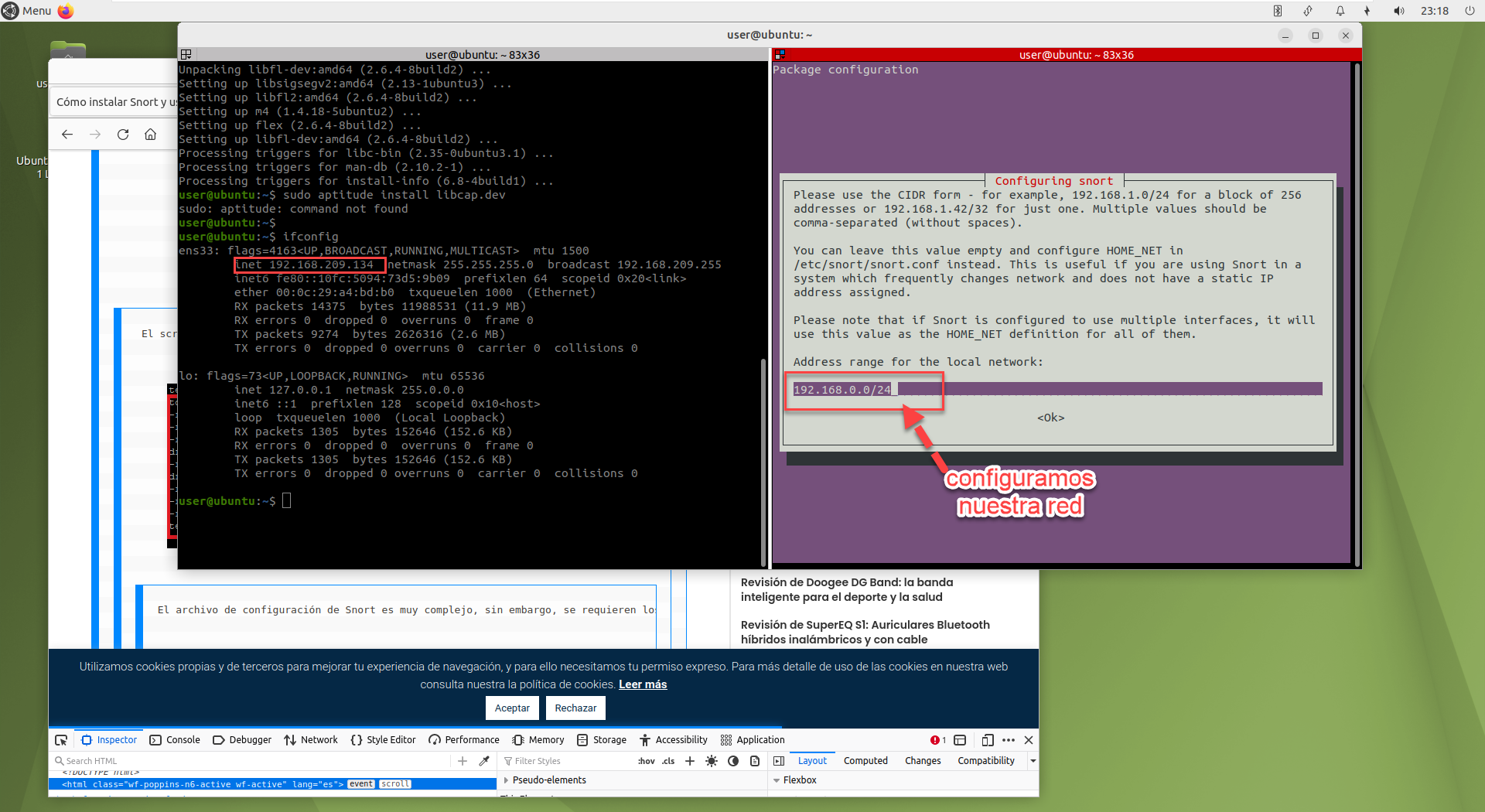
**Configuración manual de Snort**

1. **Instalación de la herramienta IPS/IDS (Snort)**



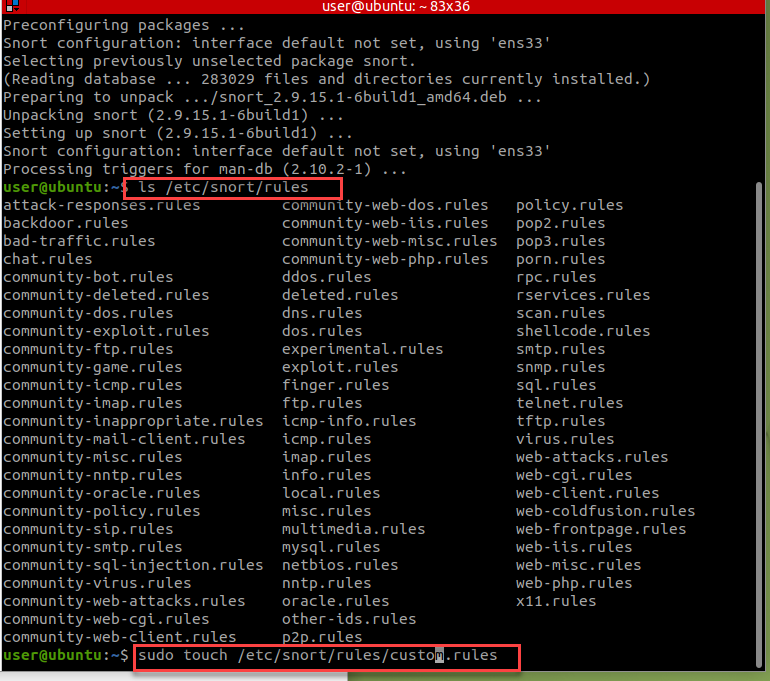
1. **Creamos un file para nuestras reglas personalizadas**

Con el siguiente comando procedemos a crear el file personalizado

# sudo touch /etc/snort/rules/custom.rules

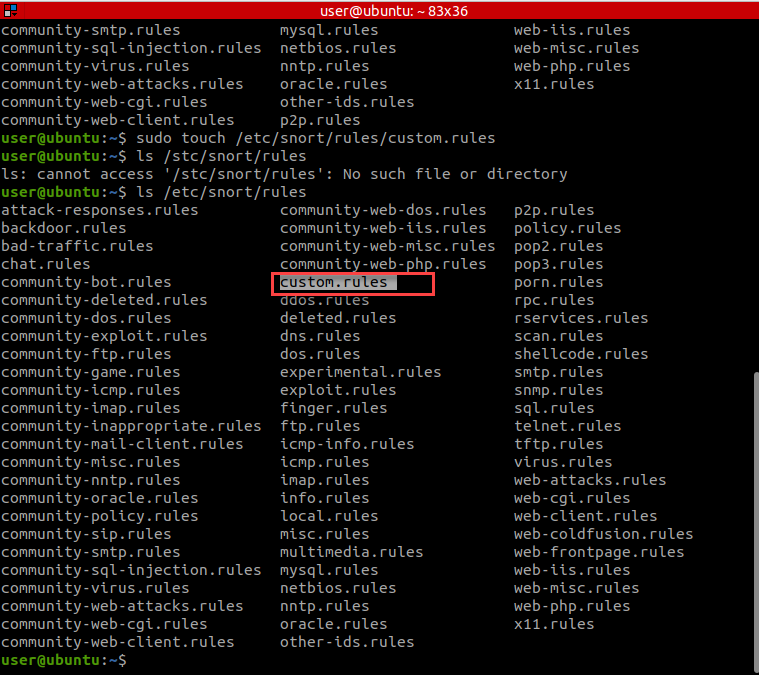
Verificamos o listamos

# ls /etc/snort/rules



1. **Verificamos que se creó la carpeta, donde podremos crear nuestras reglas**

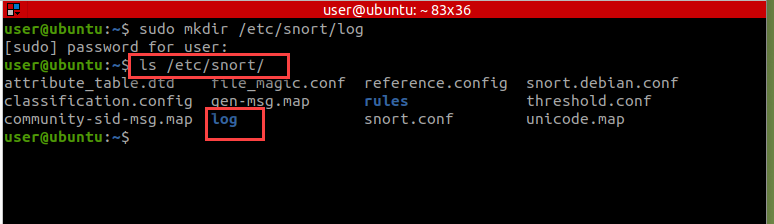
* Pero vemos que tenemos varias reglas por defecto
* Todos esos archivos son reglas ya establecidas internamente por Snort
* Dentro del archivo Custom.rules, crearemos nuestras propias reglas



1. **Creamos el directorio donde guardaremos nuestros logs, todo lo que encuentre Snort**

Se procede a crear la carpeta donde vamos a guardar los logs que la herramienta nos almacenará.

