[Cod.: CC481 Curso: Administración de Redes]
[Tema: *IPS-IDS SNORT*]

IPS-IDS SNORT

Objetivos

- Entender conceptos como el de IDS/ IPS
- Comprender el funcionamieno del IDS/IPS SNORT
- Instalar, configurar y hacer pruebas de SNORT en Ubuntu
- Verificar los resultados obtenidos después de la instalación y las pruebas.

Contenidos

- Ventajas y desventajas de usar SNORT
- Preparar entornos
- Creación del sistema
  - SNORT
  - Cliente
- Configuracion del Sistema
- Configuracion DHCP
- Instalacion de SNORT
- Configuración de SNORT
  - Prueba de funcionamiento
- Prueba de Intrusos
  - Instalacion de NMAP
  - Testeo de intrusión con NMAP

1. Ventajas y Desventajas de usar SNORT

Ventaja:
Debido a que es de código abierto, es altamente personalizable como requisito de toda empresa.
Mantiene los registros de los paquetes de datos que se muestran en forma amigable al humano desde su dirección IP.

Motorización constante de la red: Puede usarse para supervisar y monitorear tanto la conexión DSL en el hogar como un sitio web corporativo. Se puede identificar desbordamientos de búfer, ataques CGI, desbordamientos, escaneos de puertos ocultos, consultas NetBIOS y sondeos SMB, puertas traseras conocidas y vulnerabilidades del sistema, NMAP y otros escáneres de puertos y clientes DDOS. Alerta a los usuarios sobre aquellos ataques y funciones maliciosas.

Obserbvar datos en el contexto del protocolo: Cuando un NIDS realiza un análisis rotatorio, observa las cargas útiles de TCP y UDP. Los sensores pueden detectar actividad sospechosa porque saben cómo deben funcionar los protocolos.

Calificar y cuantificar ataques: Un IDS analiza la cantidad y los tipos de ataques. Esta información se puede usar para cambiar sus sistemas de seguridad o implementar nuevos controles que sean más efectivos. También se puede analizar para identificar errores o problemas de configuración de dispositivos de red. Las métricas se pueden utilizar para futuras evaluaciones de riesgo.

Desventajas:

Los softwares de detección de intrusos son por lo general la primera línea de defensa para muchas empresas, aunque son necesarios para la seguridad de la red, tienen algunas desventajas.

Direccion de Origen: los Ids proporcionan información de las direcciones de red asociadas con el paquete de red, el problema viene cuando el paquete de Ip es falsificada o codificada. En estos casos no se podrían impedir las intrusiones.

Paquetes Encriptados: No son procesados por los software de detección de intrusos. Por lo tanto, el paquete encriptado puede permitir una intrusión en la red que no se ha descubierto hasta que se hayan producido intrusiones de red más significativas. Los paquetes cifrados también se pueden configurar para que se activen a una hora o fecha específica una vez que se hayan plantado en la red. Esto podría liberar un virus u otro error de software.

Modulo Analítico: El módulo analítico tiene una capacidad limitada para analizar la información de origen que se recopila durante la detección de intrusos. El resultado de este límite es que solo una parte de la información de origen está en búfer. Si bien un profesional de TI que supervisa el sistema recibirá una alerta de que se ha detectado un comportamiento anormal, no podrá saber de dónde se originó el comportamiento. La respuesta a esta información solo puede ser intentar detener el acceso a la red no autorizado. Si se pudiera obtener más información, el profesional

de TI podría adoptar un enfoque defensivo para evitar futuras intrusiones antes de que ocurran.

Falsas Alarmas: Estas falsas alarmas se incrementan en las redes donde hay una gran cantidad de usuarios. Para evitar perseguir estas falsas alarmas, los profesionales de TI deben recibir una amplia capacitación para que puedan reconocer qué es una falsa alarma y qué no lo es. El costo de completar esta capacitación es otra desventaja del software de detección de intrusos con el que las empresas deben lidiar.

