INSTALACIÓN DE UN HONEYPOT Y NIDS

WILLIAM ALIRIO BERMON RICO
FRANCISCO JAVIER BASTOS ACEVEDO

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER
FACULTAD DE INGENIERÍAS
INGENIERÍA DE SISTEMAS
SAN JOSE DE CUCUTA
2013

INSTALACIÓN DE UN HONEYPOT Y NIDS

WILLIAM ALIRIO BERMON RICO
CÓDIGO: 1150030
FRANCISCO JAVIER BASTOS ACEVEDO
CÓDIGO: 1150124

Trabajo presentado como requisito para la asignatura de SEGURIDAD INFORMÁTICA

DOCENTE:
ING. JEAN POLO CEQUEDA

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER
FACULTAD DE INGENIERÍAS
INGENIERÍA DE SISTEMAS
SAN JOSE DE CUCUTA
2013

1. MANUAL DE CONFIGURACION DE SNORT COMO NIDS

Primero vamos a empezar definiendo Snort, el cual es un sniffer de paquetes y un detector de intrusos basado en red (se monitoriza todo un dominio de colisión).

Es un software muy flexible que ofrece capacidades de almacenamiento de sus bitácoras tanto en archivos de texto como en bases de datos abiertas como lo es MySQL. Implementa un motor de detección de ataques y barrido de puertos que permite registrar, alertar y responder ante cualquier anomalía previamente definida.
Así mismo existen herramientas de terceros para mostrar informes en tiempo real (ACID) o para convertirlo en un Sistema Detector y Preventor de Intrusos.

Este IDS implementa un lenguaje de creación de reglas flexible, potente y sencillo. Durante su instalación ya nos provee de cientos de filtros o reglas para backdoor, DDoS, finger, FTP, ataques web, CGI, 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). Cuando un paquete coincide con algún patrón establecido en las reglas de configuración, se logea. Así se sabe cuándo, de dónde y cómo se produjo el ataque.

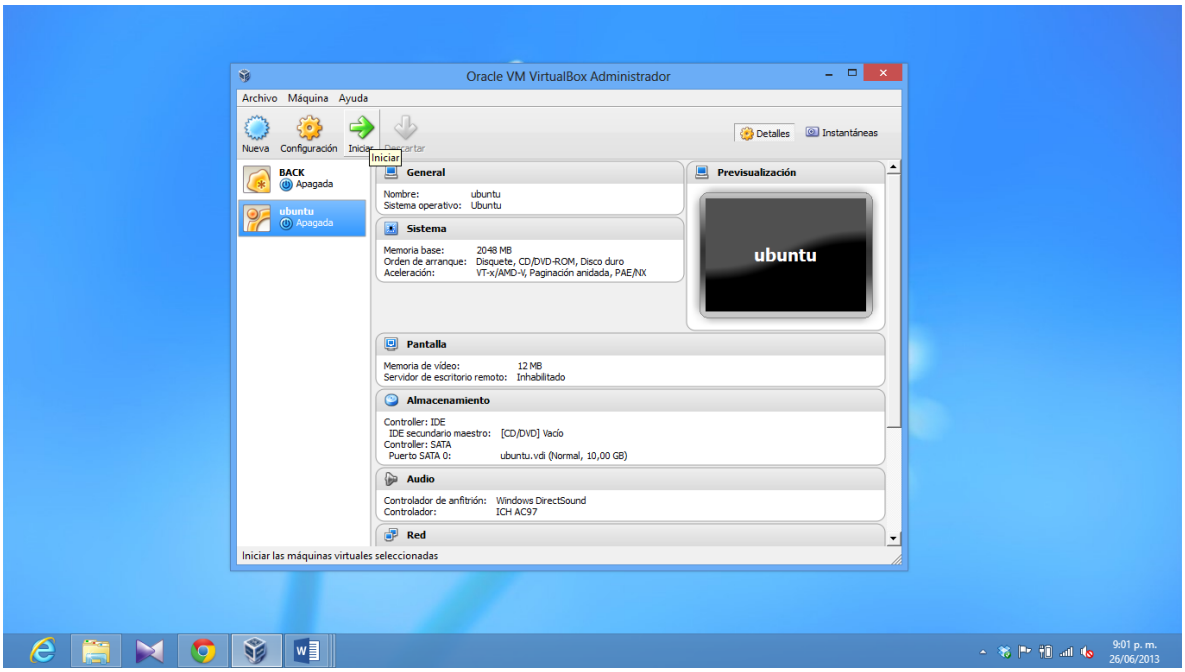
Aún cuando tcpdump es considerada una herramienta de auditoría muy útil, no se considera un verdadero IDS puesto que no analiza ni señala paquetes por anomalías. tcpdump imprime toda la información de paquetes a la salida en pantalla o a un archivo de registro sin ningún tipo de análisis. Un verdadero IDS analiza los paquetes, marca las transmisiones que sean potencialmente maliciosas y las almacena en un registro formateado, así, Snort utiliza la biblioteca estándar libcap y tcpdump como registro de paquetes en el fondo.

Snort está disponible bajo licencia GPL, gratuito y funciona bajo plataformas Windows y UNIX/Linux. 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.

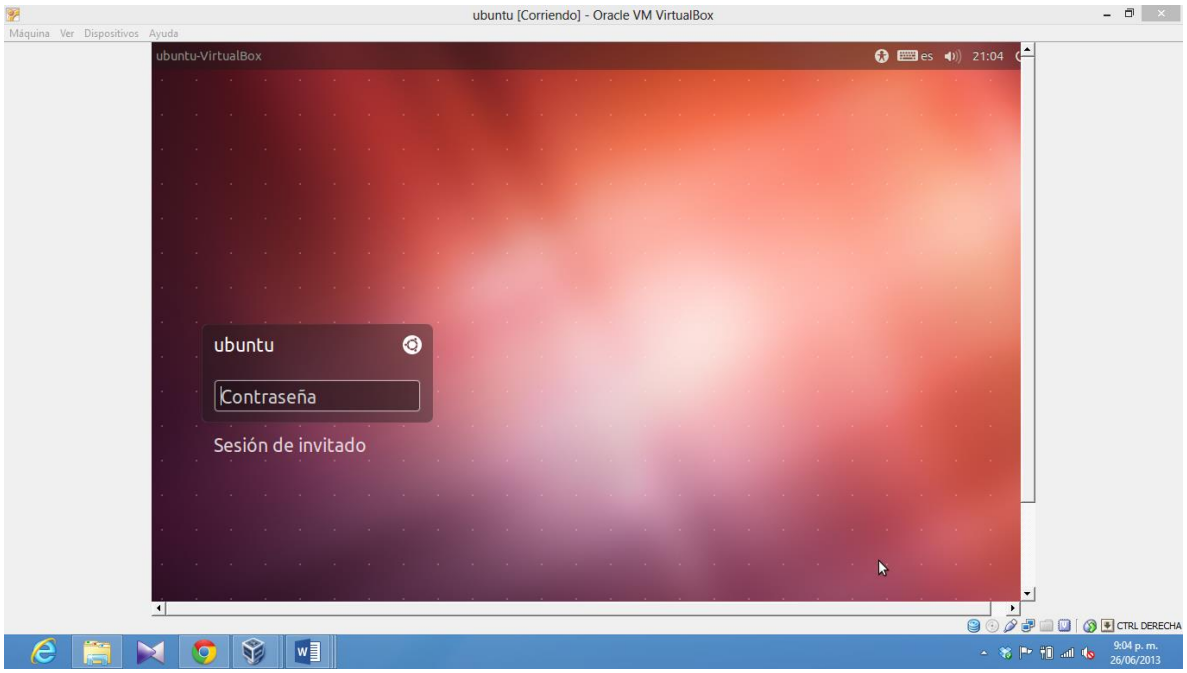
La característica más apreciada de Snort, además de su funcionalidad, es su subsistema flexible de firmas de ataques. Snort tiene una base de datos de ataques que se está actualizando constantemente y a la cual se puede añadir o actualizar a través de la Internet. Los usuarios pueden crear 'firmas' basadas en las características de los nuevos ataques de red y enviarlas a la lista de correo de firmas de Snort, para que así todos los usuarios de Snort se puedan beneficiar. Esta ética de comunidad y compartir ha convertido a Snort en uno de los IDSes basados en red más populares, actualizados y robustos.

El siguiente manual de instalación de Snort fue desarrollado en Ubuntu 12.04 como máquina virtual de la VirtualBox de Oracle. Con el fin de dar un mejor entendimiento se realizara la explicación por medio de una lista de pasos a seguir acompañados de imágenes.

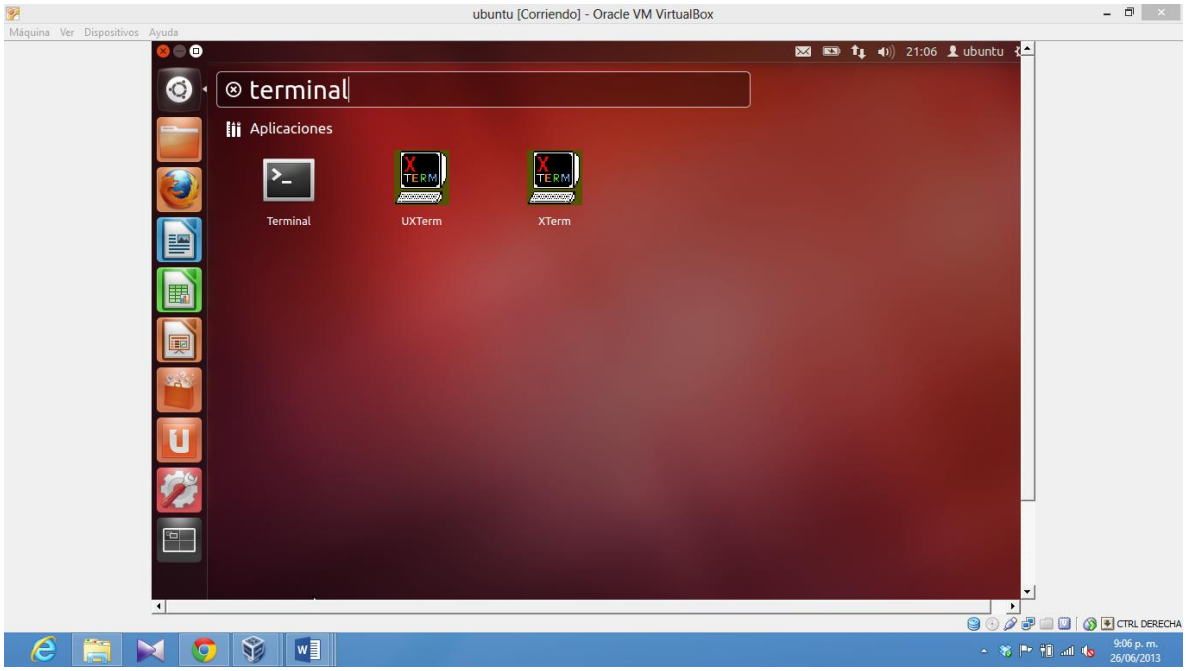
Paso 1. Iniciar la Máquina virtual de Ubuntu



Paso 2. Esperar a que termine de cargar y realizar el proceso de logeo de Ubuntu.