# sudo mkdir /etc/snort/log



1. **Definición de red Segura**

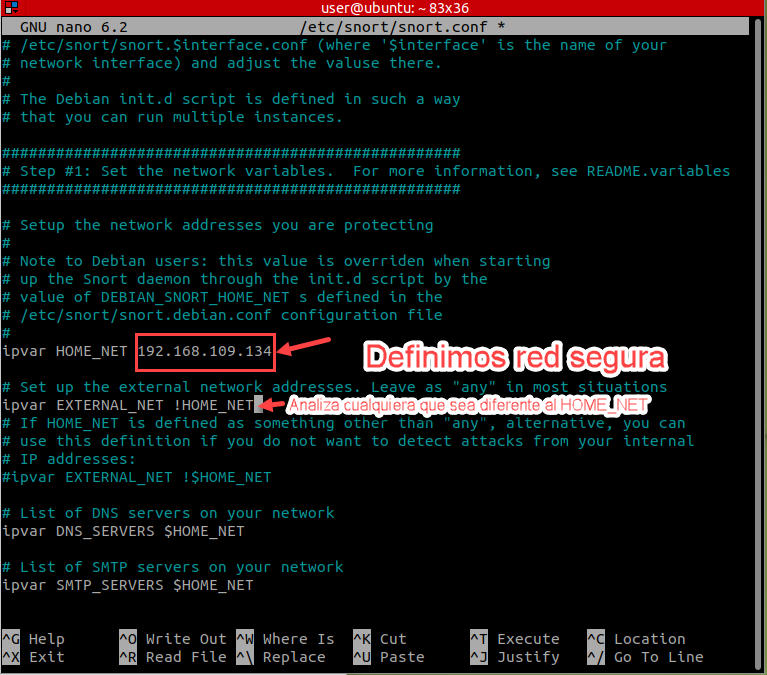
Se procede a crear las 2 reglas, El Home\_NET (Red segura), se puede colocar la red de la empresa. Lo que hace este paso se decirle a Snort, que la IP de HOME\_NET es segura y que no lo analice.

# sudo nano /etc/snort/snort.config

* Configuramos la interna: ipvar HOME\_NET [IP]
* Configuramos la externa: ipvar EXTERNAL\_NET [!HOME\_NET ] (*con esto le digo que analice cualquiera que sea diferente a la HOME\_NET)*

*NOTA:*

* A veces no hace caso a !HOME\_NET sino hay que colocar la IP: !192.168.109.134



1. **Prueba para ver si funciona bien SNORT**

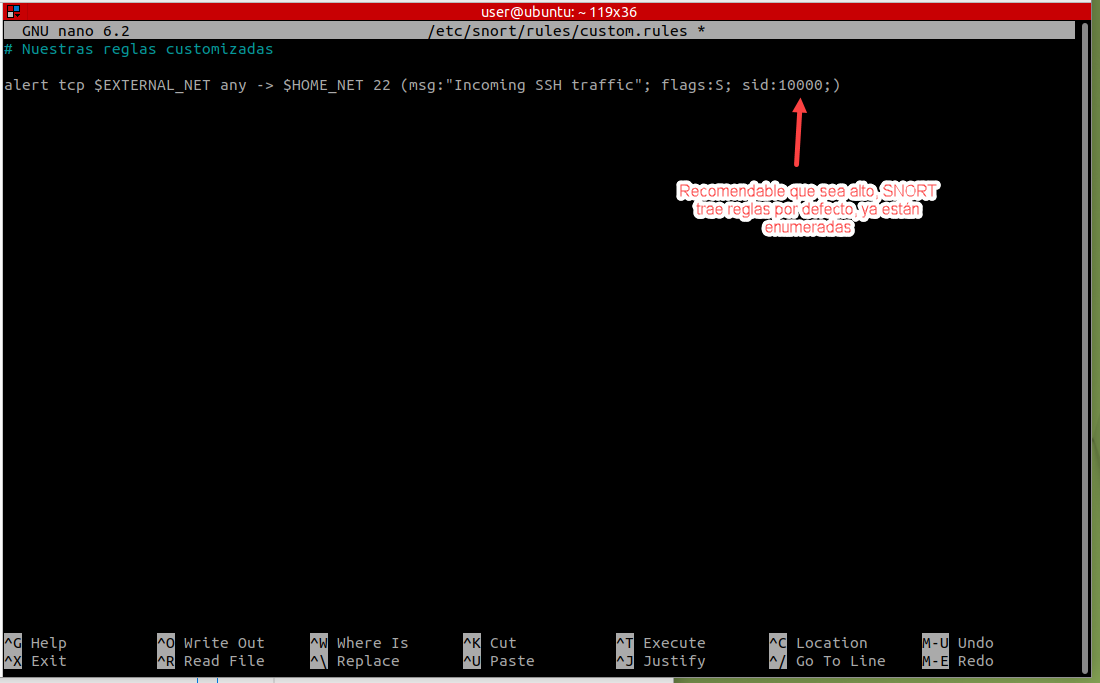
Creamos nuestra primera regla de prueba en el **custom.rules** que creamos anteriormente