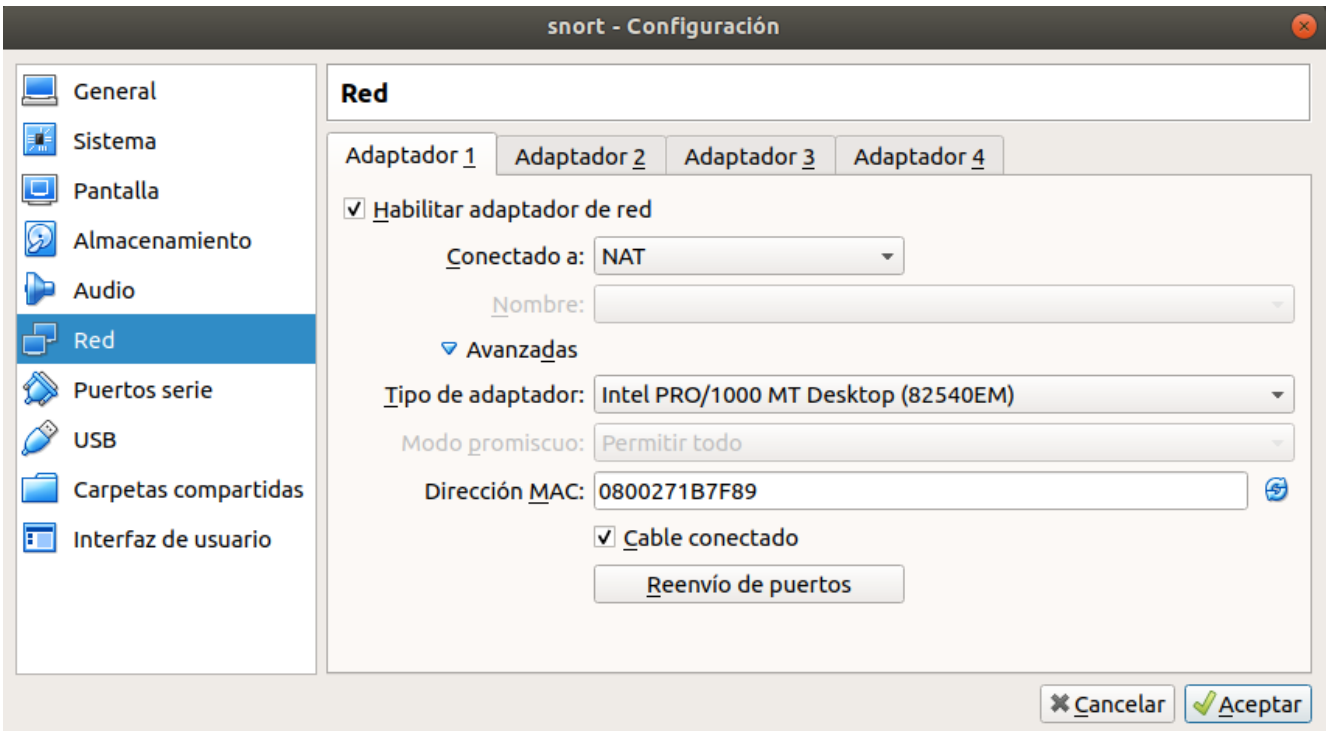
2. Preparación de entornos

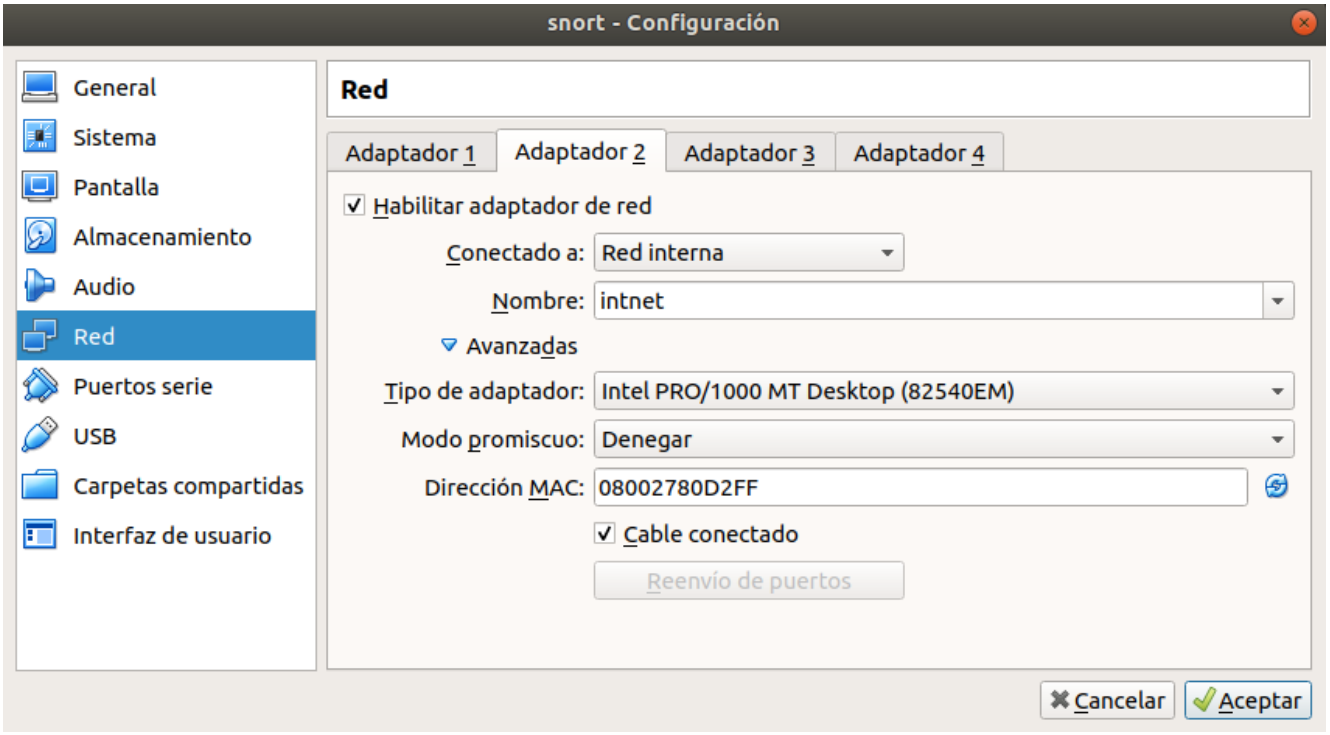
En esta práctica necesitaremos dos máquinas virtuales:

- El Servidor-SNORT en la cual se instalará y se realizará la configuración del servidor SNORT
- Una máquina estación de trabajo donde realizaremos las pruebas.

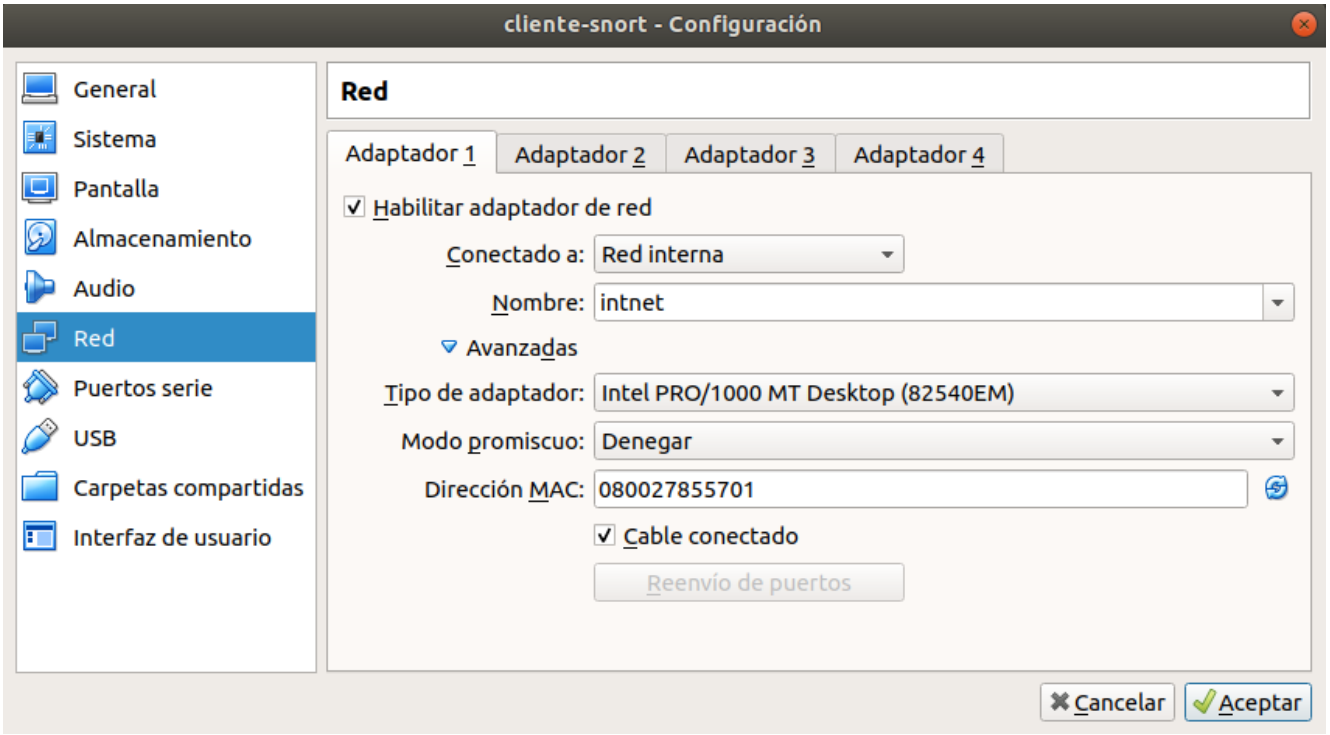
3. Creación del sistema

1. [Servidor] El servidor tiene dos tarjetas de red una que deriva el tráfico al router y otra que lleva la configuración interna. Recordemos que ninguna tarjeta de Red deberá tener la misma dirección física o MAC si es así deberemos refrescar.