Paso 3. Ya en el escritorio de Ubuntu, ejecutar el menú de Inicio y buscar el terminal y proceder a abrirlo.

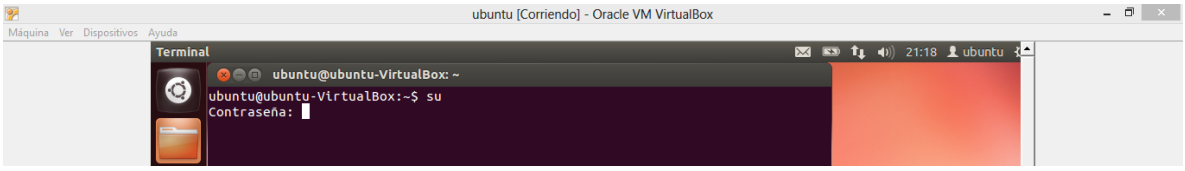


Paso 4. Ya abriendo el terminar debemos realizar el logeo para pasar al super administrador de Ubuntu para poder instalar los paquetes necesarios para el correcto funcionamiento de Snort

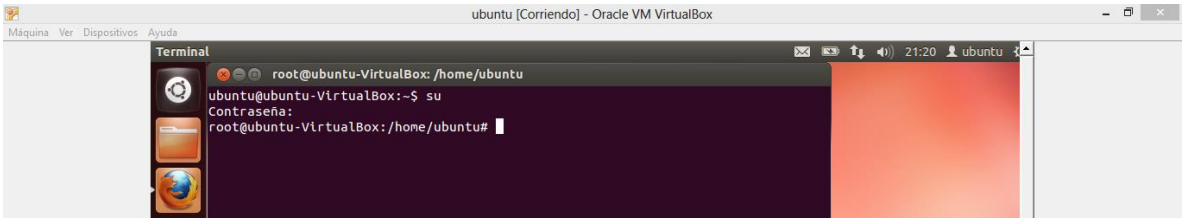
Escribiendo en el terminal su para que solicite la clave del super administrador, en nuestro caso personal aun no habíamos configurado una clave del super administrador, y para poder cambiar por la clave normal de acceso el mismo terminal se escribe el comando:

sudo passwd root

Seguido de esto el terminal solicita que digite la clave del usuario y que por favor la vuelva a escribir. Después de tener la constraseña volver a intentar con su y logearse como super administrador.

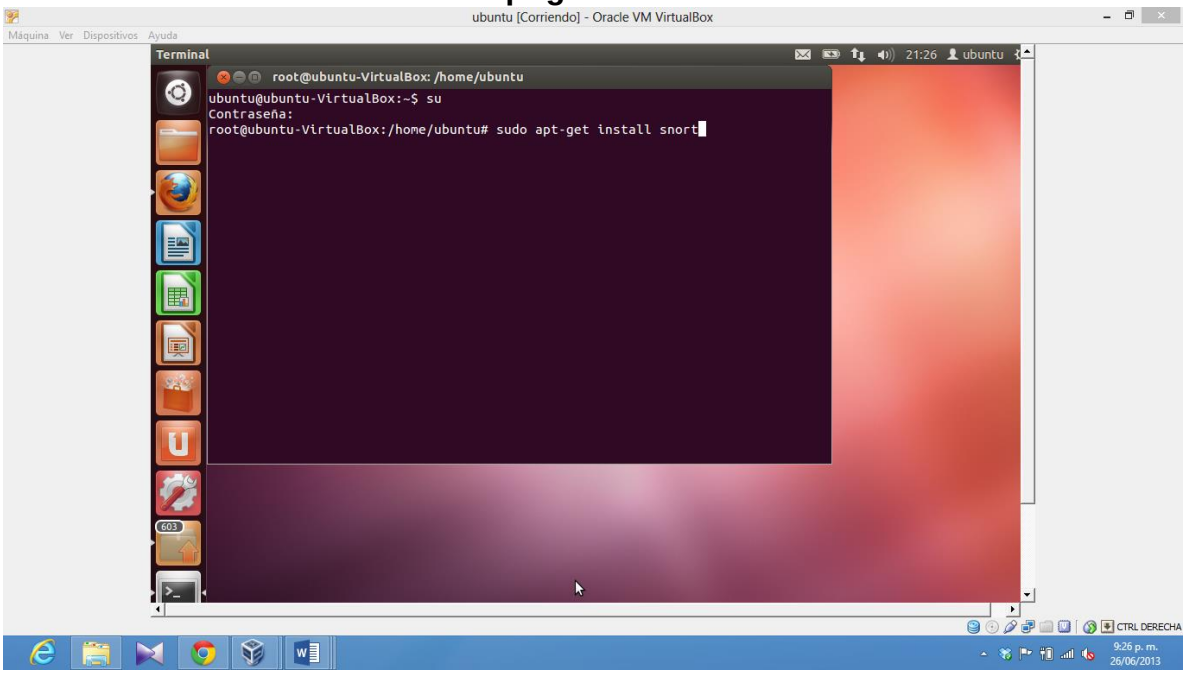


Pasando de modo usuario a modo super adinistrador.

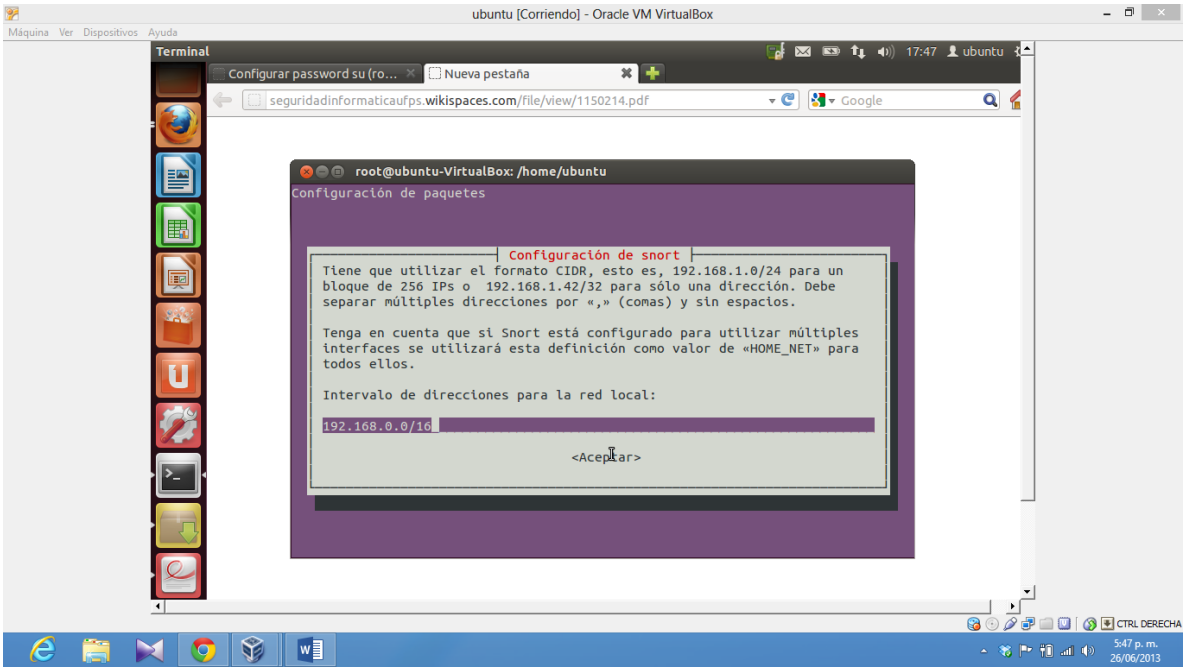


Paso 5. Ya estando en el modo super administrador procedemos a escribir el comando para instalar el snort.

sudo apt-get install snort

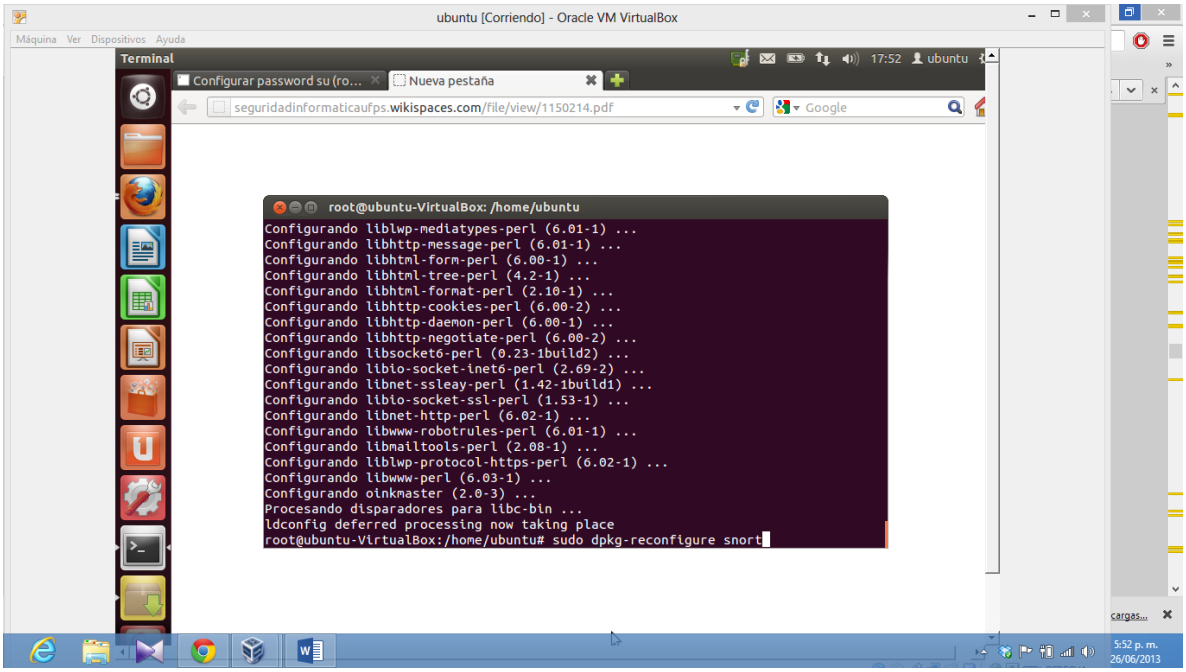


Paso 6. Después de aceptar la instalación de los paquetes snort solicita que por favor se configure la ip del computador. En este caso se dejara la que por defecto sale puesto que mas adelante se enseñara a cambiarla si ud cambia de red.