*# sudo nano /etc/snort/rules/custom.rules*

*Ejemplo:*

Para el caso, estamos diciendo que nos alerte tráfico TCP que venga de la red externa, desde cualquier puerto {any} -> y que se dirija a la HOME\_NET, desde el puerto 22, ahí nos alerta el mensaje que está ahí, vemos el paquete Syn {la flag, para esto acordarse del SYN-ACK}, el sid puede ser cualquiera, para el caso 10000

**Alert tcp $EXTERNAL\_NET any -> $HOME\_NET 22 (msg:”Incoming SSH traffic”; flags:S; sid:10000;)**



Ahora que creamos nuestra regla, lo que debemos de hacer, es decirle a SNORT que vamos a usar esa regla

*# sudo nano /etc/snort/snort.conf*



1. **Iniciamo Snort**

Ejecutamos en el prompt la siguiente linea de comando, para que podamos ejecutar la herramienta.

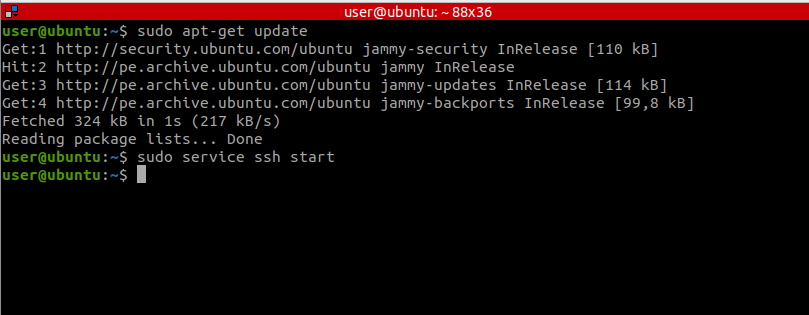
*#sudo snort -d -l /etc/snort/log -b -c /etc/snort/snort.conf*

1. **Inicio de prueba de regla con SSH**

Para el ejemplo, levantamos nuestro servicio SSH -> si no funciona, instale SSH con

*#sudo apt-get install ssh*

*# sudo service ssh start*



Ahora desde la máquina usuario me conecto mediante SSH la máquina de SNORT

# ssh [user@192.168.209.134](mailto:user@192.168.209.134)

Imagen de la pantalla de un computador

Descripción generada automáticamente con confianza media

Ahora que nos hemos conectado, deberíamos de tener una alerta en snort.

