



Universidad
Francisco de Paula Santander

NIT. 890500622 - 6

www.ufps.edu.co

INSTALACION Y CONFIGURACION DE UN NIDS (SNORT) EN UBUNTU

VIVIANA ISABEL ESPINOSA PEÑA 1150017
ANA KATERINE MONTESINOS GELVEZ 1150013

PROFESOR: JEAN POLO CEQUEDA

MATERIA: SEGURIDAD INFORMATICA

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER
INGENIERIA DE SISTEMAS
SAN JOSE DE CUCUTA
I SEMESTRE 2013

Av. Gran Colombia No. 12E-96 Colsag
Teléfono: 5776655
Cúcuta - Colombia

SISTEMAS DE DETENCION DE INTRUSOS Y SNORT

1. Introducción teórica

Un IDS es una herramienta de seguridad que intenta detectar o monitorizar los eventos ocurridos en un determinado sistema informático en busca de intentos de comprometer la seguridad de dicho sistema.

SISTEMAS IDS

Un **IDS** o **Sistema de Detección de Intrusiones** es una herramienta de seguridad que intenta **detectar o monitorizar los eventos** ocurridos en un determinado sistema informático o red informática en busca de intentos de comprometer la seguridad de dicho sistema.

- Los **IDS** buscan **patrones previamente definidos** que impliquen cualquier tipo de actividad sospechosa o maliciosa sobre nuestra red o host.
- Los **IDS** aportan a nuestra seguridad una capacidad de **prevención** y de **alerta anticipada** ante cualquier actividad sospechosa. **No** están diseñados para **detener un ataque**, aunque sí pueden generar ciertos tipos de respuesta ante éstos.
- Los **IDS**: aumentan la seguridad de nuestro sistema, vigilan el tráfico de nuestra red, examinan los paquetes analizándolos en busca de datos sospechosos y detectan las primeras fases de cualquier ataque como pueden ser el análisis de nuestra red, barrido de puertos, etc.

TIPOS DE IDS

HIDS (Host IDS)

Protege contra un único Servidor, PC o host. Monitorizan gran cantidad de eventos, analizando actividades con una gran precisión, determinando de esta manera qué procesos y usuarios se involucran en una determinada acción. Recaban información del sistema como ficheros, logs, recursos, etc, para su posterior análisis en busca de posibles incidencias. Todo ello en modo local, dentro del propio sistema. Fueron los primeros IDS en desarrollar por la industria de la seguridad informática.

NIDS (Net IDS)

Protege un sistema basado en red. Actúan sobre una red capturando y analizando paquetes de red, es decir, son sniffers del tráfico de red. Luego analizan los paquetes capturados, buscando patrones que supongan algún tipo de ataque.

Bien ubicados, pueden analizar grandes redes y su impacto en el tráfico suele ser pequeño. Actúan mediante la utilización de un dispositivo de red configurado en modo promiscuo (analizan, "ven" todos los paquetes que circulan por un segmento de red aunque estos nos vayan dirigidos a un determinado equipo). Analizan el tráfico de red, normalmente, en tiempo real. No sólo trabajan a nivel TCP/IP, también lo pueden hacer a nivel de aplicación.

Otros tipos son los híbridos.

Por el tipo de respuesta podemos clasificarlos en:

Pasivos: Son aquellos IDS que notifican a la autoridad competente o administrador de la red mediante el sistema que sea, alerta, etc. Pero no actúa sobre el ataque o atacante.

Activos: Generan algún tipo de respuesta sobre el sistema atacante o fuente de ataque como cerrar la conexión o enviar algún tipo de respuesta predefinida en nuestra configuración.

Snort puede funcionar de las dos maneras.

Arquitectura de un IDS

Normalmente la arquitectura de un IDS, a grandes rasgos, está formada:

1. La fuente de recogida de datos. Estas fuentes pueden ser un log, dispositivo de red, o como en el caso de los IDS basados en host, el propio sistema.
 2. Reglas que contienen los datos y patrones para detectar anomalías de seguridad en el sistema.
 3. Filtros que comparan los datos snifados de la red o de logs con los patrones almacenados en las reglas.
 4. Detectores de eventos anormales en el tráfico de red.
 5. Dispositivo generador de informes y alarmas. En algunos casos con la sofisticación suficiente como para enviar alertas vía mail, o SMS.
- Esto es a modo general. Cada IDS implementa la arquitectura de manera diferente.

¿Dónde colocar un IDS?

Una actitud paranoica por nuestra parte nos podría llevar a instalar un IDS en cada host ó en cada tramo de red. Esto último sería un tanto lógico cuando se trata de grandes redes, no es nuestro caso ahora. Lo lógico sería instalar el IDS en un dispositivo por donde pase todo el tráfico de red que nos interese.

Posición del IDS:

Si colocamos el IDS antes del cortafuegos capturaremos todo el tráfico de entrada y salida de nuestra red. La posibilidad de falsas alarmas es grande.

La colocación detrás del cortafuegos monitorizará todo el tráfico que no sea detectado y parado por el firewall o cortafuegos, por lo que será considerado como malicioso en un alto porcentaje de los casos. La posibilidad de falsas alarmas muy inferior.

Algunos administradores de sistemas colocan dos IDS, uno delante y otro detrás del cortafuegos para obtener información exacta de los tipos de ataques que recibe nuestra red ya que si el cortafuegos está bien configurado puede parar o filtrar muchos ataques.

En ambientes domésticos, que es el propósito de este taller sobre IDS y Snort, podemos colocar el IDS en la misma máquina que el cortafuegos. En este caso actúan en paralelo, es decir, el firewall detecta los paquetes y el IDS los analizaría.

¿Qué es SNORT?