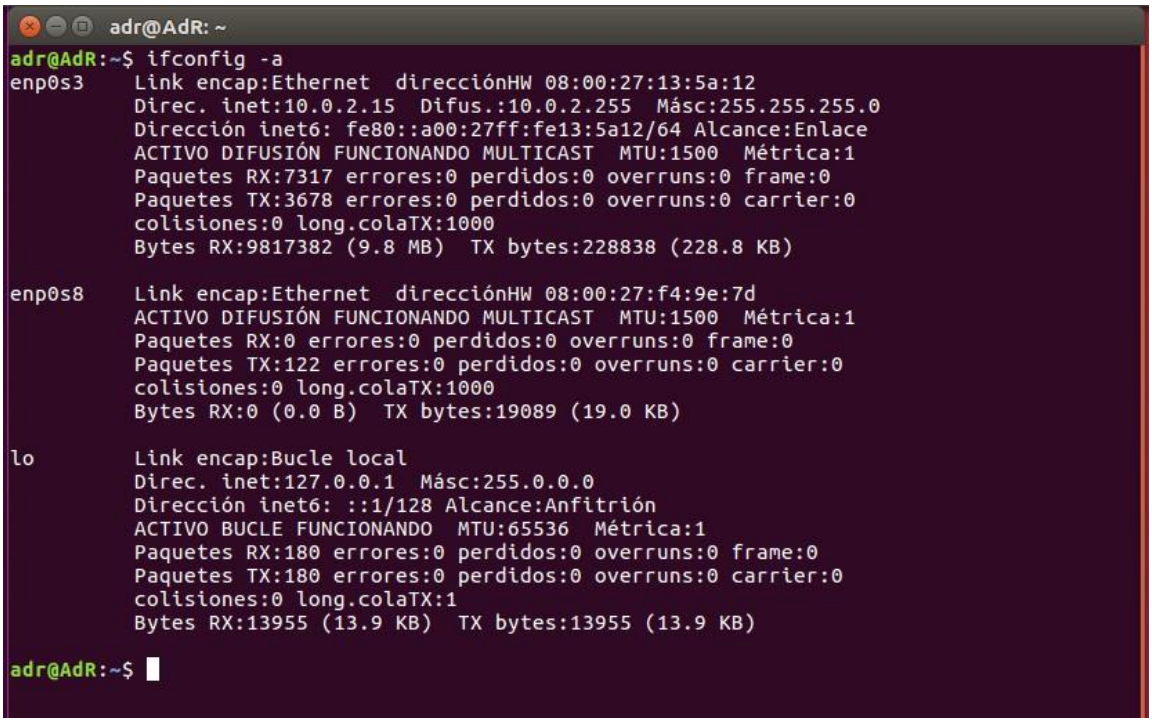


2. [Cliente] Se realiza la conexión a la red interna.



4. Configuración DHCP

De acuerdo con la preparación del entorno esta maquina debe tener 2 subredes, una que tiene salida a internet (enp0s3) y la otra sera nuestra subred vigilada por el SNORT (enp0s8)



Procederemos a hacer la configuración respectiva para la subred enp0s8.

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto enp0s3
iface enp0s3 inet dhcp


auto enp0s8
iface enp0s8 inet static
address 192.168.0.1
network 192.168.0.0
netmask 255.255.255.0
broadcast 192.168.0.255
```

Realizamos un reinicio de nuestro servicio network con el siguiente comando **sudo /etc/init.d/networking restart** ahora procederemos a verificar que la configuración ha sido establecido correctamente realizando un **ifconfig.**

```
adr@AdR:/etc/snort$ ifconfig
enp0s3    Link encap:Ethernet  direcciónHW 08:00:27:1b:7f:89
          Direc. inet:10.0.2.15  Difus.:10.0.2.255  Másc:255.255.255.0
          Dirección inet6: fe80::a00:27ff:fe1b:7f89/64 Alcance:Enlace
          ACTIVO DIFUSIÓN FUNCIONANDO MULTICAST  MTU:1500  Métrica:1
          Paquetes RX:3807 errores:0 perdidos:0 overruns:0 frame:0
          Paquetes TX:2186 errores:0 perdidos:0 overruns:0 carrier:0
          colisiones:0 long.colaTX:1000
          Bytes RX:3453613 (3.4 MB)  TX bytes:258745 (258.7 KB)

enp0s8    Link encap:Ethernet  direcciónHW 08:00:27:80:d2:ff
          Direc. inet:192.168.0.1  Difus.:192.168.0.255  Másc:255.255.255.0
          Dirección inet6: fe80::a00:27ff:fe80:d2ff/64 Alcance:Enlace
          ACTIVO DIFUSIÓN FUNCIONANDO MULTICAST  MTU:1500  Métrica:1
          Paquetes RX:3280 errores:0 perdidos:0 overruns:0 frame:0
          Paquetes TX:4676 errores:0 perdidos:0 overruns:0 carrier:0
          colisiones:0 long.colaTX:1000
          Bytes RX:330315 (330.3 KB)  TX bytes:5006148 (5.0 MB)