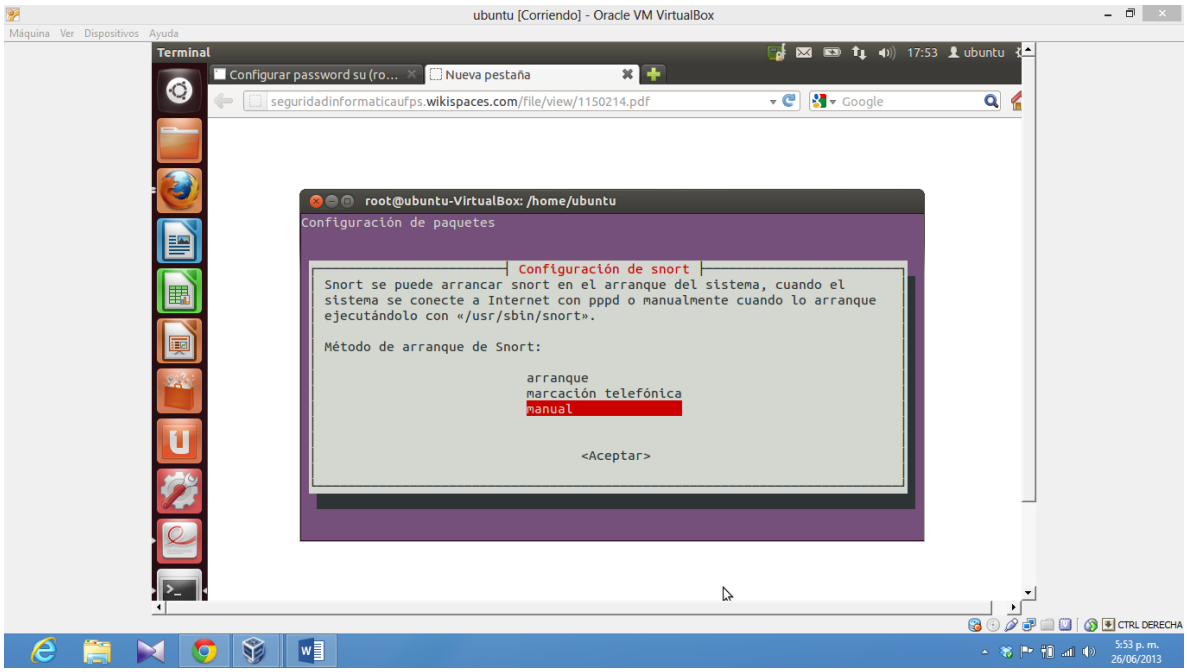


Si usted no conoce la ip que tiene asignada por favor digite en otro terminal el comando **ifconfig** y revise la ip que tiene asignada en inet.

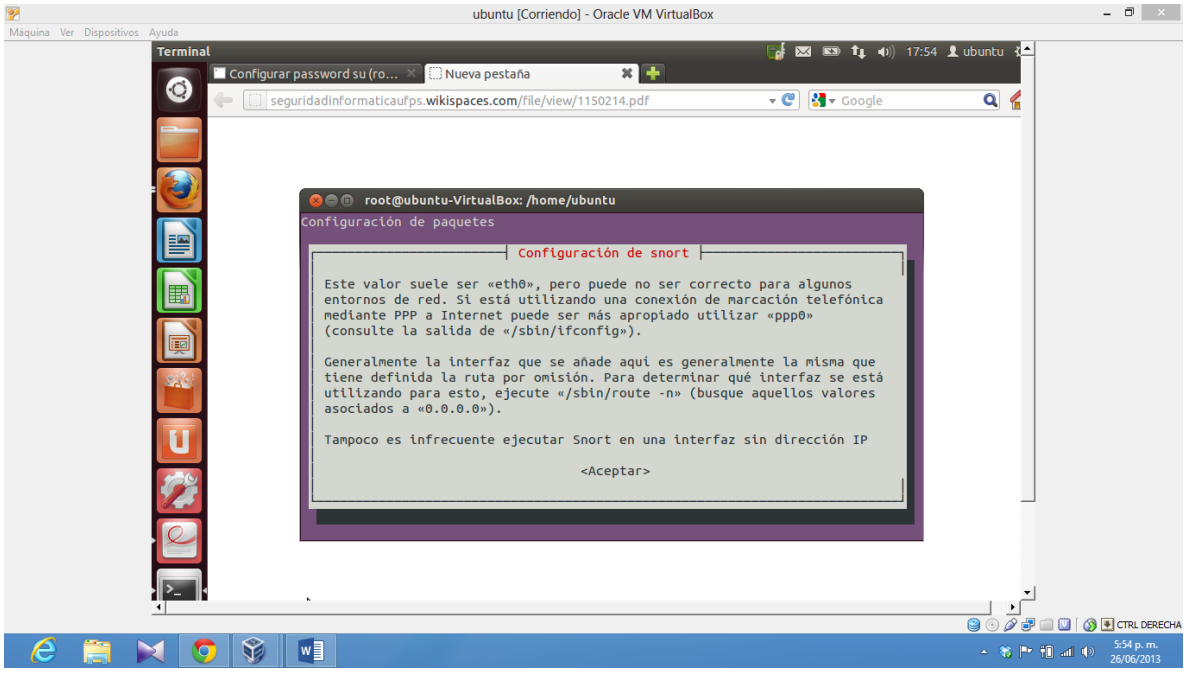
Paso 7. Esperar el proceso normal de la instalación y configuración.



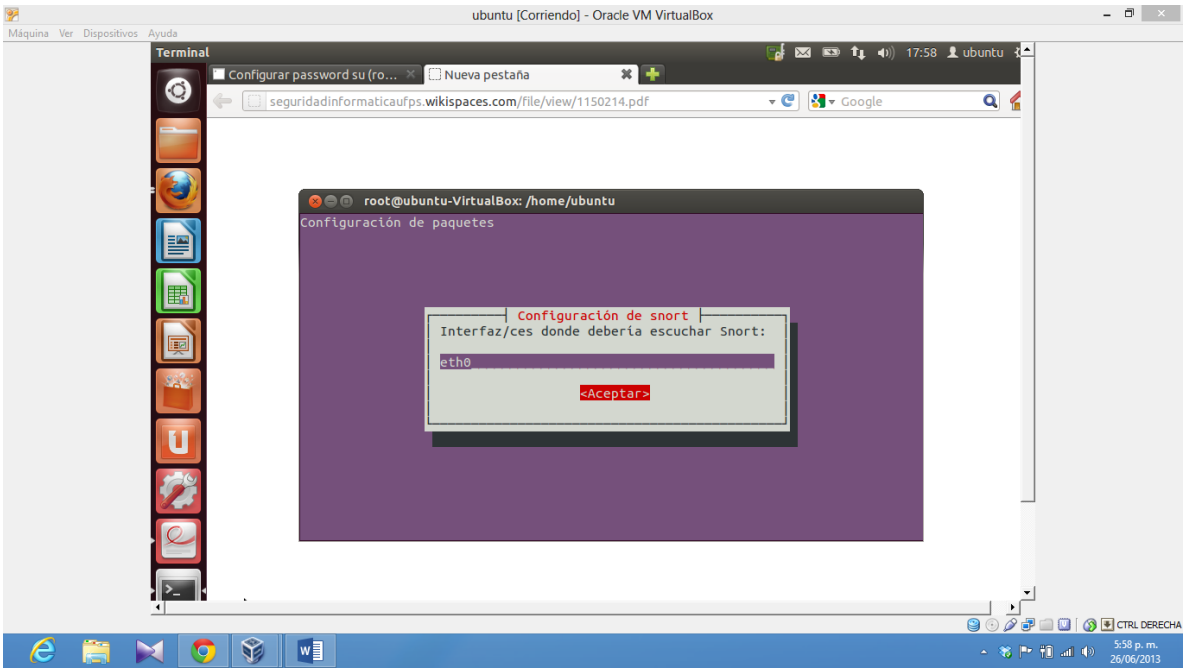
Paso 8. La instalación pedirá escoger como desea configurar snort a la cual escogeremos manual para realizar nuestras configuraciones respectivas.