Snort es un IDS o Sistema de detección de intrusiones basado en red (NIDS). Implementa un motor de detección de ataques y barrido de puertos que permite registrar, alertar y responder ante cualquier anomalía previamente definida como patrones que corresponden a ataques, barridos, intentos aprovechar alguna vulnerabilidad, análisis de protocolos, etc. conocidos. Todo esto en tiempo real.

Snort está disponible bajo licencia GPL, gratuito y funciona bajo plataformas Windows y UNIX/Linux. Es uno de los más usados y dispone de una gran cantidad de filtros o patrones ya predefinidos, así como actualizaciones constantes ante casos de ataques, barridos o vulnerabilidades que vayan siendo detectadas a través de los distintos boletines de seguridad.

Este IDS implementa un lenguaje de creación de reglas flexibles, potente y sencillo. Durante su instalación ya nos provee de cientos de filtros o reglas para backdoor, ddos, finger, ftp, ataques web, CGI, escaneos Nmap....

Puede funcionar como sniffer (podemos ver en consola y en tiempo real qué ocurre en nuestra red, todo nuestro tráfico), registro de paquetes (permite guardar en un archivo los logs para su posterior análisis, un análisis offline) o como un IDS normal (en este caso NIDS).

La colocación de Snort en nuestra red puede realizarse según el tráfico quieren vigilar: paquetes que entran, paquetes salientes, dentro del firewall, fuera del firewall... y en realidad prácticamente donde queramos.

SNORT puede funcionar en:

- Modo sniffer, en el que se motoriza por pantalla en tiempo real la actividad en la red en que se ha configurado el Snort.
- Modo Packet logger (registro de paquetes), en el que se almacena en un sistema de log toda actividad de la red en que se ha configurado Snort para un posterior análisis.
- Modo IDS, en el que motoriza por pantalla o en un sistema basado en log, toda la actividad de la red a través de un fichero de configuración en el que se especifican las reglas y patrones a filtrar para estudiar los posibles ataques.

Funcionamiento del motor de Snort

El motor de Snort se divide en los siguientes componentes:

- Decodificador del paquete
- Preprocesadores.
- Motor de detección (Comparación contra firmas).
- Loggin y sistema de alerta
- Plugins de salida.
- El decodificado de paquete, toma los paquetes de diferentes tipos de interfaces de red y prepara el paquete para ser preprocesado o enviado al motor de detección.

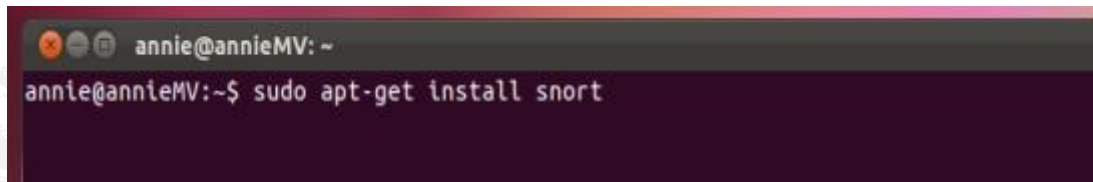
INSTALACION Y CONFIGURACION DE SNORT

1. Instalación

La instalación se hará en la distribución de Linux (Ubuntu 12.04). Para instalarlo se debe abrir el terminal,

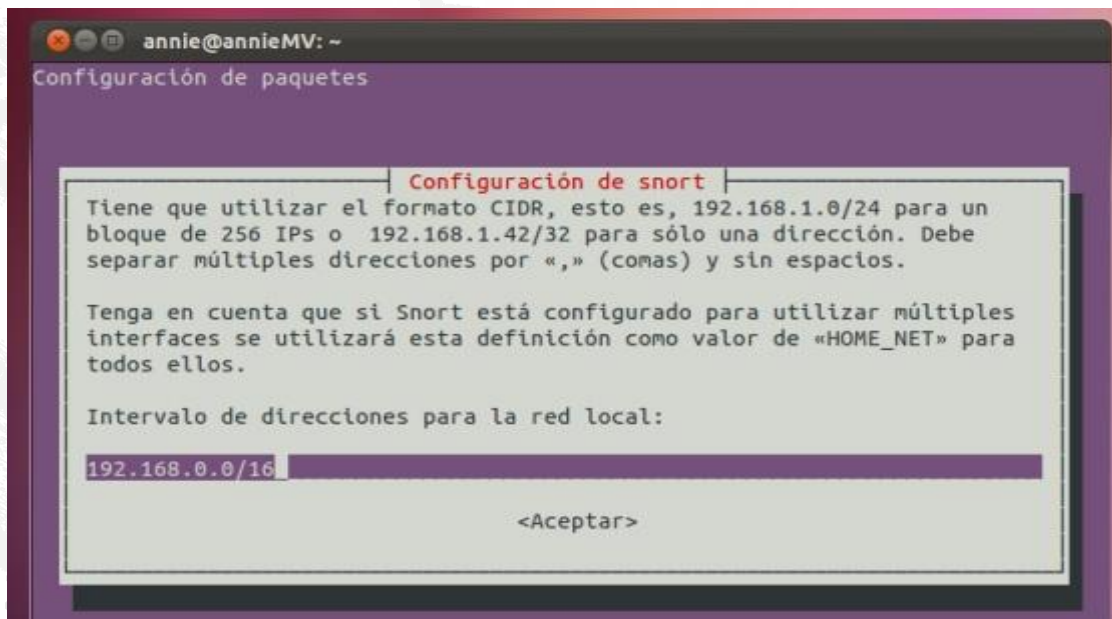
Y se digita el comando:

sudo apt-get install snort



```
annie@annieMV: ~
annie@annieMV:~$ sudo apt-get install snort
```