lo        Link encap:Bucle local
          Direc. inet:127.0.0.1  Másc:255.0.0.0
          Dirección inet6: ::1/128 Alcance:Anfitrión
          ACTIVO BUCLE FUNCIONANDO  MTU:65536  Métrica:1
          Paquetes RX:167 errores:0 perdidos:0 overruns:0 frame:0
          Paquetes TX:167 errores:0 perdidos:0 overruns:0 carrier:0
          colisiones:0 long.colaTX:1
          Bytes RX:12227 (12.2 KB)  TX bytes:12227 (12.2 KB)
```

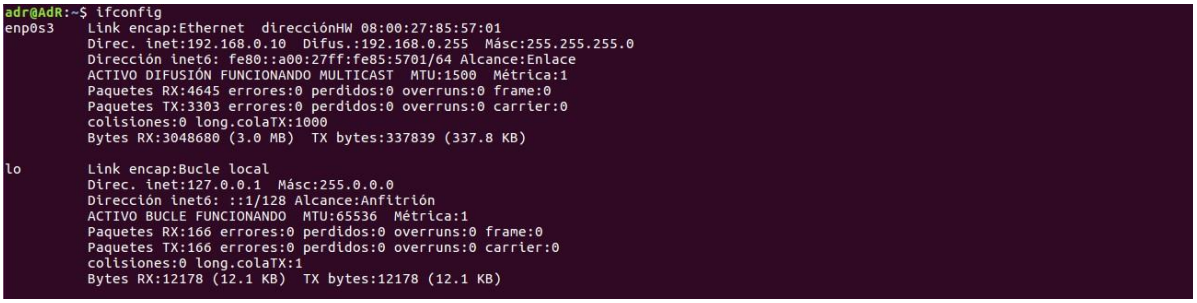
Ahora se procederá a la instalación de servicio DHCP con la regla **sudo apt-get install isc-dhcp-server** en el .siguiente paso procederemos a hacer la configuración correspondiente para dar servicio DHCP a nuestros clientes , en este caso para la configuración usaremos **gedit** ustedes pueden usar nano vim o lo que prefieran , accedemos al archivo de cnfiguracion **dhcpd.conf** con el siguiente comando **sudo gedit /etc/dhcp/dhcpd.conf** y realizamos la siguiente configuración.

```
option domain-name "example.org";
option domain-name-servers 8.8.8.8,8.8.4.4;

default-lease-time 600;
max-lease-time 7200;

log-facility local7;

subnet 192.168.0.0 netmask 255.255.255.0{
  range 192.168.0.10 192.168.0.40;
  option domain-name-servers 8.8.8.8,8.8.4.4;
  option subnet-mask 255.255.255.0;
  option routers 192.168.0.1;
  option broadcast-address 192.168.0.255;
  default-lease-time 600;
  max-lease-time 7200;
}
```

Procederemos a reiniciar el servicio DHCP con el siguiente comando **sudo /etc/init.d/isc-dhcp-server restart** en el servidor .

Cliente

después vamos a verificar que nuestro cliente ha recibido una IP de acuerdo al rango que hemos establecido.



5. Configuración de IPTABLES en el servidor

Aunque tenemos un tema que explica al detalle el firewall de un servidor con el paquete IPTABLES necesitaremos configurar nuestro servidor para que pueda asignar direcciones a los clientes que lo soliciten. Se ha creado un fichero para la configuración que vamos a realizar en estos momentos y en él podemos observar una breve explicación de cada sentencia que realiza. Un aspecto muy importante es cambiar las variables de **“INTERNET”** y **“LAN_IN”** por las interfaces de red correctas según hayamos configurado nuestro servidor.

El primer paso que deberemos realizar es la descarga del archivo para esta práctica, el archivo está configurado para un proxy transparente:

• bit.ly/IplUZw

Tener en cuenta que en el fichero se encuentran las interfaces correctas para la configuración de la guía no para las de su máquina. Por tanto, cambie

el nombre de las interfaces (expuesta como constantes al comienzo del script) por la correcta configuración de sus máquinas.

Así mismo, tener en cuenta que la siguiente regla firewall es el que nos otorga acceso a Internet para los clientes en nuestra red local.

```
# iptables -t nat -A POSTROUTING 192.168.0.1/24 -o enp0s3 -j MASQUERADE
```

Para no tener que configurar IPTABLES cada vez que reiniciemos el equipo vamos a hacer que lance el script cada vez que se reinicie nuestro equipo. El primer paso es copiar el script descargado a **"/etc/init.d"**

```
# sudo cp iptables_proxy.sh /etc/init.d
```

Deberemos de cambiar el propietario y permisos:

```
# sudo chown root:root iptables_proxy.sh
# sudo chmod 700 iptables_proxy.sh
```

Por último editamos el fichero **"/etc/rc.local"** para que ejecute el shell que acabamos de crear al iniciar el sistema. Para ello añadimos antes de "exit 0" del fichero: XXX ver como es para ubuntu 18.04

```
### END INIT INFO
cd /etc/init.d
./iptables_proxy.sh
```

```
# Default-Start:     2 3 4 5
# Default-Stop:
# Short-Description: Run /etc/rc.local if it exist
### END INIT INFO
cd /etc/init.d
./iptables_proxy.sh

PATH=/sbin:/usr/sbin:/bin:/usr/bin
```

Por último reiniciamos el servidor para que realice los cambios y una vez realizado verificamos que las nuevas reglas de Firewall.

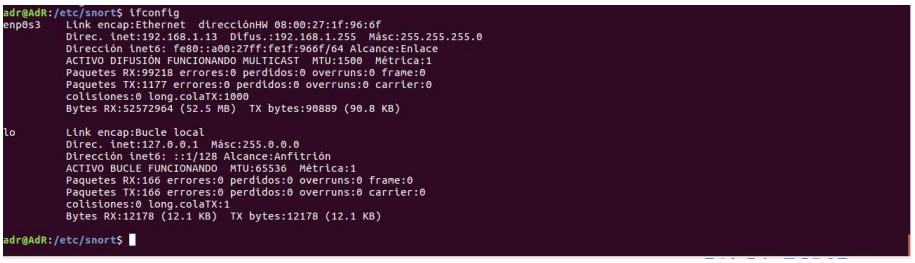
```
# sudo shutdown -r now

# sudo iptables -S
```

Ahora vamos a nuestro cliente y verificamos que tenga acceso a internet

6. Instalación de SNORT

Ahora se instalara el snort en nuestra maquina que tendrá SNORT , tenemos que tener la información de la dirección nuestra subred y el nombre de esta misma.

La cual podremos visualizar esta información con un **ifconfig** para nuestro caso estamos trabajando y el el nombre de esa subred. en este caso es 192.168.1.0/24 y enp0s3.



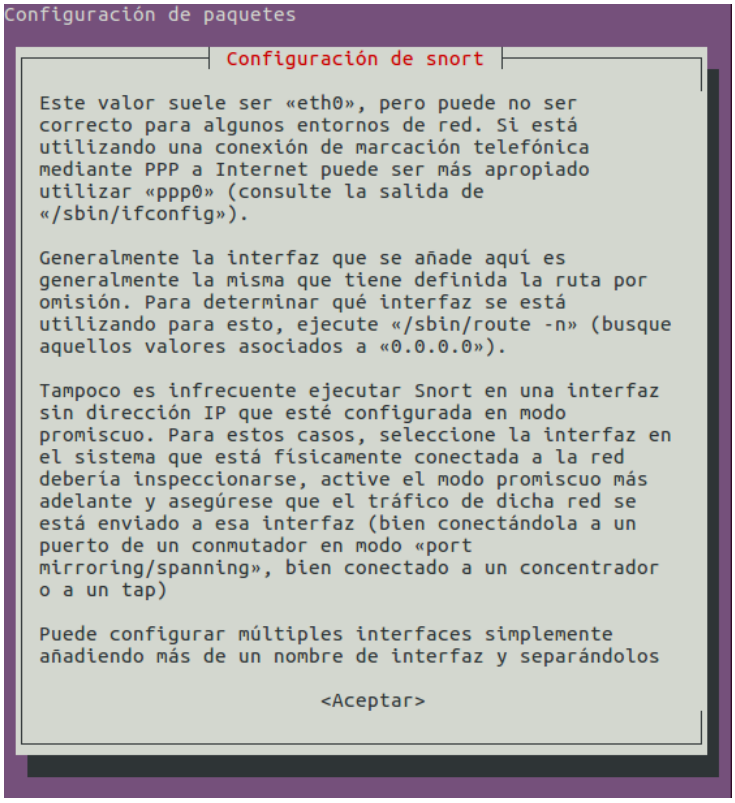
Ahora procederemos a instalar el snort para eso haremos un :