Lo verificamos en la siguiente ruta

# cat /etc/snort/log/snort.alert.fast

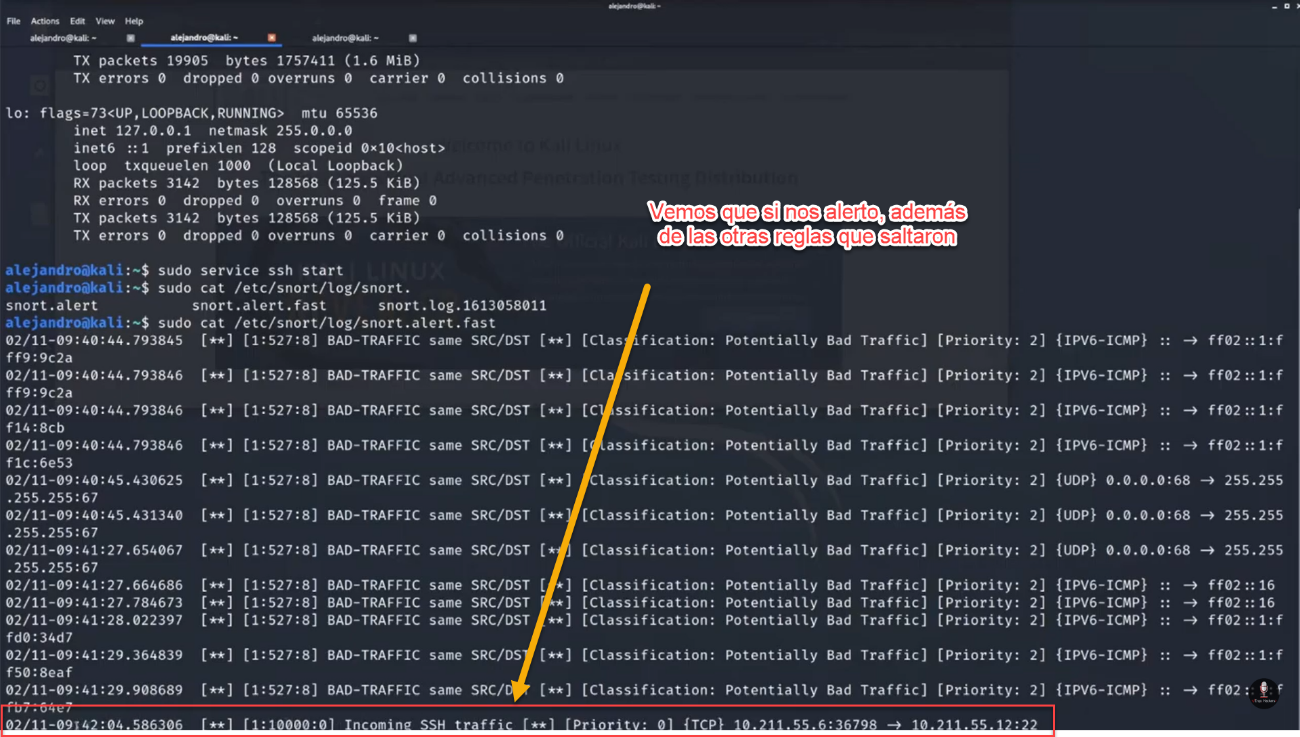
Texto

Descripción generada automáticamente con confianza media

Texto

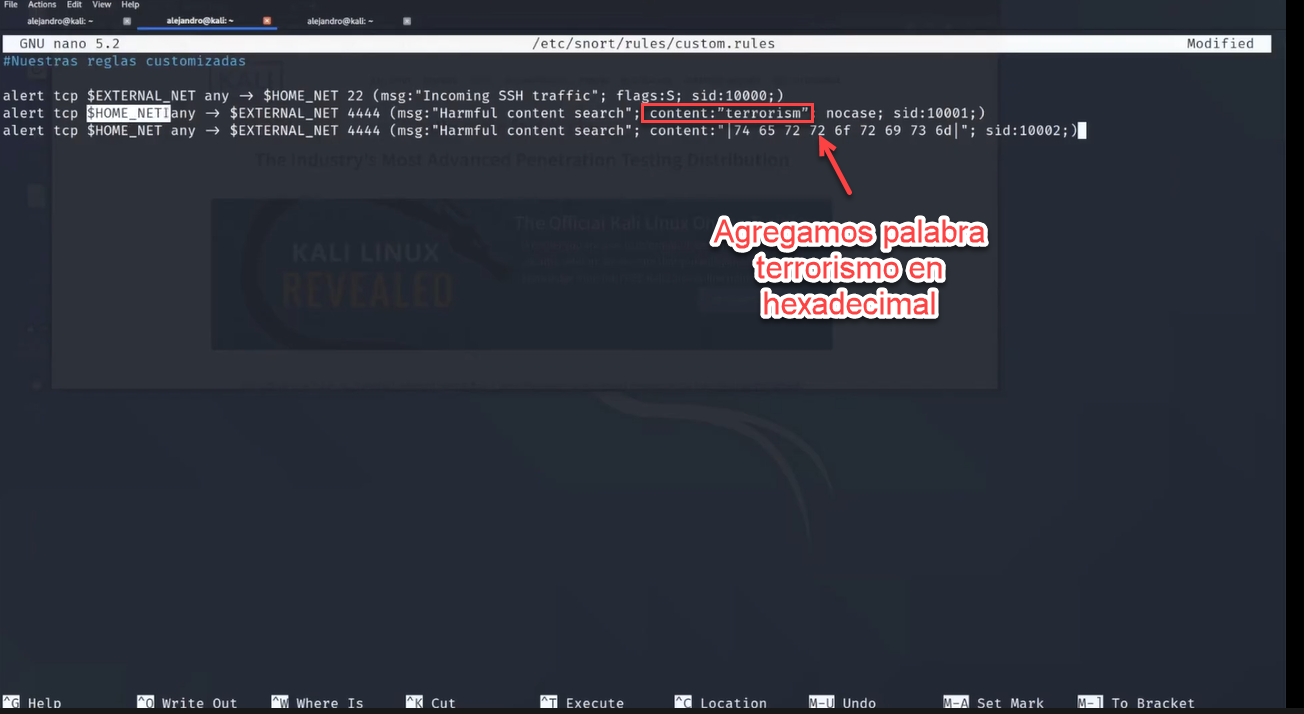
Descripción generada automáticamente

Para el caso no me alerta, por la configuración que se puso. 192.168.x.x.  
Las 2 IP al pertenecer la misma red, no salta.   
Pero si saltara, se vería así.