El terminal le pide la clave del superusuario en este caso annie, para dar permisos para la instalación, cuando empieza a descargar los paquetes, muestra una ventana que pida una configuración antes de seguir con la descarga.



```
annie@annieMV: ~
Configuración de paquetes

Configuración de snort
Tiene que utilizar el formato CIDR, esto es, 192.168.1.0/24 para un
bloque de 256 IPs o 192.168.1.42/32 para sólo una dirección. Debe
separar múltiples direcciones por « , » (comas) y sin espacios.

Tenga en cuenta que si Snort está configurado para utilizar múltiples
interfaces se utilizará esta definición como valor de «HOME_NET» para
todos ellos.

Intervalo de direcciones para la red local:
192.168.0.0/16
<Aceptar>
```

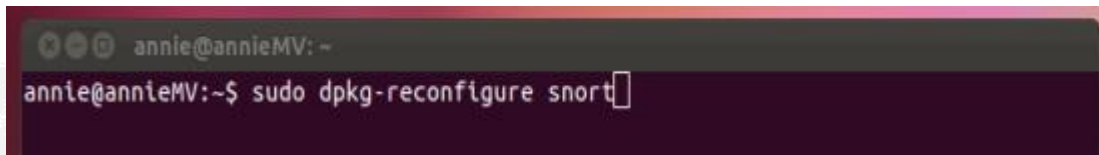
En el paso anterior pide la dirección de red local (la cual va a ser la que se estará monitoreando). En este punto puede haber 3 opciones de configuración:

- Si es una única dirección se colocara con máscara de sured /32
- Si es un bloque de 256 IPs se utilizará la máscara /24
- Si es una red más amplia se utilizará la máscara /16

2. Configuración

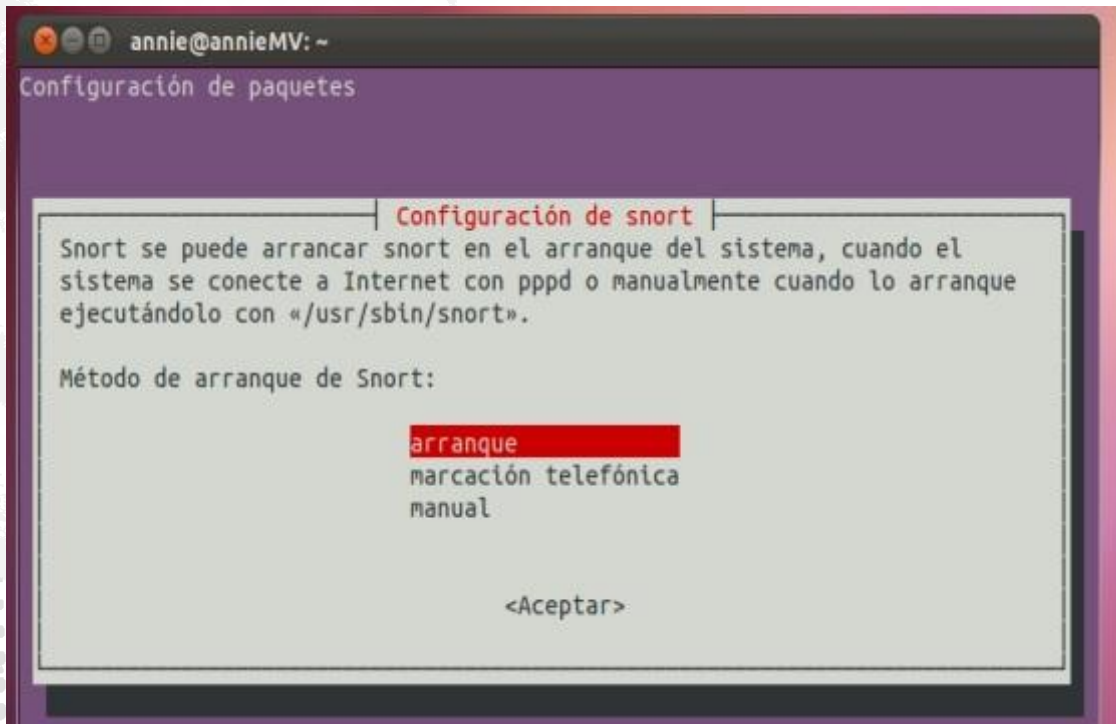
Cuando finaliza el proceso de instalación se procede a la configuración. Para esto tenemos que utilizar el siguiente comando:

`sudo dpkg-reconfigure snort`



```
annie@annieMV: ~
annie@annieMV:~$ sudo dpkg-reconfigure snort
```