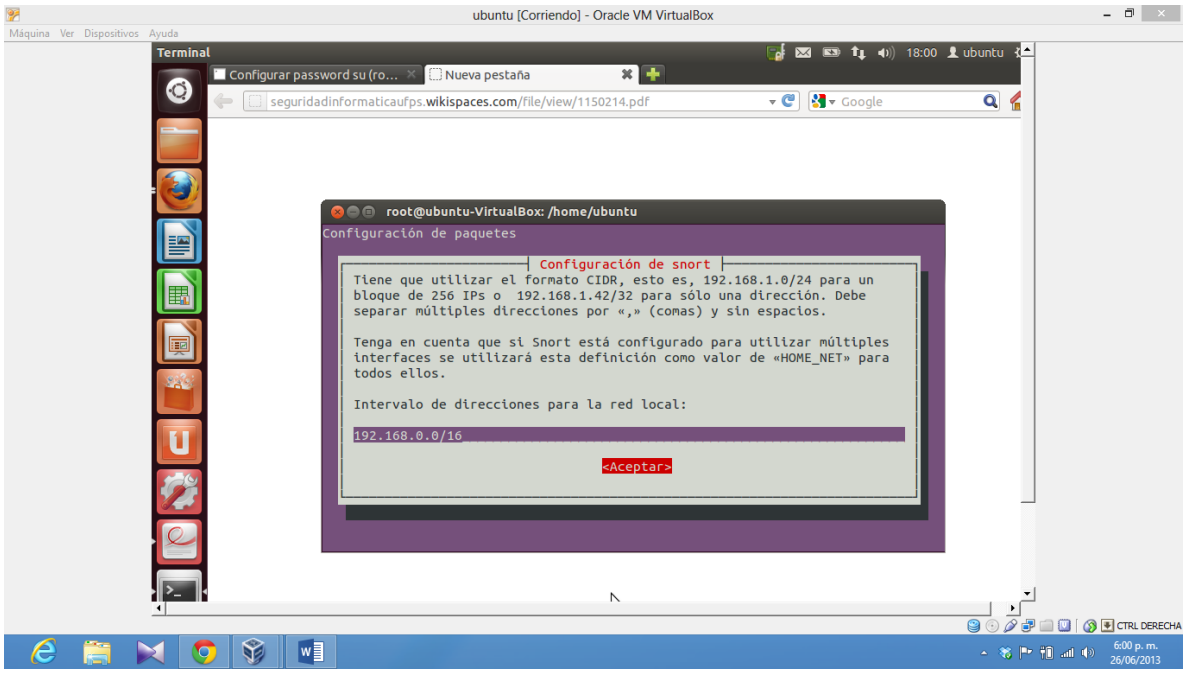
Paso 9. Seguido de esto solicita al usuario la aprobación de la configuración manual y da a conocer los datos que solicitara para dicha configuración, al cual daremos **Aceptar**.



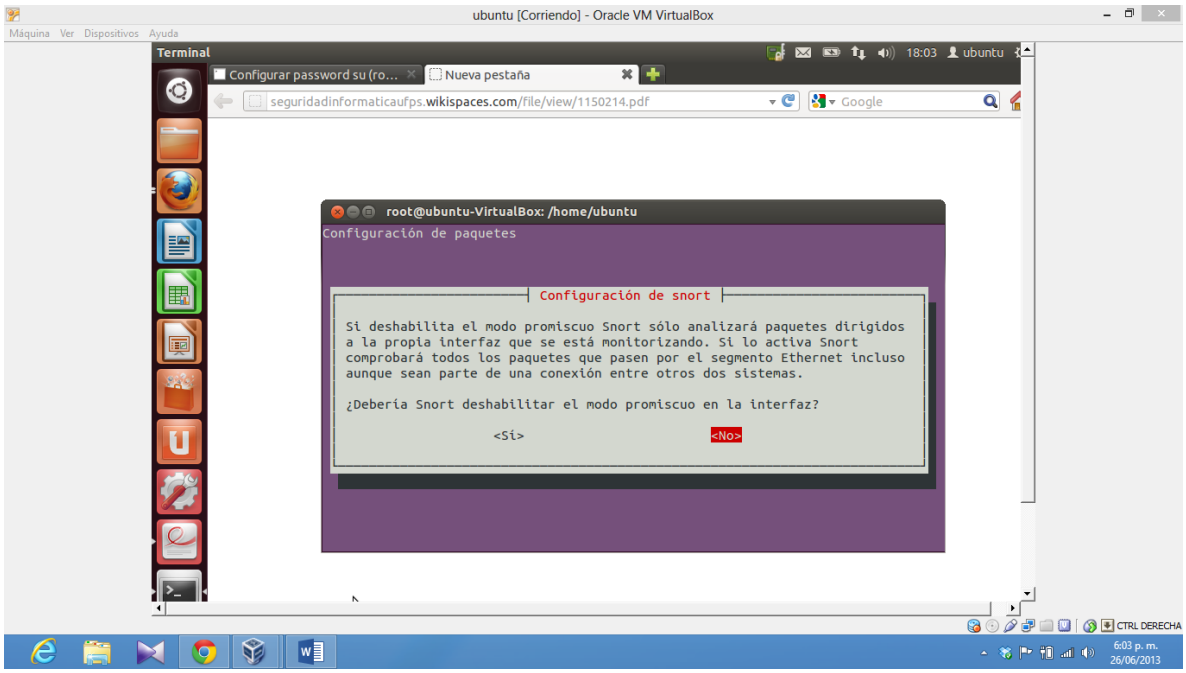
Paso 10. Solicitará al usuario el tipo de interfaz de conexión a internet, para el caso de que este Ubuntu es virtualizado el puerto por defecto es **eth0**, pero se debe escoger el puerto que usted este utilizando si es por red inalámbrica seria **wlan0** el puerto por defecto.



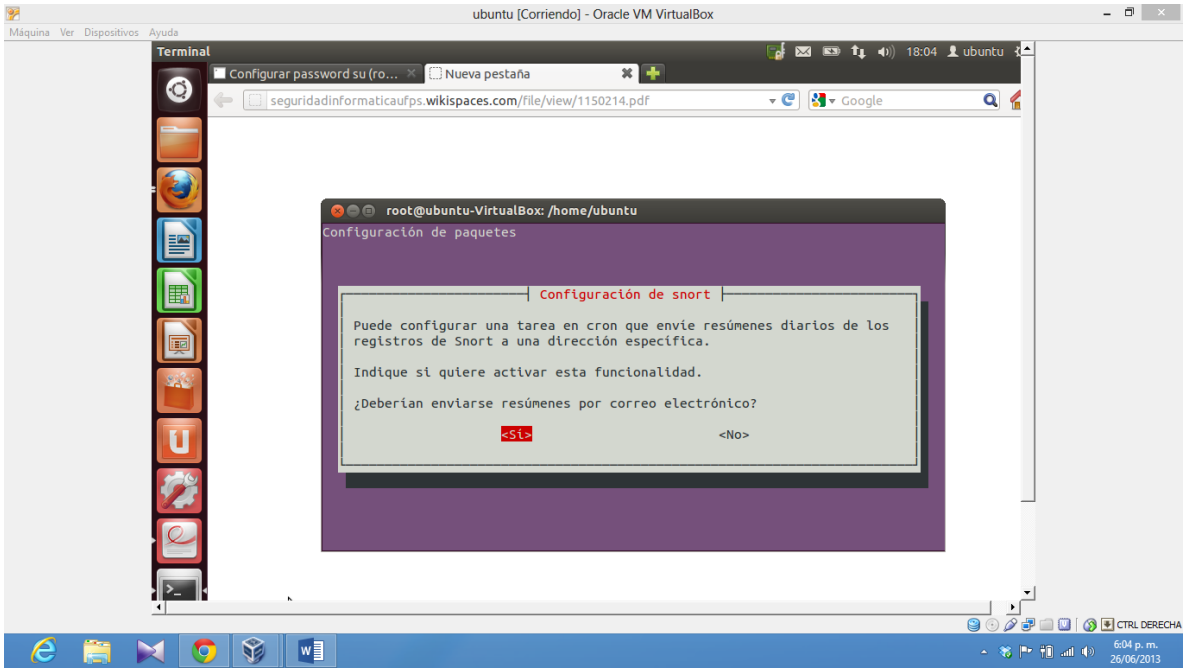
Paso 11. Solicita al usuario configurar el intervalo de direcciones para la red local, en este caso se dejo el valor por defecto y se da enter



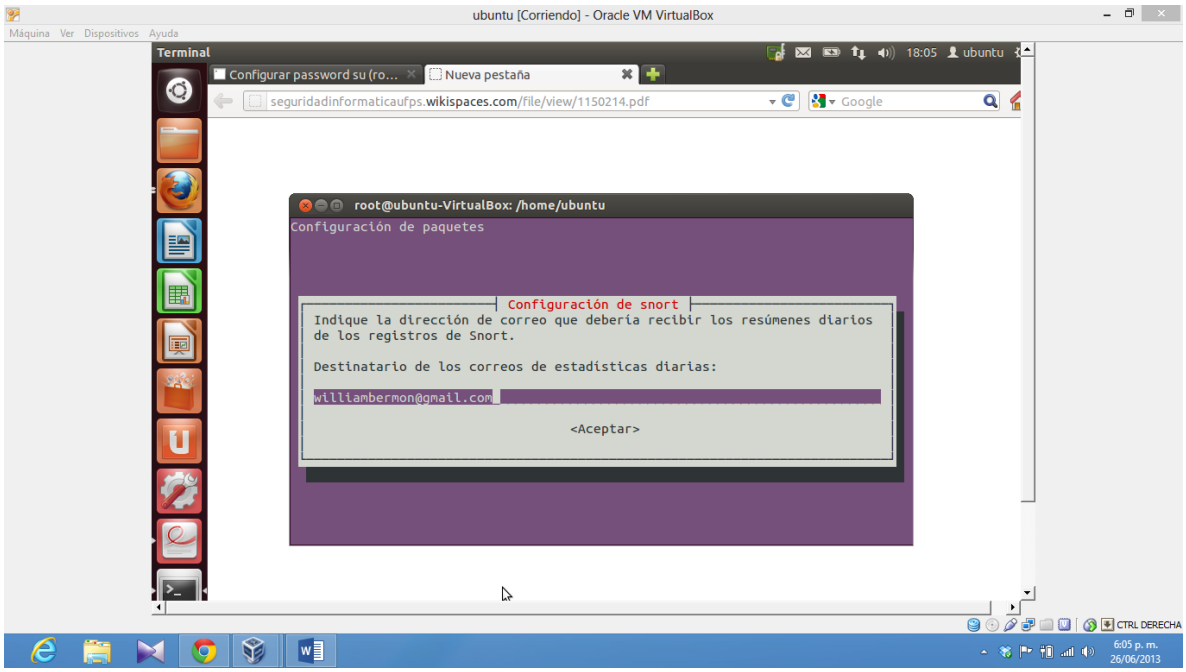
Paso 12. El snort pregunta si se desea activar el modo promiscuo, al cual diremos que no, puesto que de esta forma el snort solo analiza los paquetes que están dirigidos a la misma interfaz y no todo el tráfico de la red.