```
# sudo apt-get install snort
```

6. Configuración de SNORT

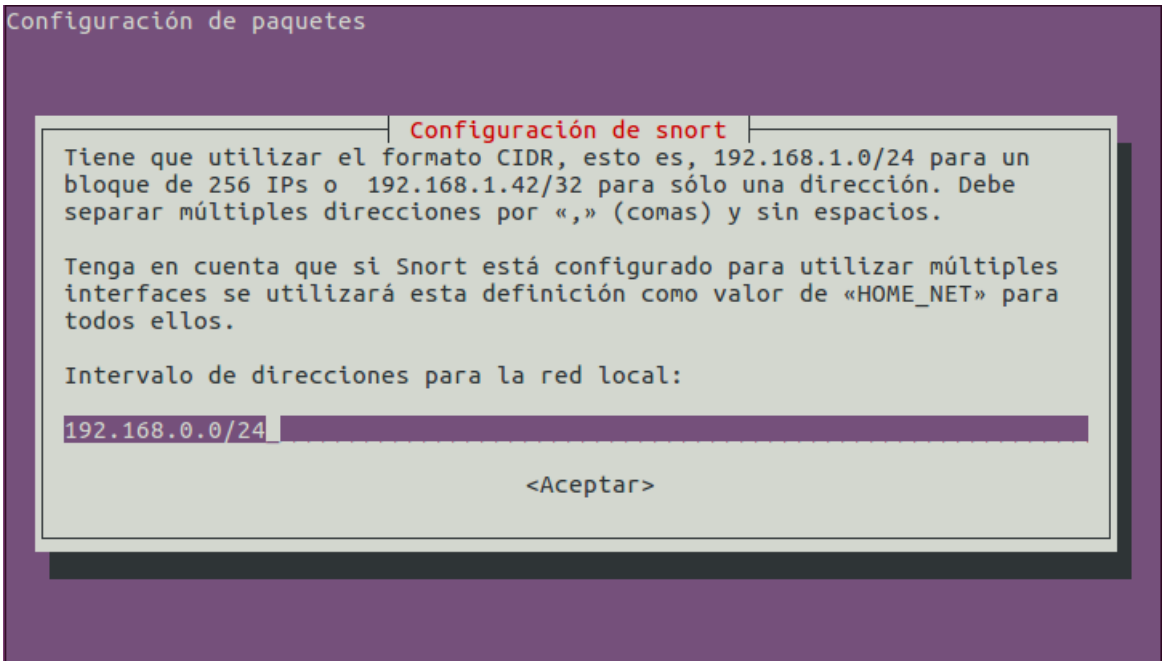
Una vez hacemos los comando de la instalación del SNORT nos aparecerá un cuadro donde nos indica que valores debemos de tener en cuenta para la configuración como el nombre de la subred y la dirección, en el punto anterior ya habíamos guardado esos datos.

Para seguir con la configuración del SNORT al cuadro que nos aparece le daremos en **“Aceptar”.**



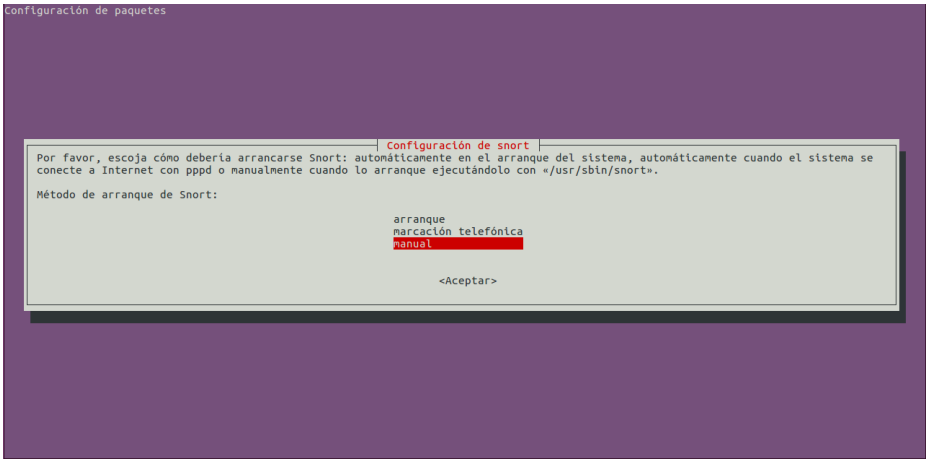
Despues de **“Aceptar”** nos pedirá el tipo de red que tenemos en nuestro caso es **enp0s3** y lo pondremos en el cuadro.

En el cuadro siguiente que nos aparecerá colocamos la subred en que queremos que funcione el SNORT en nuestro caso será **192.168.0.0/24**



Una vez de colocar la subred y aceptar , regresaremos a la línea de comados y escribiremos lo siguiente: # sudo dpkg-reconfigure snort

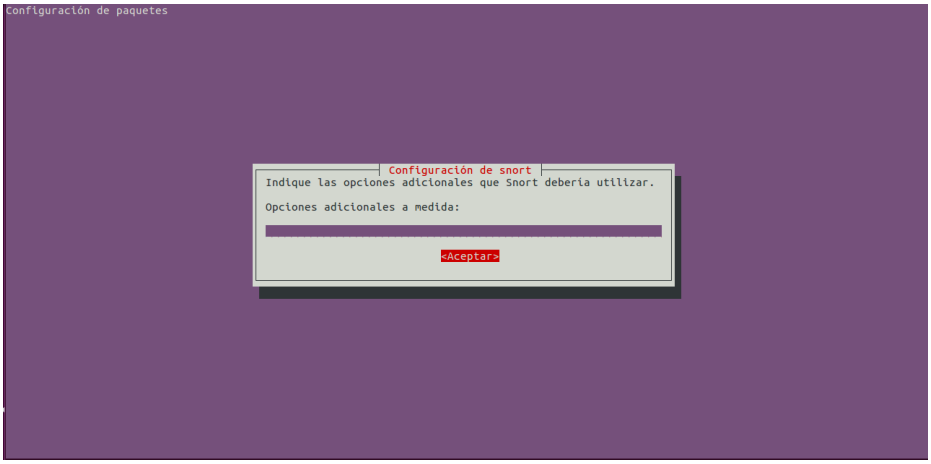
Aparecera algo parecido a la siguiente imagen y tendremos que escoger la opción **manual** y aceptamos.



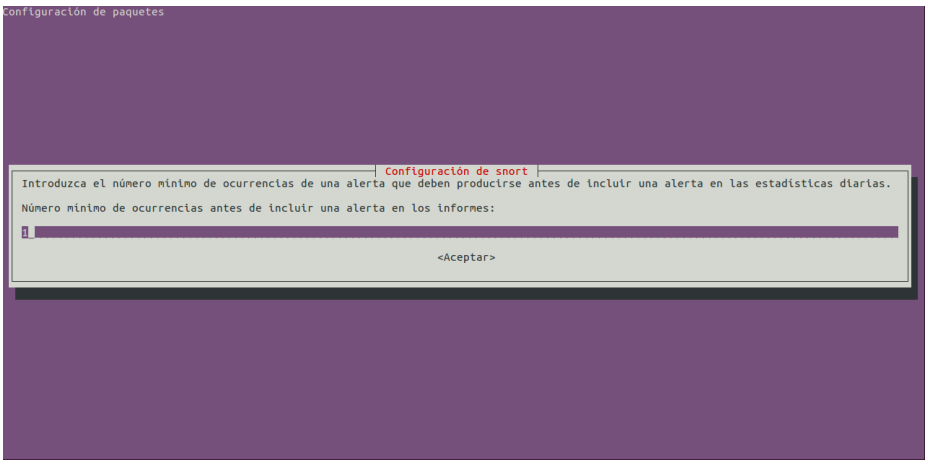
Volvemos a elegir la subred que queremos trabajar.

Al cuadro siguiente escogemos la opción **No .**

Al cuadro siguiente no se escribirá nada y se dara en **Aceptar**



Al cuadro siguiente que nos aparecerá nos pedirá si queremos que los resúmenes se envie a nuestro correo electrónico le daremos en **Si** , nos volverá aparecer un cuadro mas ,pondremos nuestro correo y le damos en **aceptar**.



Una vez acabado el proceso anterior es recomendable reiniciar el servicio SNORT para es haremos:

```
# sudo /etc/init.d/snort restart
```

Ahora se preocedera a configurar las reglas para decirle al SNORT que va a escanear, para eso creamos el siguiente fichero en la siguiente ruta , usaremos gedit para hacer la configuración de este fichero para eso haremos :

```
# sudo gedit /etc/snort/rules/sites.rules
```

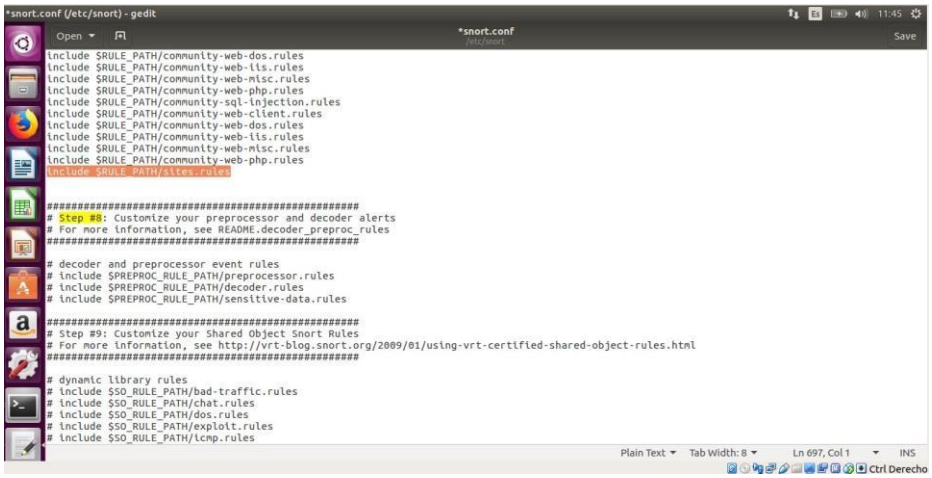
Una vez dentro del fichero colocaremos las siguientes reglas , ojo no equivocarse con ningún **“ ;** o algo parecido.

```
alert tcp 192.168.0.0/24 any -> any any (msg: "alguien esta ingresando a youtube";content:"youtube";sid:199;rev:1;)
alert tcp any any -> any any (msg: "alguien esta ingresando a facebook";content:"facebook";sid:198;rev:1;)
alert tcp any any -> any any (msg: "alguien esta ingresando a ebay";content:"ebay";sid:197;rev:1;)
alert icmp any any -> any any (msg: "ping ads";sid:196;rev:1;)
alert tcp 192.168.0.0/24 any -> 192.168.0.1 20:21 (msg: "Conexion al servidor FTP";sid:1000001;rev:1;)
```

Ahora vamos a editar el archivo de configuración SNORT para eso haremos :