Lo cual mostrara cual opción de arranque desea configurar. Y se escoge el modo manual y damos enter en aceptar.



```
annie@annieMV: ~
Configuración de paquetes

Configuración de snort

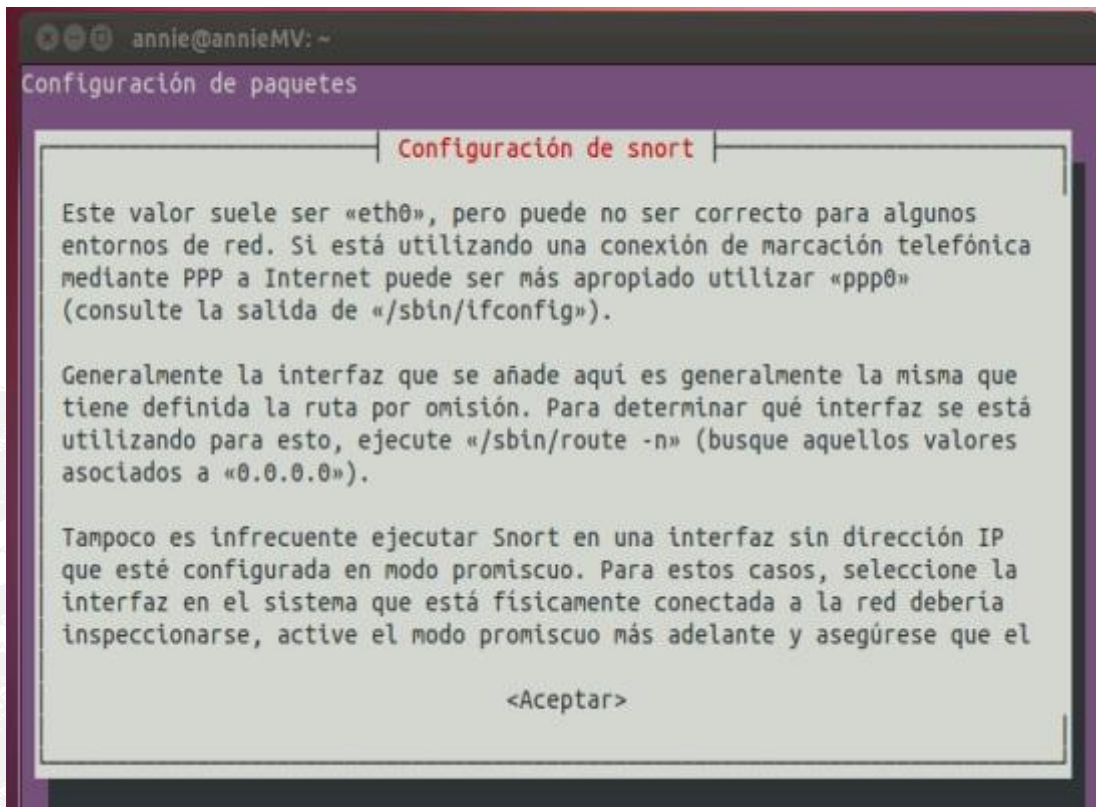
Snort se puede arrancar snort en el arranque del sistema, cuando el
sistema se conecte a Internet con pppd o manualmente cuando lo arranque
ejecutándolo con «/usr/sbin/snort».

Método de arranque de Snort:

  arranque
  marcación telefónica
  manual

<Aceptar>
```

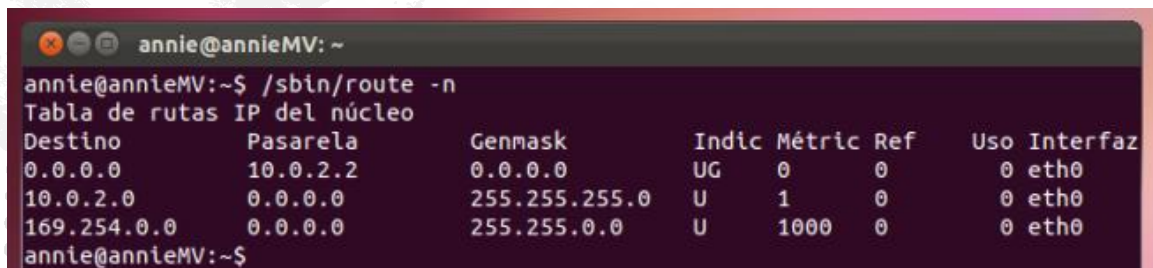

Luego sale una ventana de explicación de lo que será el próximo requisito a pedir, la interface de red q se escaneará.



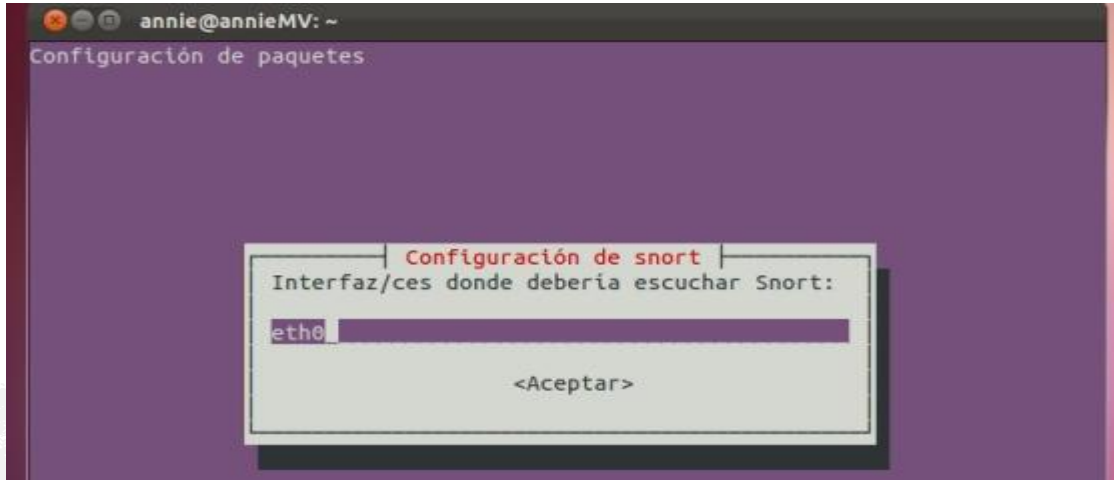
Aquí se explica que utiliza el siguiente comando para encontrar la interface (esto se hace en otro terminal para no interrumpir el proceso de configuración).