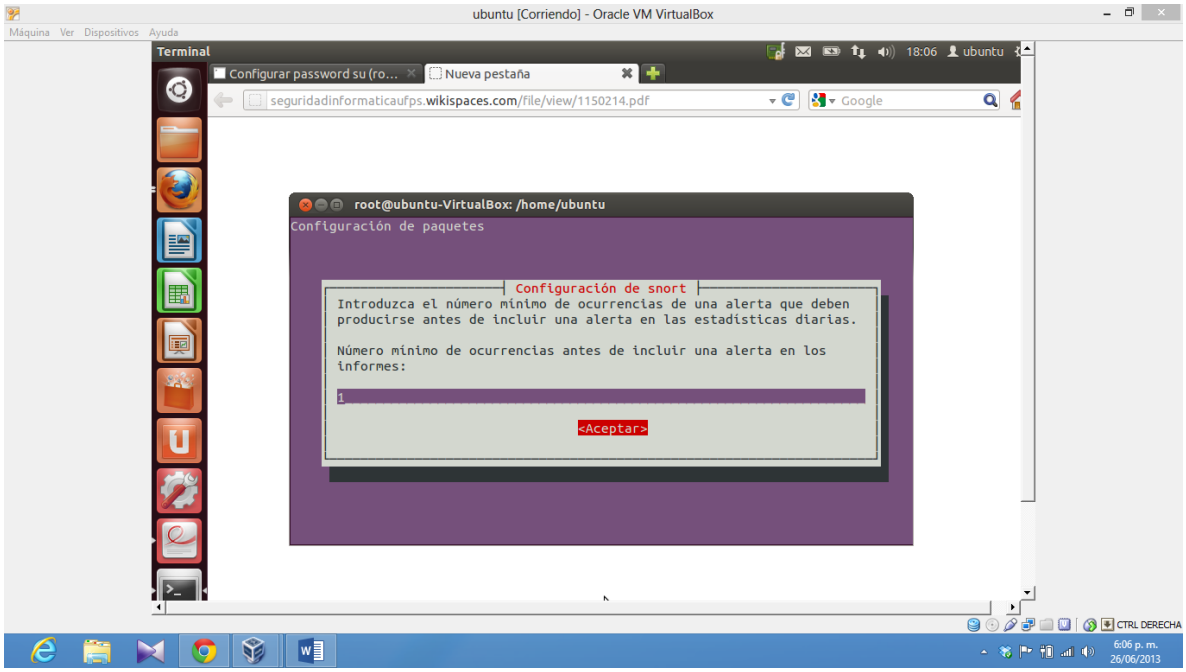
Paso 13. El instalador solicita al usuario si desea recibir resúmenes por correo electrónico con los registros de snort, cabe tener en cuenta que de habilitar dicha configuración para que funciones debe tener configurado en el servidor de SMTP.



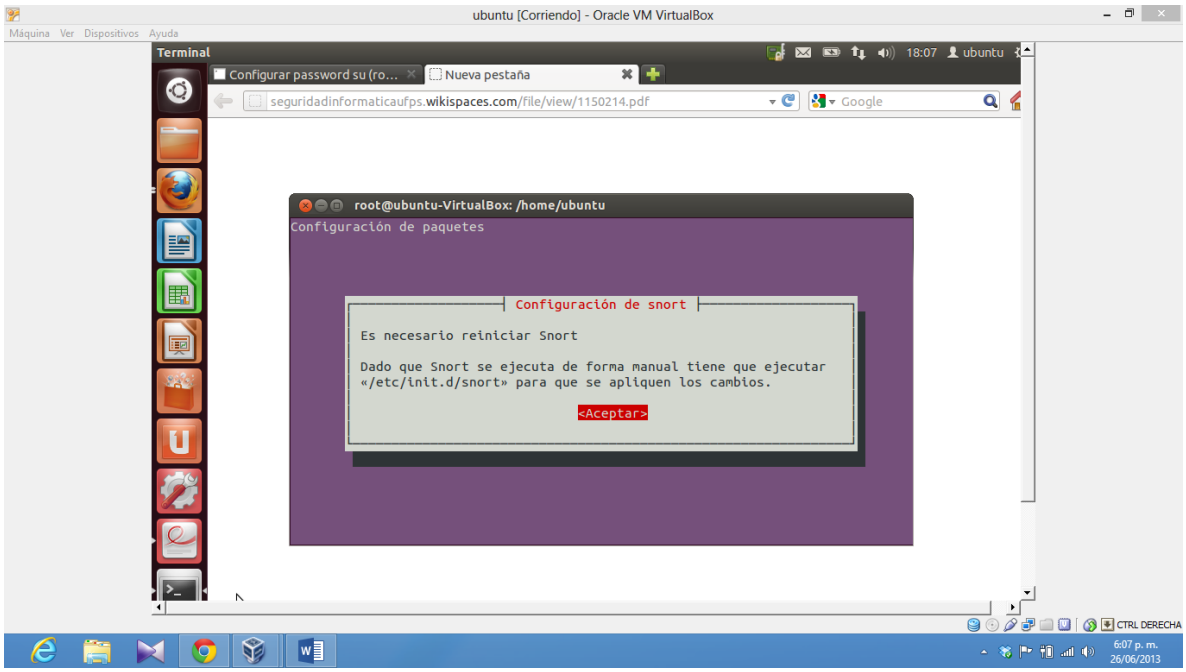
Paso 14. Como en el anterior dimos que **SI,** solicitara la cuenta de correo a donde desea enviar el resumen.



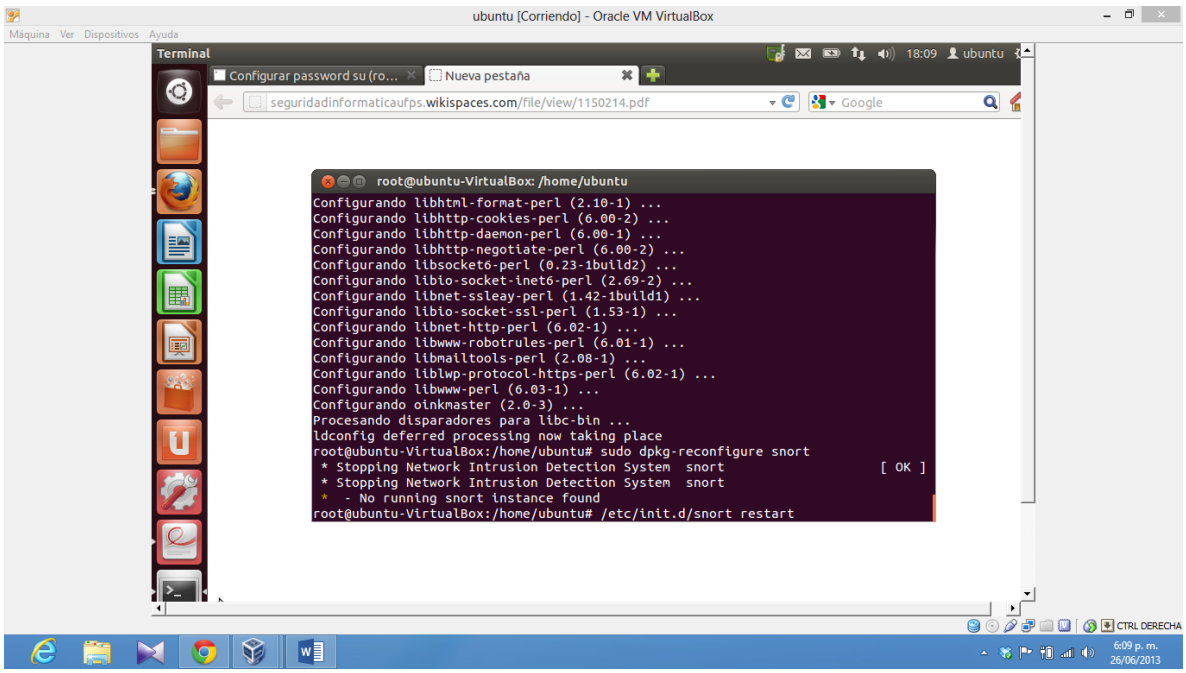
Paso 15. Para este caso solicita al usuario que configure la cantidad de ocurrencias para poder enviar un correo con el resumen.



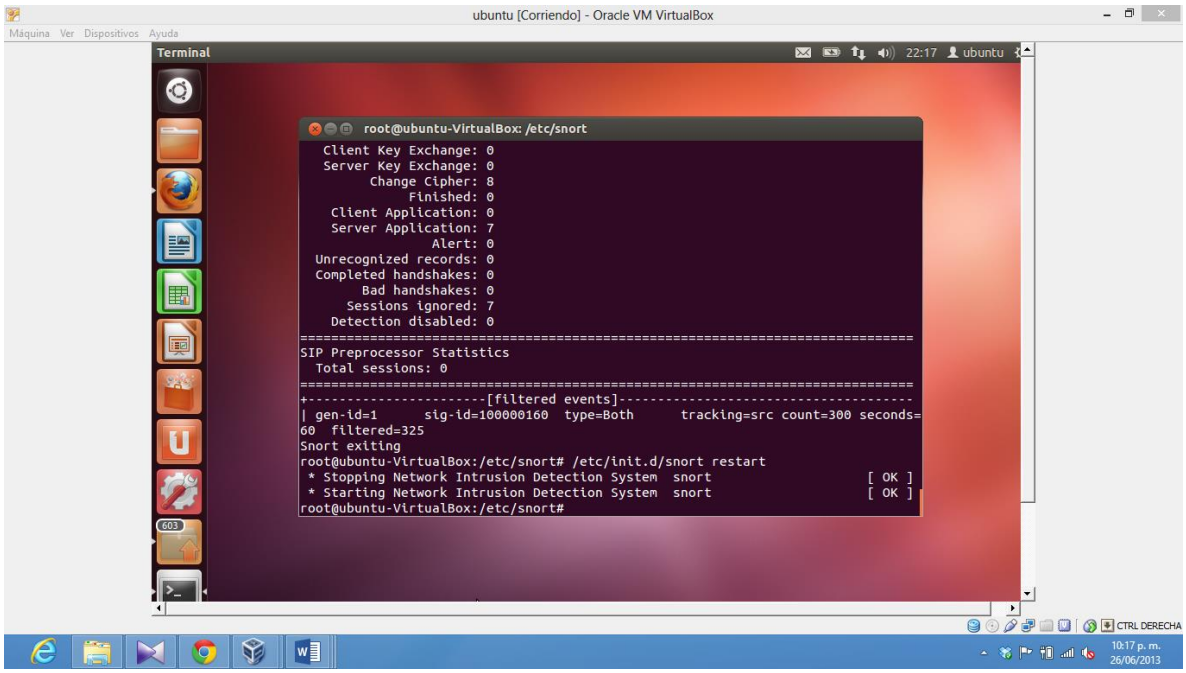
Paso 16. La instalación ha terminad con éxito, pero para poder utilizar el servicio de debe reiniciar el servicio de snort.