```
# sudo gedit /etc/snort/snort.conf
```

Si estamos utilizando gedit podemos utilizar el buscador con ,ctrl F, y buscar **step #8** y colocamos la reglas que creamos como se muestra en la siguiente imagen.



Un vez que agregamos la regla y guardamos volvemos a reiniciar el servicio hacemos :

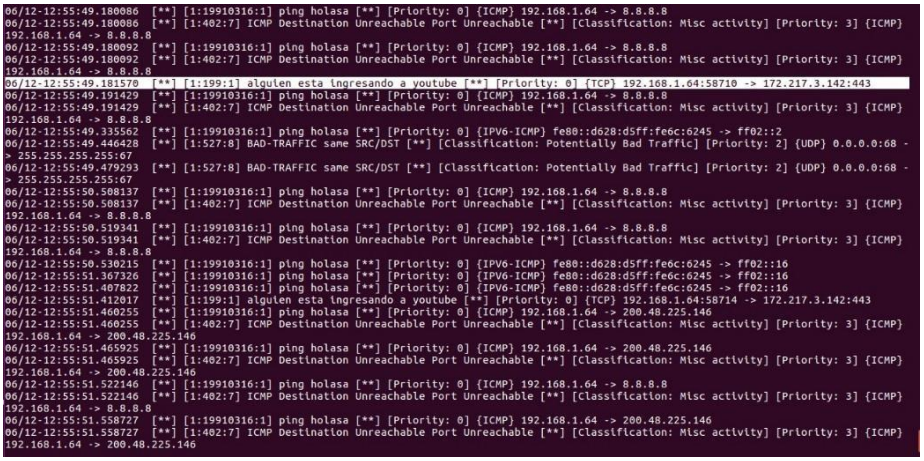
```
# sudo /etc/init.d/snort restart
```

Ingresamos a la siguiente carpeta para el correcto funcionamiento hacemos un **“cd /etc/snort”** luego colocamos el comando “**sudo snort –A console –c snort.conf –i enp0s3”** para iniciar nuestro SNORT.

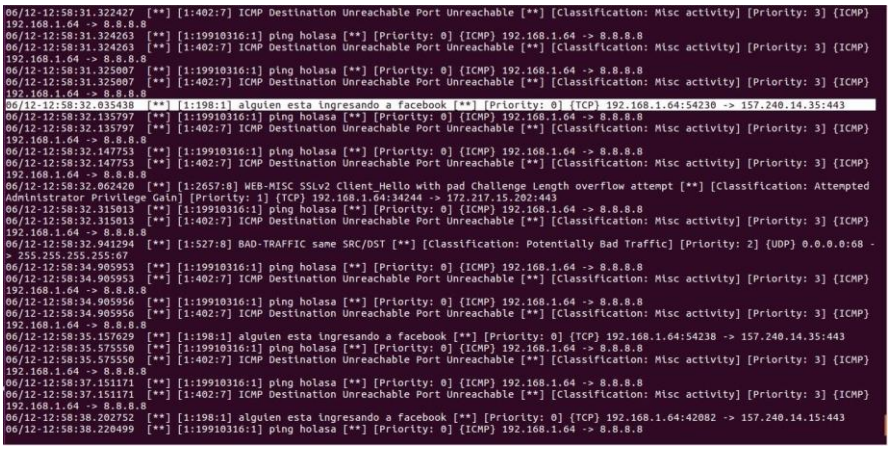
6.1 Prueba de Funcionamiento

Ahora iremos a nuestra maquina cliente y procederemos a las paginas para las respectivas pruebas, accedemos desde cualquier navegador que tengamos y entramos a la pagina **www.youtube.com** .

Ahora vamos a nuestra maquina que tenga el SNORT y verificamos que salga el siguiente mensaje :



Ahora vamos a nuestra maquina cliente y entramos a www.facebook.com y veremos desde nuestra maquina que tiene el SNORT el siguiente mensaje:



7. Prueba de Intrusos

7.0 Prueba de FTP

En esta parte haremos el comando el comando:

```
ftp 192.168.0.1
```

7.1 Instalación de NMAP

Ahora para la prueba de intrusos haremos la instalación de NMAP en la maquina que tiene el SNORT.

```
# sudo apt-get install nmap
```

7.1.2 Establecer reglas para NMAP

modo ICMP:

```
alert icmp any any -> 192.168.0.1 any (msg: "ICMP NMAP ping detectado"; dsize:0;sid:10000004; rev: 1;)
```

modo TCP:

```
alert tcp any any -> 192.168.0.1 22 (msg: "TCP NMAP detectado";sid:10000005; rev:2; )
```

modo UDP:

```
alert udp any any -> 192.168.0.1 22 ( msg:"UDP Nmap detectado"; sid:1000010; rev:1; )
```

• La palabra clave **msg** contiene el mensaje que se mostrará una vez que se detecte el tráfico de ataque.

• La palabra clave **flags** se usa para verificar si el indicador TCP SYN está establecido.

• La palabra clave **sameip** permite que las reglas de snort comprueben si la fuente P es la misma que la de destino P.

• La palabra clave **sid** se utiliza para identificar de manera simple las reglas de Snort.

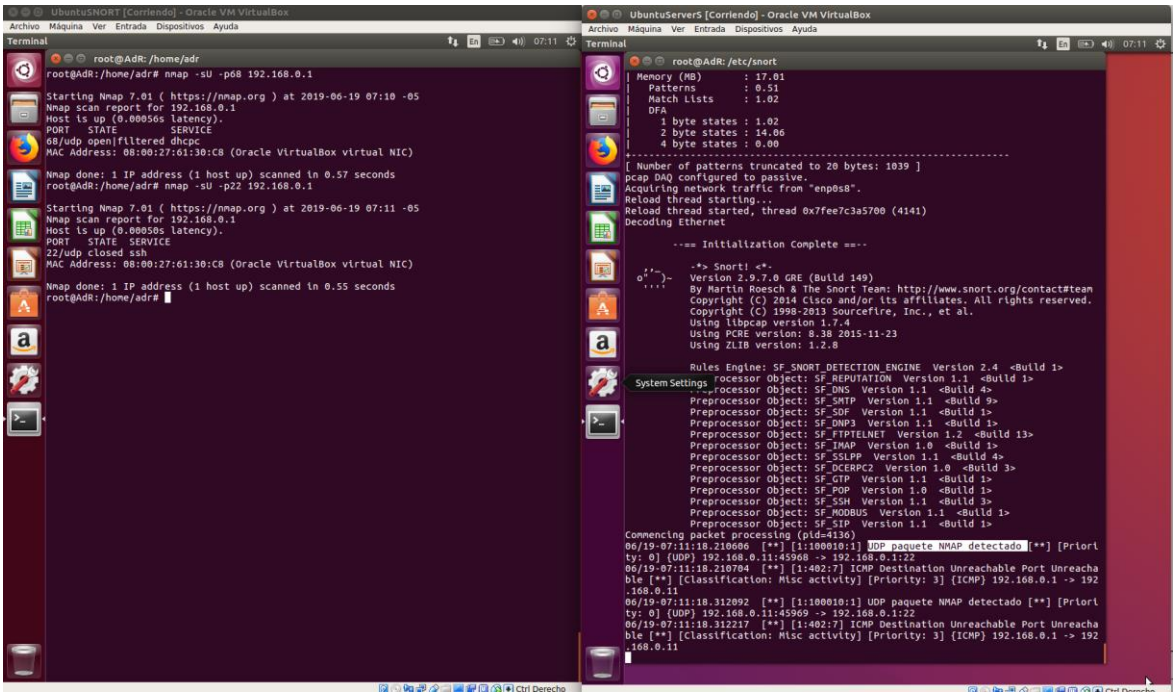
• La palabra clave **rev** se utiliza para identificar de forma única las revisiones de las reglas de Snort.

7.1.3 Testeo de intrusión con NMAP

Despues de la instalación en el cliente ponemos el siguiente comando:

```
# nmap -sP 192.168.0.1 –disable-arp-ping

# nmap -sT -p22 192.168.0.1

#nmap -sU -p22 192.168.0.1
```

Esto hará que se simule un ataque, y ahora iremos a nuestra máquina que contiene nuestro SNORT y saldrá el siguiente mensaje:



7.2 Prueba de Intrusos detección Syn Flood

7.2.1 Instalación de Syn Flood

Ahora para la prueba de intrusos haremos la instalación de hping en la maquina de donde enviaremos el ataque.