`/sbin/route -n`

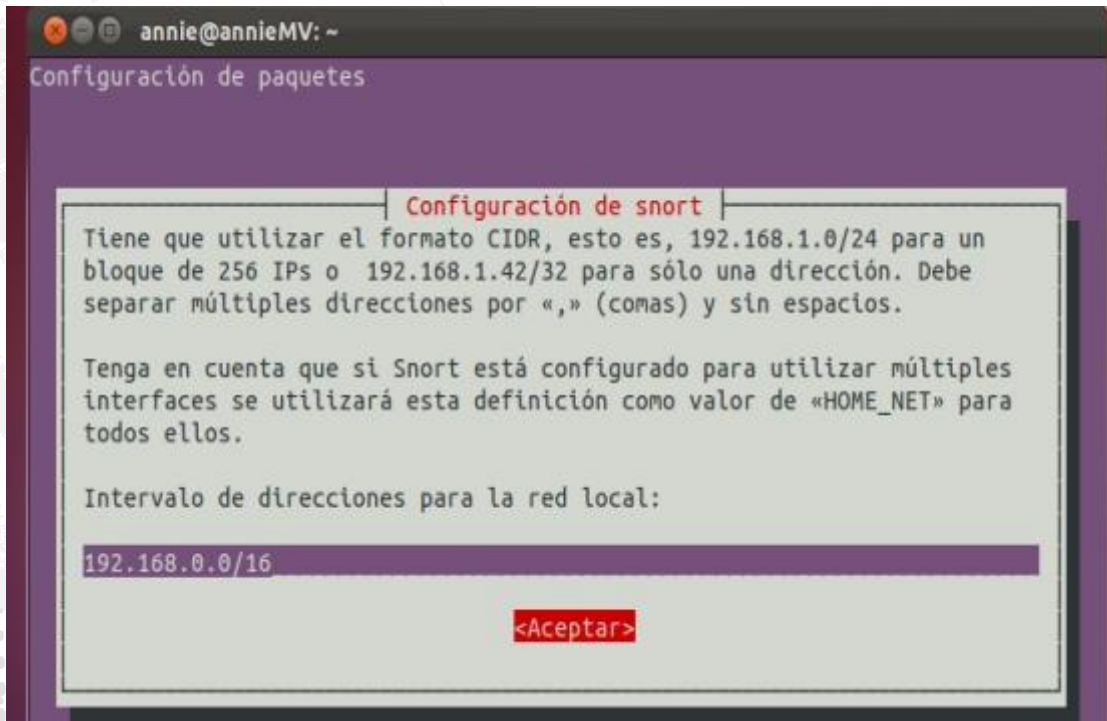
Lo cual denota que la interfaz necesaria es la eth0.



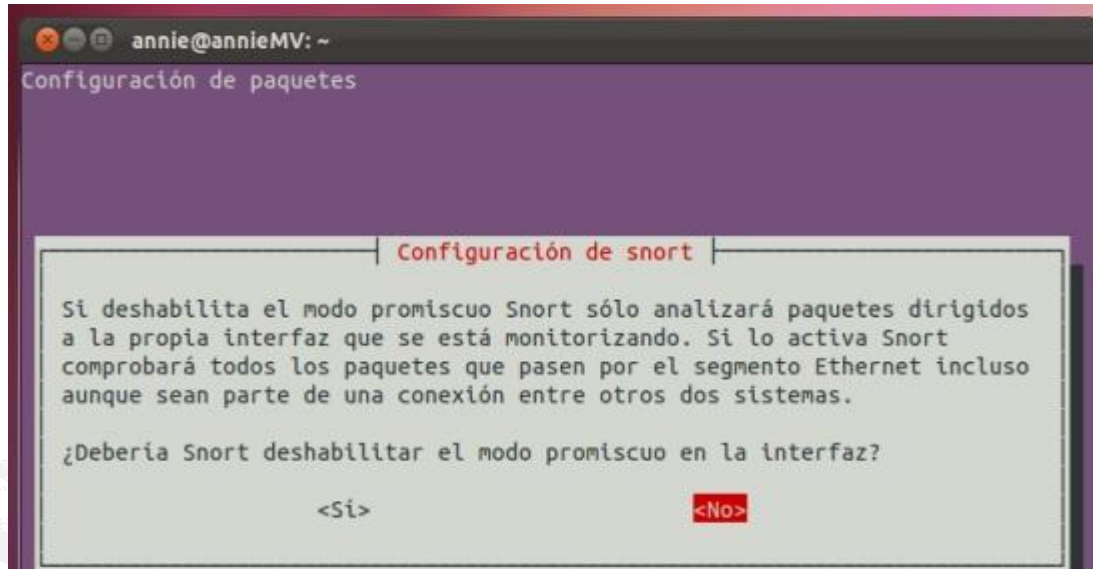
En la siguiente ventana de se escribe la interfaz obtenida de la anterior instrucción, y damos aceptar.



Ahora se deberá escribir la dirección de red que se desea escanear.

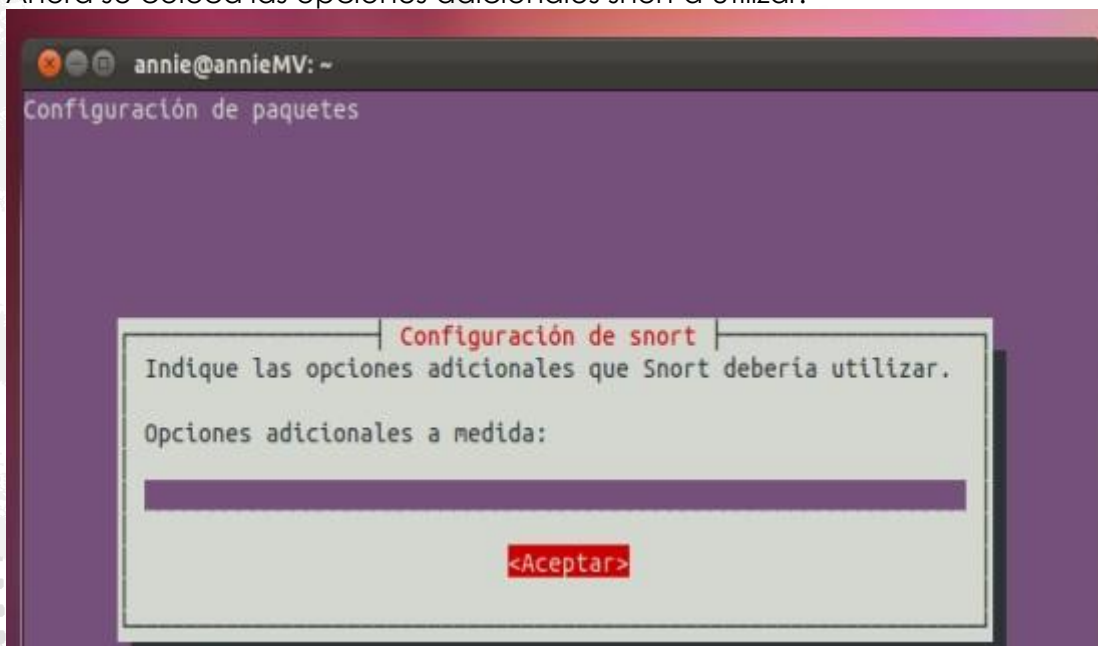


Ahora pide deshabilitar el modo promiscuo y le damos enter a la opción No.