1. **Agregamos otra regla de prueba**

Se puede crear más reglas, entrando internamente para leer las palabras del paquete

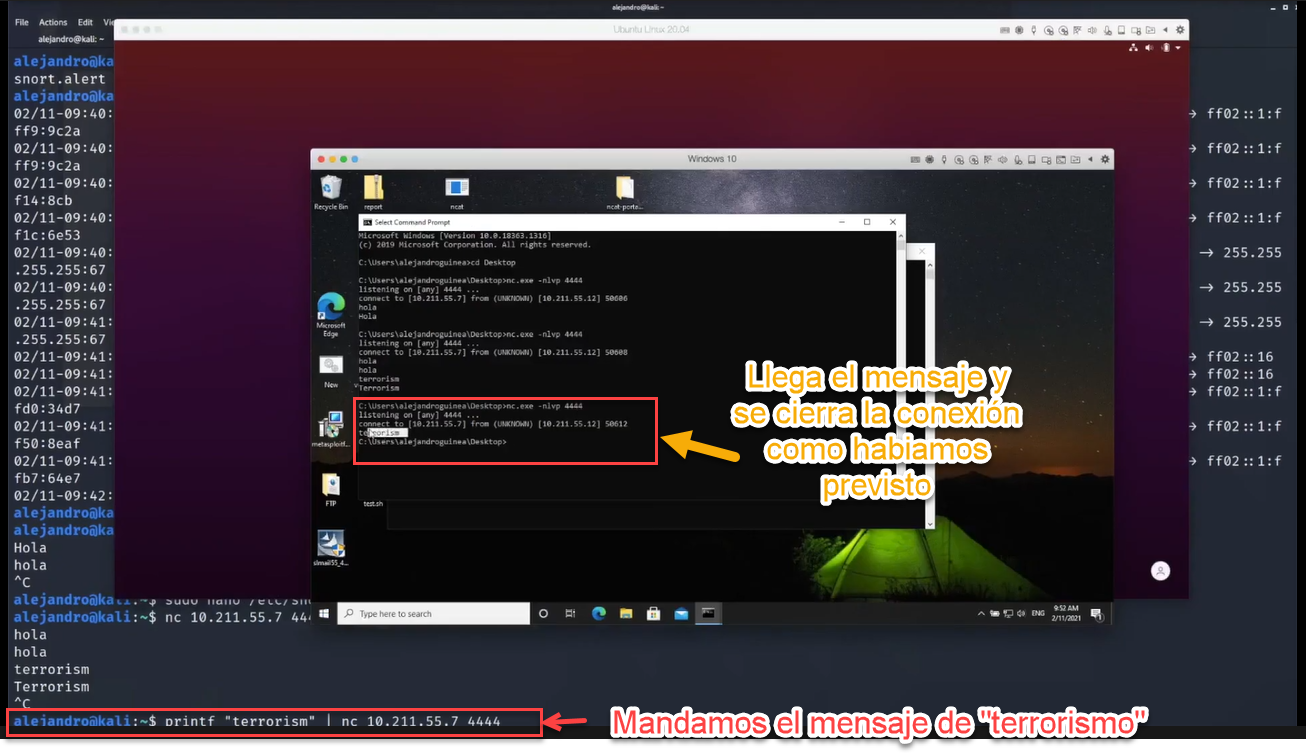


Esto lo podemos simular con el netcat.

Para estos casos que son escuchas activas, se le agrega la bandera “-k” al comando que corre snort

# sudo snort -d -l /etc/snort/log -b -c /etc/snort/snort.conf

Lo que pasa es que cuando se coloca la escucha o se escribe palabras, snort adjunta el salto de espacio y da fallos, no reconoce bien, para evitar eso, se coloca el “-k”



Verificamos en los logs de snort

# sudo cat /etc/snort/log/snort.alert.fast

Texto

Descripción generada automáticamente