Paso 17. Reiniciar el servicio snort de comando **/etc/init.d/snort restart**

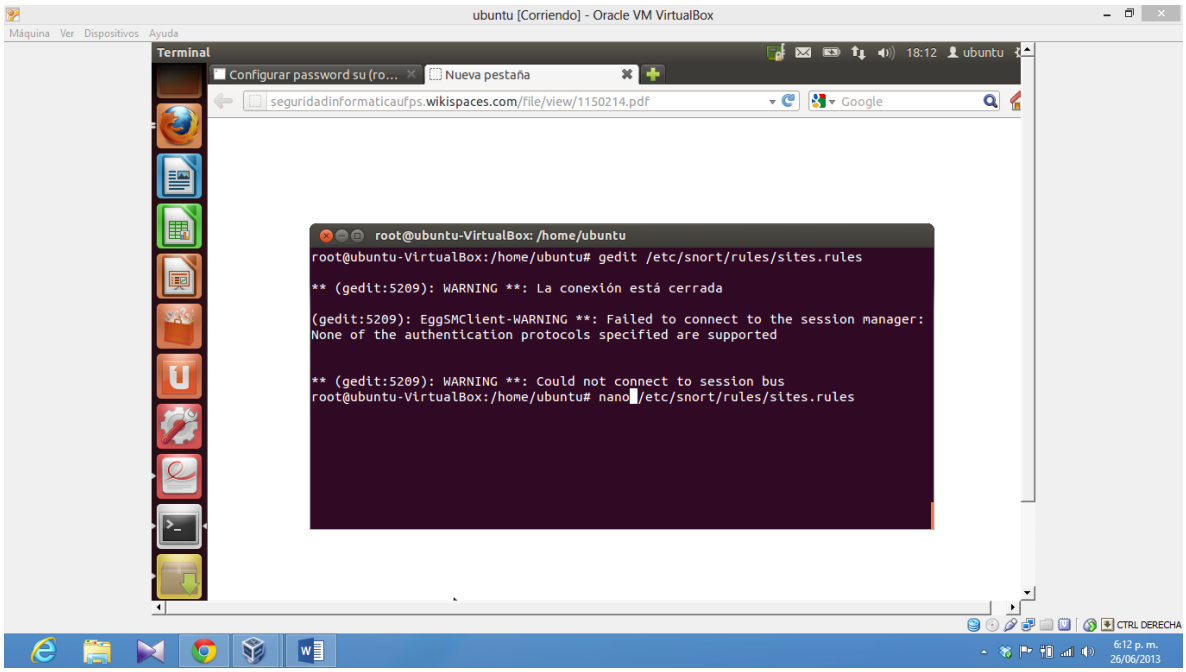


Paso 18. Si el servicio quedo correctamente instalado deberá decir que todo quedo **OK,** de la siguiente forma.



Paso 19. Ahora procederemos a configurar al reglas de revisión del **snort,** en este caso crearemos el siguiente archivo en la ubicación de instalación del snort, para este caso fue la siguiente ubicación:

/etc/snort/rules/sites.rules



Recordemos que se puede crear con editor de texto gedit o si no lo tiene instalado como nos sucedió utilizar el nano.

Paso 20. En el archivo creado se escribirán las reglas de la siguiente manera.

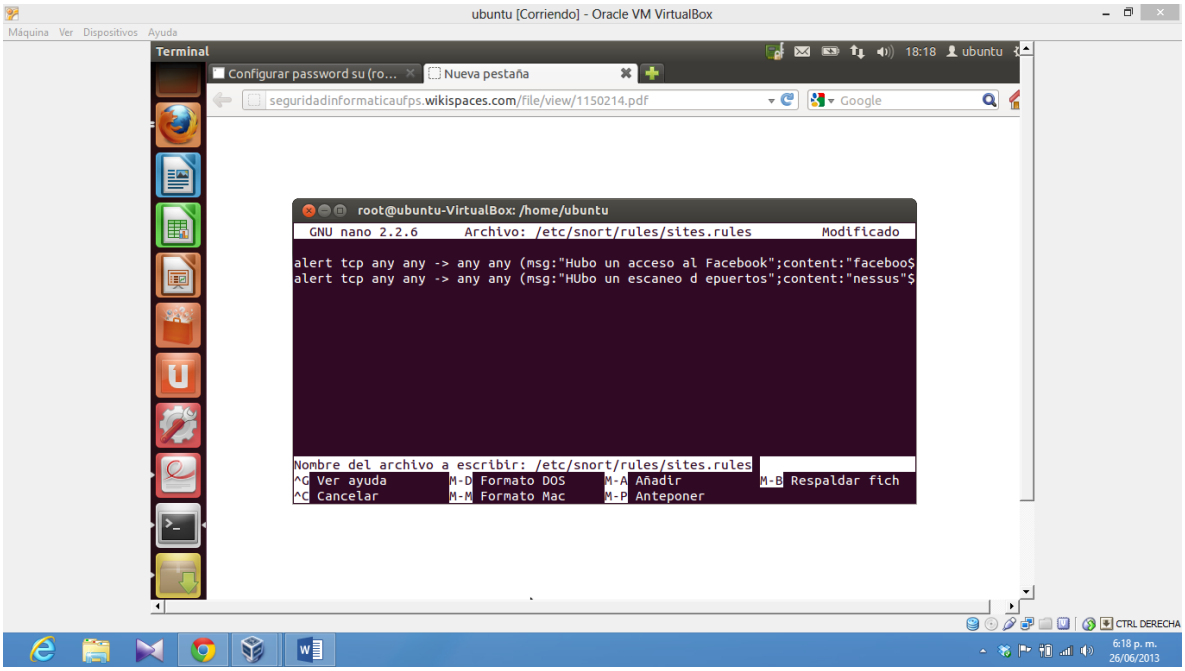
```
+----------------+-----------------+
|  RULE HEADER   |   RULE OPTIONS  |
+----------------+-----------------+
```

Y el RULE HEADER tiene una forma similar a:

```
+--------+----------+---------+------+-----------+---------+------+
| ACTION | PROTOCOL | ADDRESS | PORT | DIRECTION | ADDRESS | PORT |
+--------+----------+---------+------+-----------+---------+------+
```

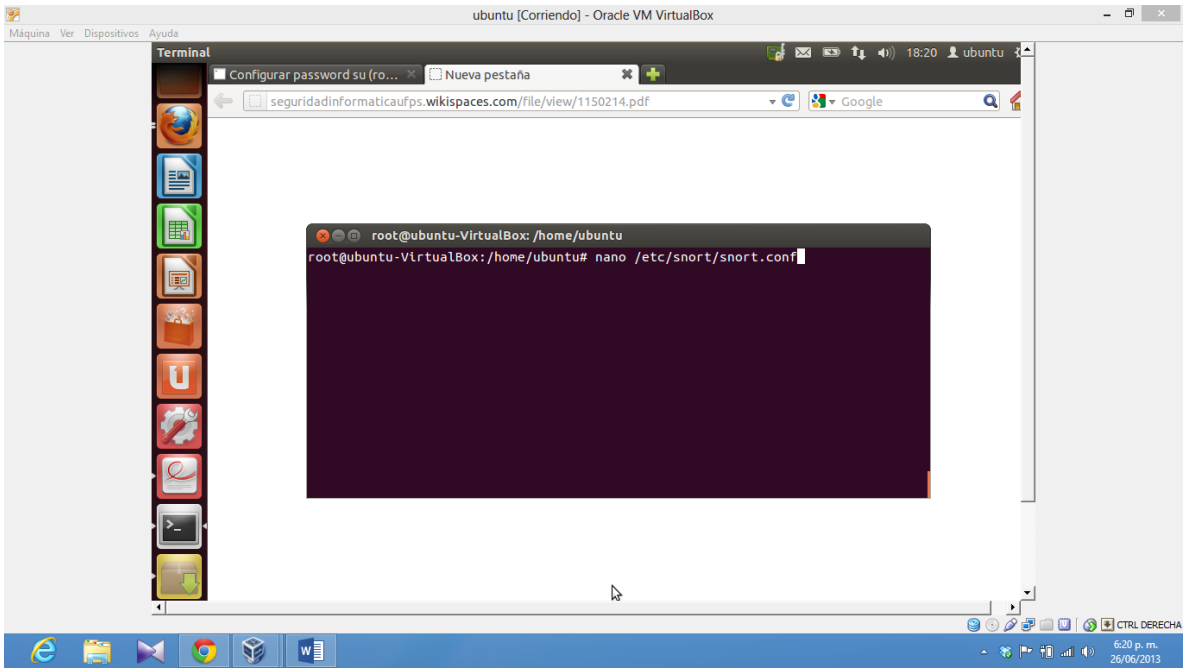
Quedando de la siguiente manera.

alert tcp any any -> any any (msg = “Hubo un acceso al Facebbok”; content:“facebook”; sid:19910314;rev:1;)