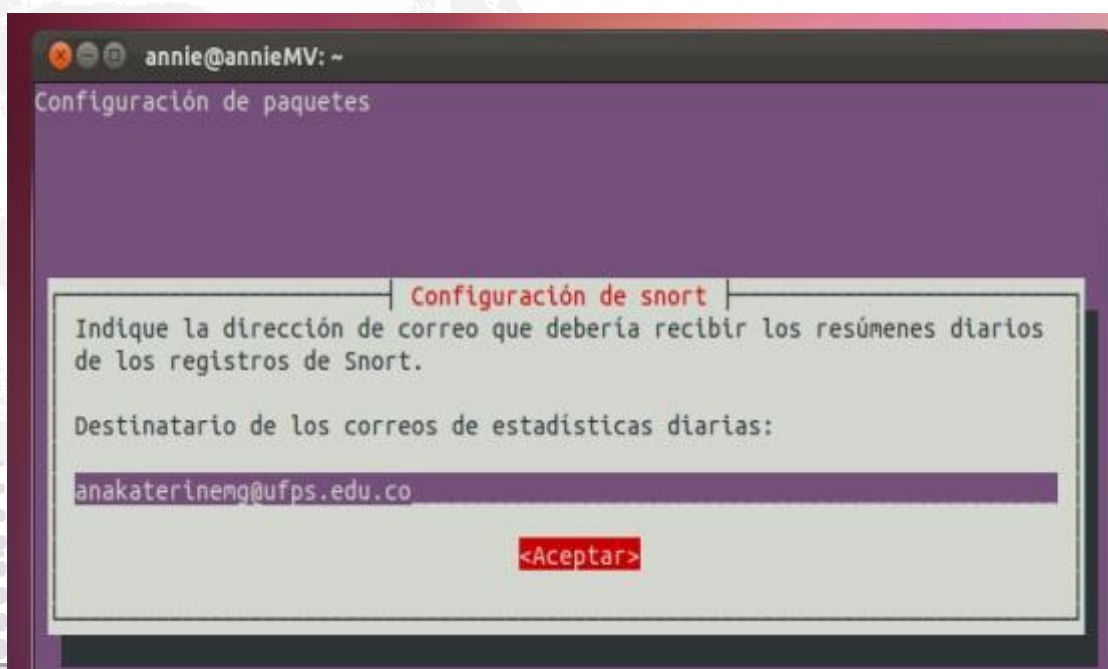
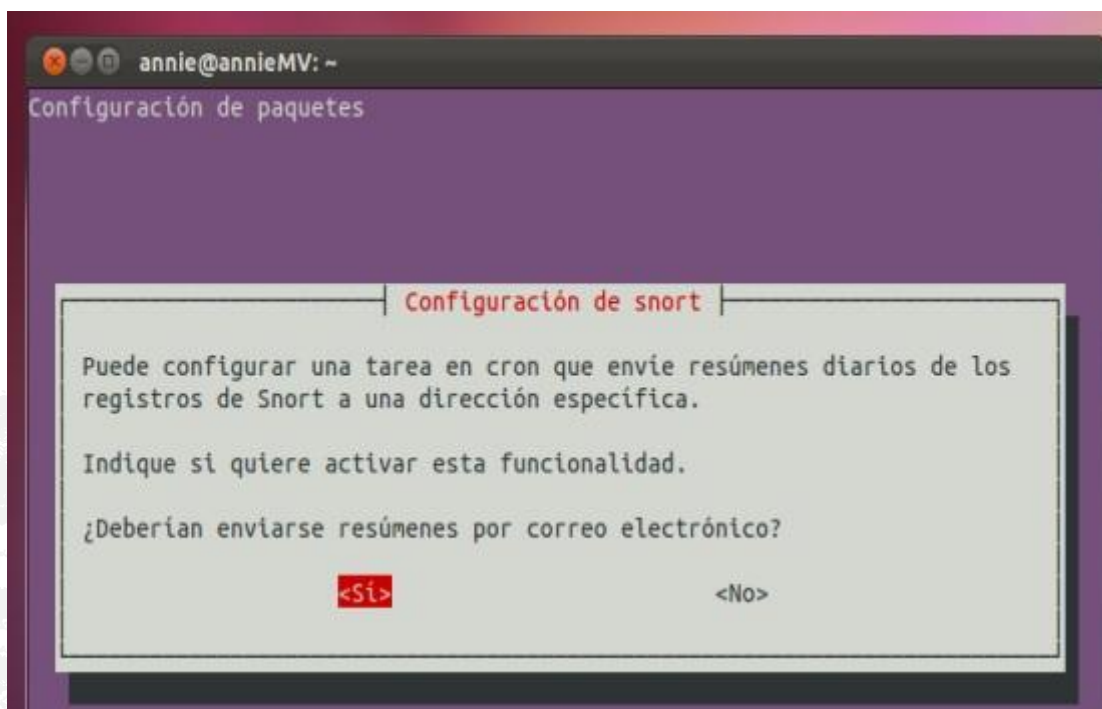


El modo promiscuo significa que se analizará todos los paquetes que pasen por el segmento aunque no sean de una conexión propia.