```
# sudo apt-get install hping3
```

7.2.3 Establecer reglas para Syn Flood

modo TCP:

```
alert tcp any any -> 192.168.0.1 22 (msg: "TCP SYN paquete detectado";flags:S;
threshold: type threshold, track by_dst, count 20,seconds 60 ;sid:5000001; rev:1; )
```

modo UDP:

```
alert udp any any -> 192.168.0.1 22 (msg: "UDP SYN paquete detectado"; threshold: type
threshold, track by_dst, count 20,seconds 60 ;sid:5000001; rev:1; )
```

La palabra clave umbral significa que esta regla se registra cada 20:

- La palabra clave threshold significa que esta regla se registra cada 20 evento en este SID durante un intervalo de 60 segundos. Entonces, si menos de 10 eventos ocurren en 60 segundos, nada se registra. Una vez que un el evento se registra, se inicia un nuevo período de tiempo para el tipo = threshold.

- La palabra clave track by_dst significa hacer un rastreo por IP de destino.
- La palabra clave de count significa el número de conteos de eventos.

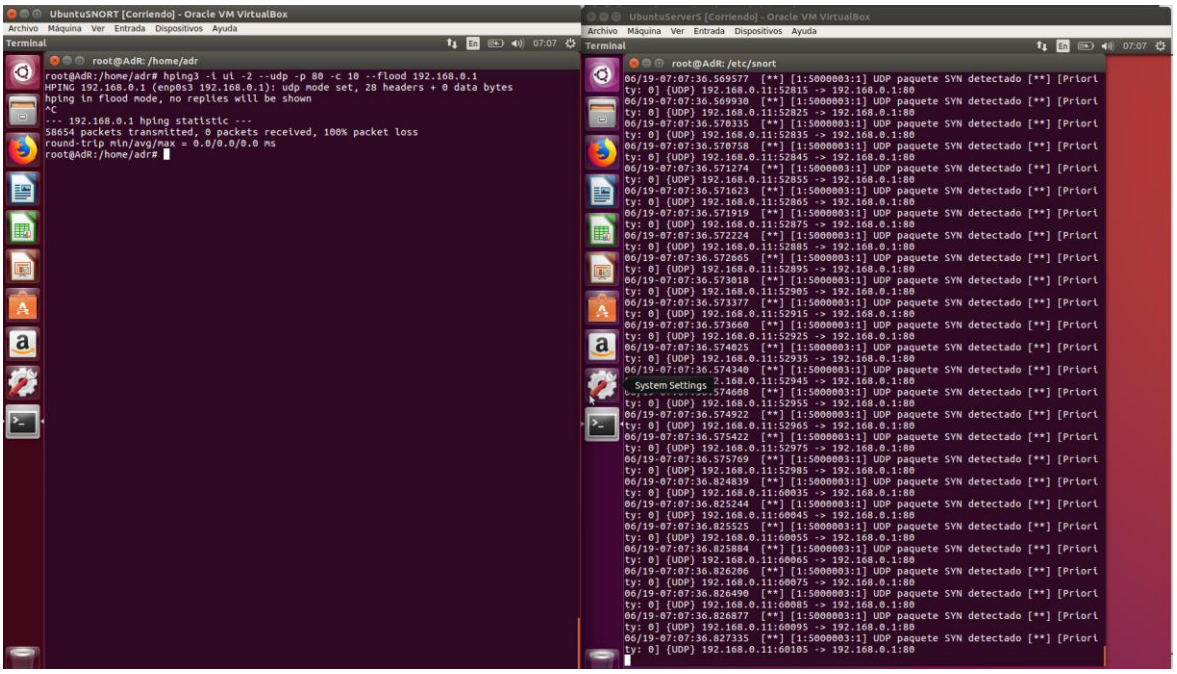
- La palabra clave seconds es el período de tiempo durante el cual se acumula el recuento.

7.2.4 Testeo de intrusión con Sys flood

Despues de la instalación en el cliente ponemos el siguiente comando:

```
# hping3 -i ui -S -p -80 -c -10 --flood 192.168.0.1

# hping3 -i ui -S -2 –udp -S -p -80 -c -10 --flood 192.168.0.1
```

-c indica el numero de paquetes enviados



8. Casos Extras

8.1 Instalación de Interface GUI-snort(BASE)

BASE es el motor de análisis y seguridad básico. Se basa en el código del proyecto Analysis Console for Intrusion Databases (ACID). Esta aplicación ofrece una interfaz web para consultar y analizar las alertas provenientes de un sistema SNORT IDS.

Seguir con los siguietes pasos de instalación y confguraciones:

Ingresar al directorio donde se realiza la descarga

 # cd /tmp && wget

http://sourceforge.net/projects/secureideas/files/latest/download

Descomprimir archivo

 # tar -xzvf base-1.4.5.tar.gz

cambiar de directorio

 # cp -r base-1.4.5/ /var/www/base

Ingresar al directorio

 # cd /var/www/base/

Realizar copia

Para la configuración, editamos el archivo base_conf.php.dist, modificamos a base_conf.php, y modificamos los siguientes parámetros

 # cp base_conf.php.dist base_conf.php

#vi base_conf.php

El campo está vacío, así que insertamos la base.

 # BASE_urlpath = '/base';

insertando adodb directorio

#DBlib_path = '/usr/share/php/adodb';

Pondremos aquí el nombre de la base de datos que se creó anteriormente

#alert_dbname = 'snort';

Este es el nombre de la máquina donde se encuentra la base de datos

#alert_host = 'localhost';

El puerto de las alertas, se puede dejar vacío si se desea.

#alert_port = '3306';

Debe insertar el nombre de usuario de la base de datos

#alert_user = 'snort';

Debe insertar la contraseña de la base de datos

#alert_password = 'snortpassword';

Después de que todo esté listo, podemos abrir un navegador y escribir

https://localhost/base

8.2 Otros comandos

Para visualizar el tráfico de paquetes TCP, UDP e ICMP en el terminal: **Snort –v**

Snort excepto por interceptar el tráfico, también registra los contenidos de este último en el disco duro, y todos los que se reciben se organizarán en un directorio / registro, en función del origen de la IP: **snort –vde –l /var/log/snort**

Para los paquetes de "registro" solo en una red específica, simplemente especifique el rango de direcciones que se utilizan en ella:

snort –vde –l /var/log/snort 192.168.0.0/24

Una vez que se hayan guardado los paquetes, puede consultar con la opción -r: **snort –dvr packet.log** o también mostrar con: **snort –dvr packet.log icmp**