de opciones preconfigurados mas las reglas especificas que queremos tener y que se puede hacer de manera que se pueda monitorear de manera desatendida con telegram