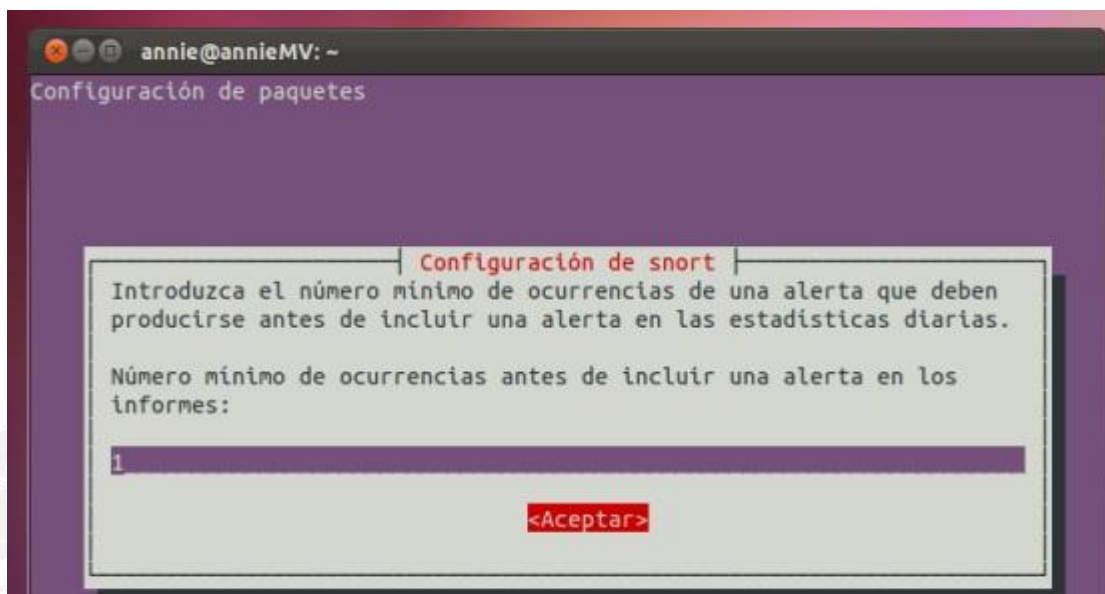
Ahora se coloca las opciones adicionales snort a utilizar:



La siguiente parte es para confirmar el envío de resúmenes al correo, primero se confirma si quiere habilitar esta opción y luego se digita el correo al cual se desea que se envíe dicha información.



Ahora se especifica la cantidad de informes que se incluyen por alerta:



Finalmente la solicitud del comando al finalizar para recargar las configuraciones hechas.



Una vez finalizado el asistente de configuración, se ejecuta el comando mostrado en la siguiente instrucción

```
annie@annieMV: ~
annie@annieMV:~$ sudo /etc/init.d/snort restart
[sudo] password for annie:
* Starting Network Intrusion Detection System snort [ OK ]
annie@annieMV:~$
```

CREACION DE REGLAS

Se puede crear reglas en el siguiente directorio

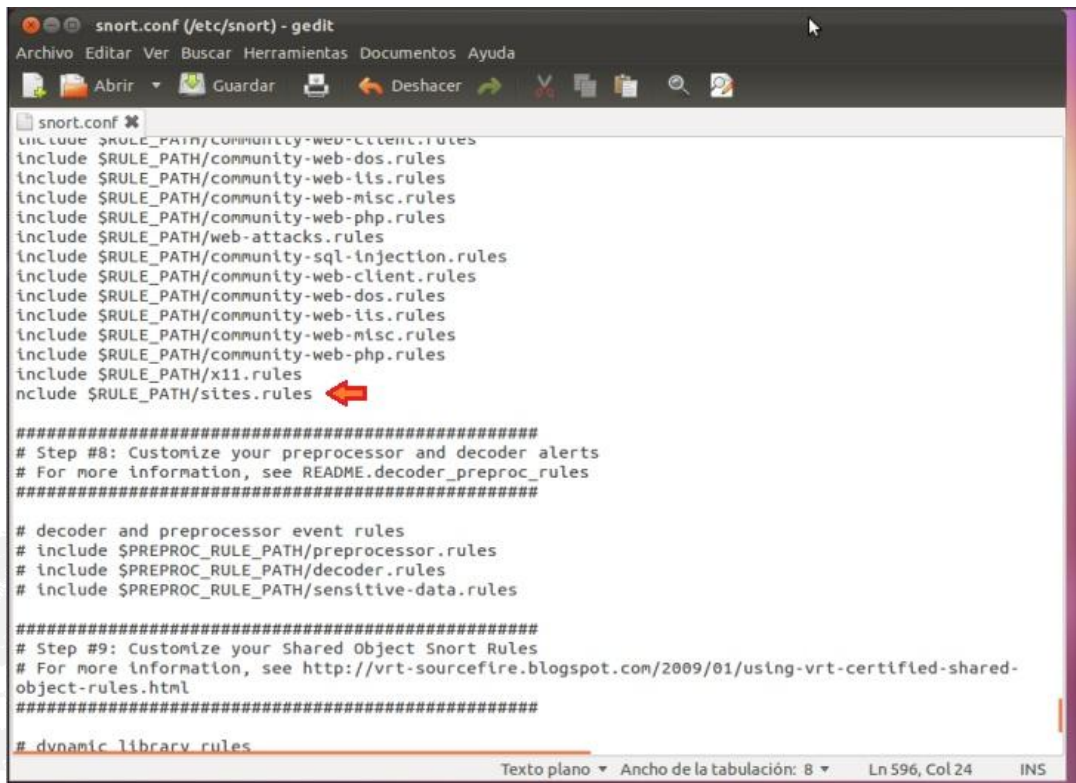
`/etc/snort/rules/nombreArchivo.rules`

```
*sites.rules (/etc/snort/rules) - gedit
Archivo Editar Ver Buscar Herramientas Documentos Ayuda
Abrir Guardar Deshacer
*sites.rules
alert tcp any any -> any any (msg:"Alguien entro a Facebook";content:"facebook";std:19910314;rev:1;)
alert tcp any any -> any any (msg:"Alguien esta intentando leer los puertos por
nessus";content:"nessus";std:19910315;rev:1;)
alert tcp any any -> any any (msg:"Ping";std:19919316;rev:1;)
```

Abro:

`/etc/snort/snort.conf`

En este archivo se agrega la nueva regla.



```

snort.conf (/etc/snort) - gedit
Archivo Editar Ver Buscar Herramientas Documentos Ayuda
snort.conf
include $RULE_PATH/community-web-client.rules
include $RULE_PATH/community-web-dos.rules
include $RULE_PATH/community-web-lis.rules
include $RULE_PATH/community-web-misc.rules
include $RULE_PATH/community-web-php.rules
include $RULE_PATH/web-attacks.rules
include $RULE_PATH/community-sql-injection.rules
include $RULE_PATH/community-web-client.rules
include $RULE_PATH/community-web-dos.rules
include $RULE_PATH/community-web-lis.rules
include $RULE_PATH/community-web-misc.rules
include $RULE_PATH/community-web-php.rules
include $RULE_PATH/x11.rules
include $RULE_PATH/sites.rules

#####
# Step #8: Customize your preprocessor and decoder alerts
# For more information, see README.decoder_preproc_rules
#####

# decoder and preprocessor event rules
# include $PREPROC_RULE_PATH/preprocessor.rules
# include $PREPROC_RULE_PATH/decoder.rules
# include $PREPROC_RULE_PATH/sensitive-data.rules

#####
# Step #9: Customize your Shared Object Snort Rules
# For more information, see http://vrt-sourcefire.blogspot.com/2009/01/using-vrt-certified-shared-
# object-rules.html
#####

# dynamic library rules

```

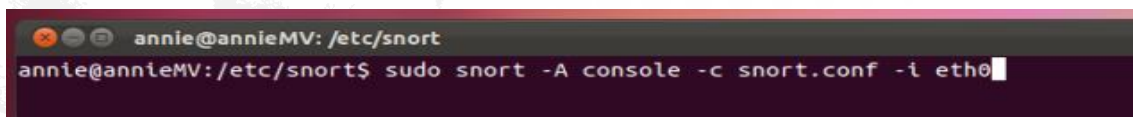
EJECUCION DE SNORT

1. Primero hay que dirigirse al directorio de snort.

```
cd /etc/snort/
```

2. Ahora ejecutamos la siguiente instrucción

```
snort -A console -c snort.conf -i eth0
```



```

annie@annieMV: /etc/snort
annie@annieMV:/etc/snort$ sudo snort -A console -c snort.conf -i eth0

```

Empieza a correr...


```
[9880] password for snort:
Running in packet dump mode

--== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "eth0".
Decoding Ethernet

--== Initialization Complete ==--

--== Snort! <*-
Version 2.9.2 IPv6 GRE (Build 78)
By Martin Roesch & The Snort Team: http://www.snort.org/snort/snort-team
Copyright (C) 1998-2011 Sourcefire, Inc., et al.
Using libpcap version 1.1.1
Using PCRE version: 8.12 2011-01-15
Using ZLIB version: 1.2.3.4
```

```
annie@annieMV: /etc/snort
15:37386 -> 66.220.152.19:443
06/26-14:00:11.741409 11.741409 11.741409 [1:19919316:1] Ping [1:19919316:1] [Priority: 0] {TCP} 66.220.152.19:443 -> 10.0.2.15:37386
06/26-14:00:11.741461 11.741461 11.741461 [1:19919316:1] Ping [1:19919316:1] [Priority: 0] {TCP} 10.0.2.15:37386 -> 66.220.152.19:443
06/26-14:00:11.741578 11.741578 11.741578 [1:19919316:1] Ping [1:19919316:1] [Priority: 0] {TCP} 66.220.152.19:443 -> 10.0.2.15:37387
06/26-14:00:11.744920 11.744920 11.744920 [1:19919316:1] Ping [1:19919316:1] [Priority: 0] {TCP} 66.220.152.19:443 -> 10.0.2.15:37386
06/26-14:00:11.785259 11.785259 11.785259 [1:19919316:1] Ping [1:19919316:1] [Priority: 0] {TCP} 66.220.152.19:443 -> 10.0.2.15:37385
06/26-14:00:11.793533 11.793533 11.793533 [1:19919316:1] Ping [1:19919316:1] [Priority: 0] {TCP} 66.220.152.19:443 -> 10.0.2.15:37385
06/26-14:00:11.889778 11.889778 11.889778 [1:19919316:1] Ping [1:19919316:1] [Priority: 0] {TCP} 66.220.152.19:443 -> 10.0.2.15:37385
06/26-14:00:11.893653 11.893653 11.893653 [1:19919316:1] Ping [1:19919316:1] [Priority: 0] {TCP} 10.0.2.15:37385 -> 66.220.152.19:443
06/26-14:00:11.897243 11.897243 11.897243 [1:19919316:1] Ping [1:19919316:1] [Priority: 0] {TCP} 66.220.152.19:443 -> 10.0.2.15:37385
06/26-14:00:11.897332 11.897332 11.897332 [1:19919316:1] Ping [1:19919316:1] [Priority: 0] {TCP} 10.0.2.15:37385 -> 66.220.152.19:443
06/26-14:00:11.897811 11.897811 11.897811 [1:19919316:1] Ping [1:19919316:1] [Priority: 0] {TCP} 66.220.152.19:443 -> 10.0.2.15:37385
```