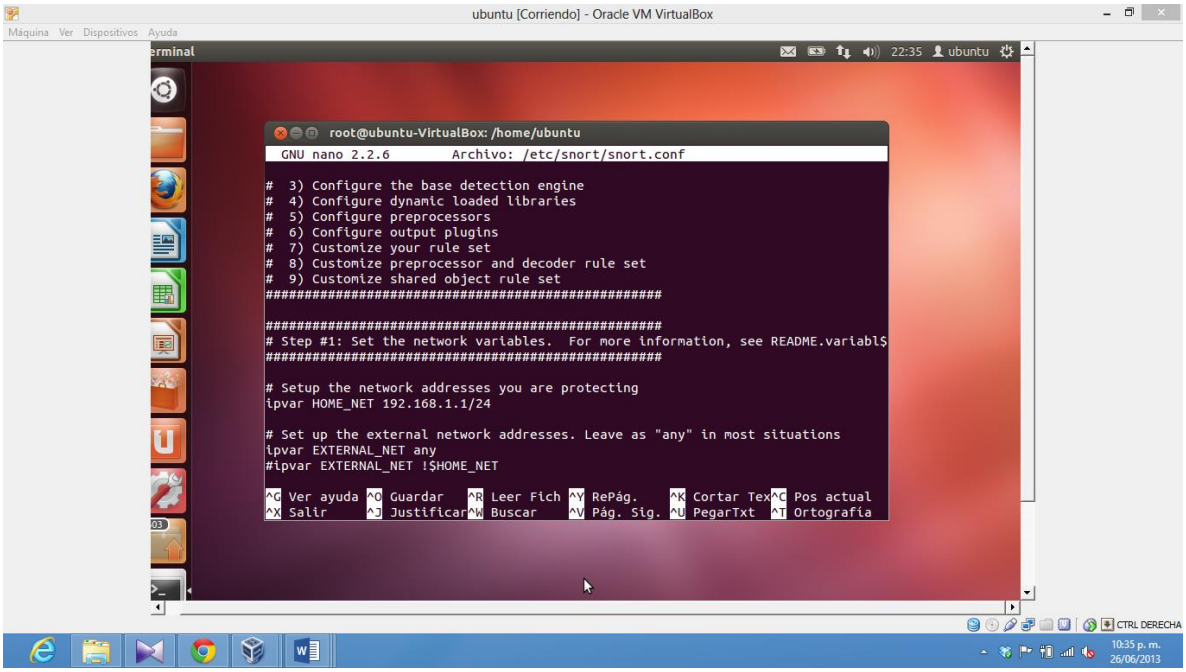
Paso 21. Despues de guardar el documento se procede a configurar dicho archivo para que trabaje de reglas del snort, para eso debemos abrir **snort.conf**el archivo ubicado en la dirección:

/etc/snort/snort.conf



Paso 22. Ya dentro este archivo el paso 1 o **Step#1,** en la parte donde dice **ipvar HOME_NET** se debe escribir que este computador tiene asignada separada por puntos y seguida de un **/** y el puerto. Quedando de la siguiente forma:

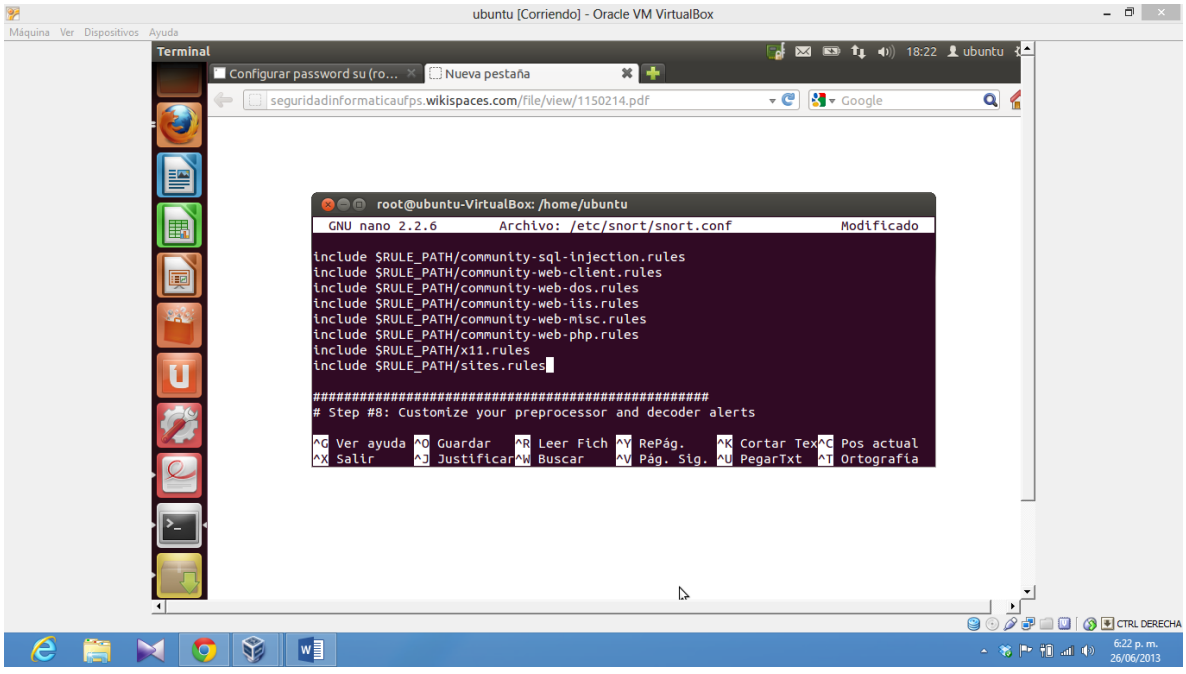
Ipvar HOME_NET 192.168.1.1/24



Si no se conoce la ip asignada para este computador se debe escribir en un terminal el comando **ifconfig,** y se identifica con el nombre de **inet.**

Paso 23. En el paso 8 o **step#7** se debe agregar la línea con la ubicación de la reglas creadas anteriormente, pata este caso se escribe

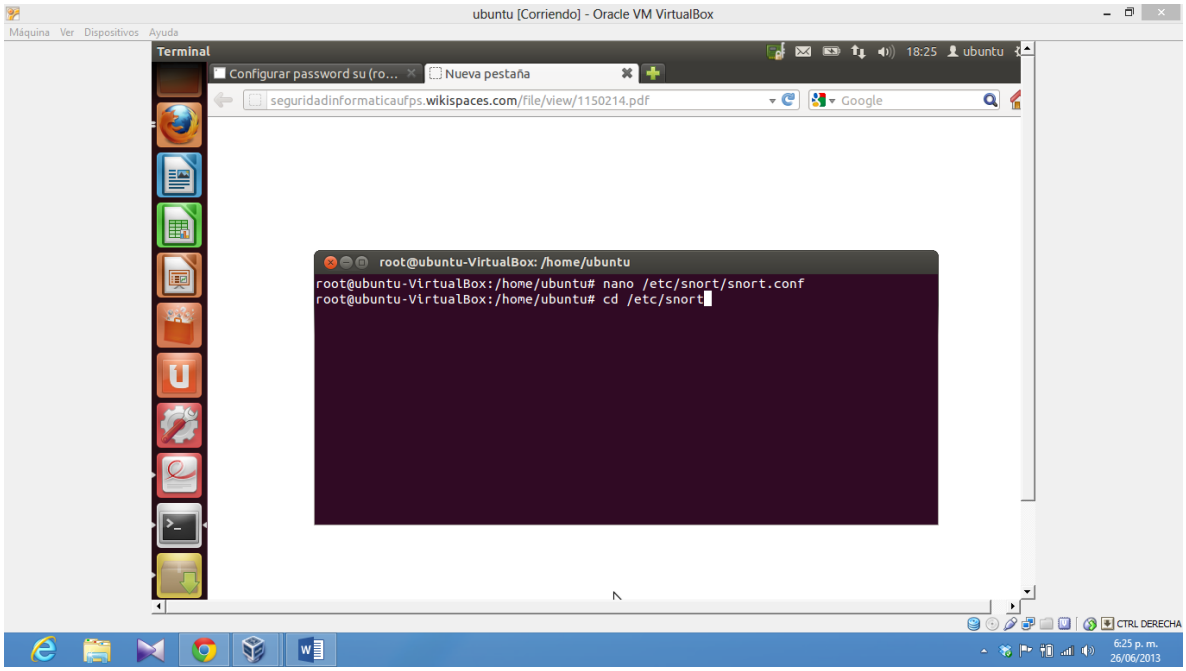
include $RULE_PATH/sites.rules



Paso 24. Se procede a guardar los cambios y a reiniciar el servicio nuevamente (Ver Paso 17).

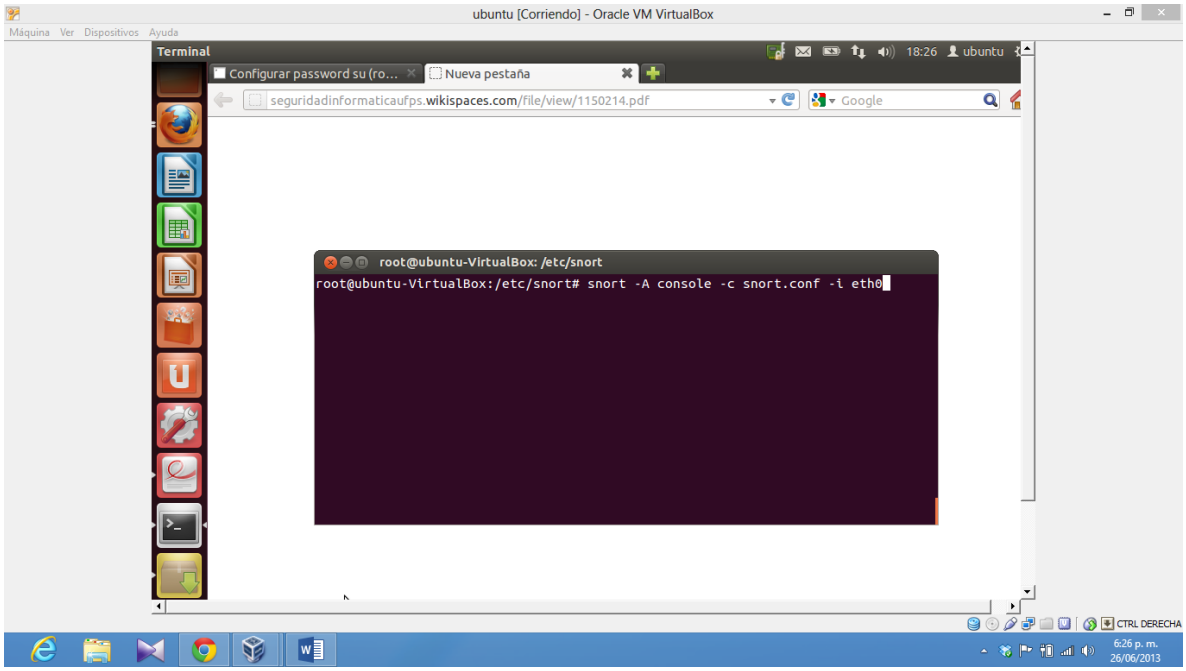
Paso 25. Para verificar que el **snort,** está funcionando correctamente debemos entrar a la ubicación del snort con el siguiente comando:

cd /etc/snort



Paso 26. Escribir el siguiente comando para ejecutar el snort y estar a la espera de intrusos:

Snort –A console –c snort.conf –i eth0

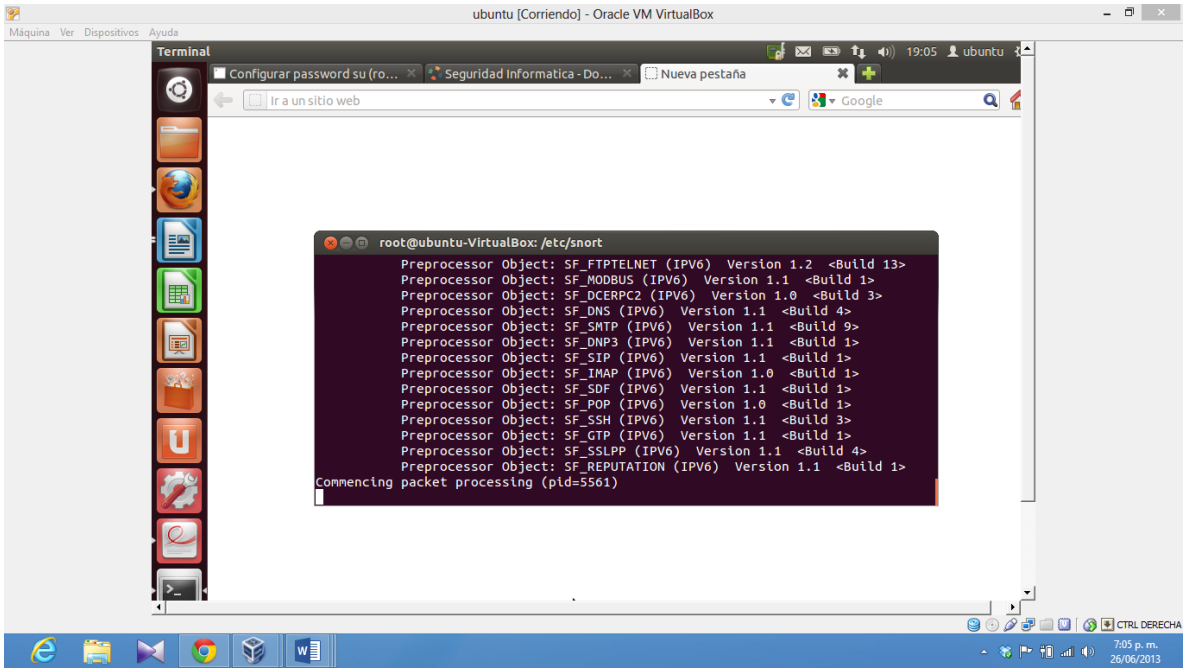


Teniendo en cuenta que los comando utilizados para este IDS.

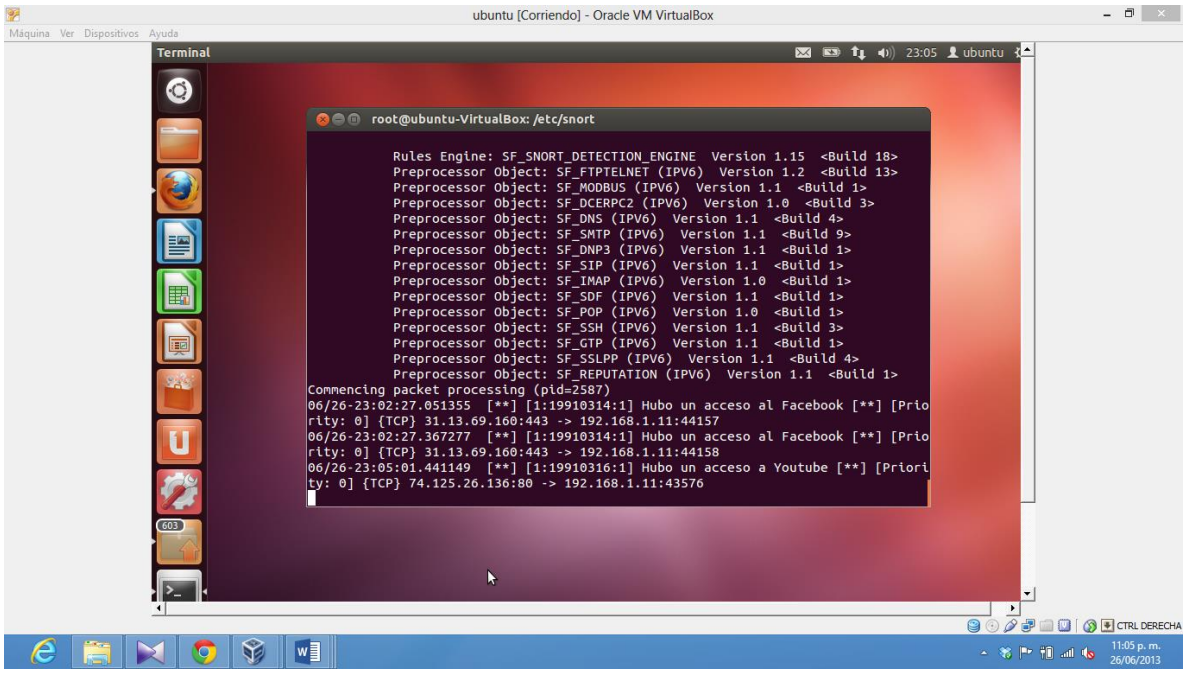
Options:

-A Set alert mode: fast, full, console, or none (alert file alerts only)
-b Log packets in tcpdump format (much faster!)
-c <rules> Use Rules File <rules>
-C Print out payloads with character data only (no hex)
-d Dump the Application Layer
-e Display the second layer header info
-E Log alert messages to NT Eventlog. (Win32 only)
-f Turn off fflush() calls after binary log writes
-F <bpf> Read BPF filters from file <bpf>
-h <hn> Home network = <hn>
-i <if> Listen on interface <if>
-I Add Interface name to alert output
-k <mode> Checksum mode (all,noip,notcp,noudp,noicmp,none)
-l <ld> Log to directory <ld>
-L <file> Log to this tcpdump file
-n <cnt> Exit after receiving <cnt> packets
-N Turn off logging (alerts still work)
-o Change the rule testing order to Pass|Alert|Log
-O Obfuscate the logged IP addresses
-p Disable promiscuous mode sniffing
-P <snap> Set explicit snaplen of packet (default: 1514)
-q Quiet. Don't show banner and status report
-r <tf> Read and process tcpdump file <tf>
-R <id> Include 'id' in snort_intf<id>.pid file name
-s Log alert messages to syslog
-S <n=v> Set rules file variable n equal to value v
-T Test and report on the current Snort configuration
-U Use UTC for timestamps
-v Be verbose
-V Show version number
-W Lists available interfaces. (Win32 only)
-w Dump 802.11 management and control frames
-X Dump the raw packet data starting at the link layer
-y Include year in timestamp in the alert and log files
-z Set assurance mode, match on established sesions (for TCP)
-? Show this information

Paso 27. En este momento se ve que el **snort** queda a la espera de intrusos.



Paso 28. Si intentamos un acceso a Facebook o a Youtube nos va a mostrar de los siguientes resultados.



2. INSTALACIÓN DE UN HONEYPOT

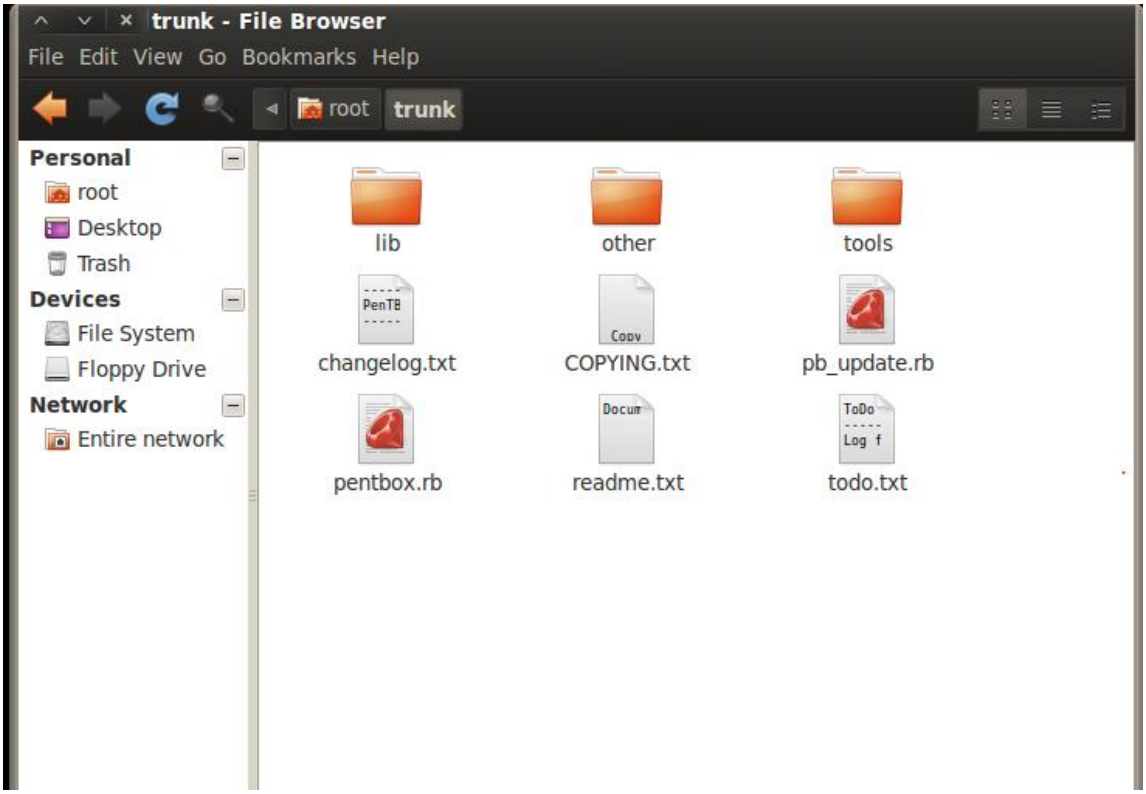
Para la instalación del honeypot se hizo uso de Backtrack 5 y de PentBox.

PenTBox es una suite de seguridad, paquetes de seguridad y la estabilidad de las herramientas de prueba orientada a las redes y sistemas. Está Programado en Ruby y orientado a GNU / Linux, aunque es compatible con Windows, MacOS y sistemas en los que cada Rubí trabaja. Está libre, licenciado bajo GNU / GPLv3.

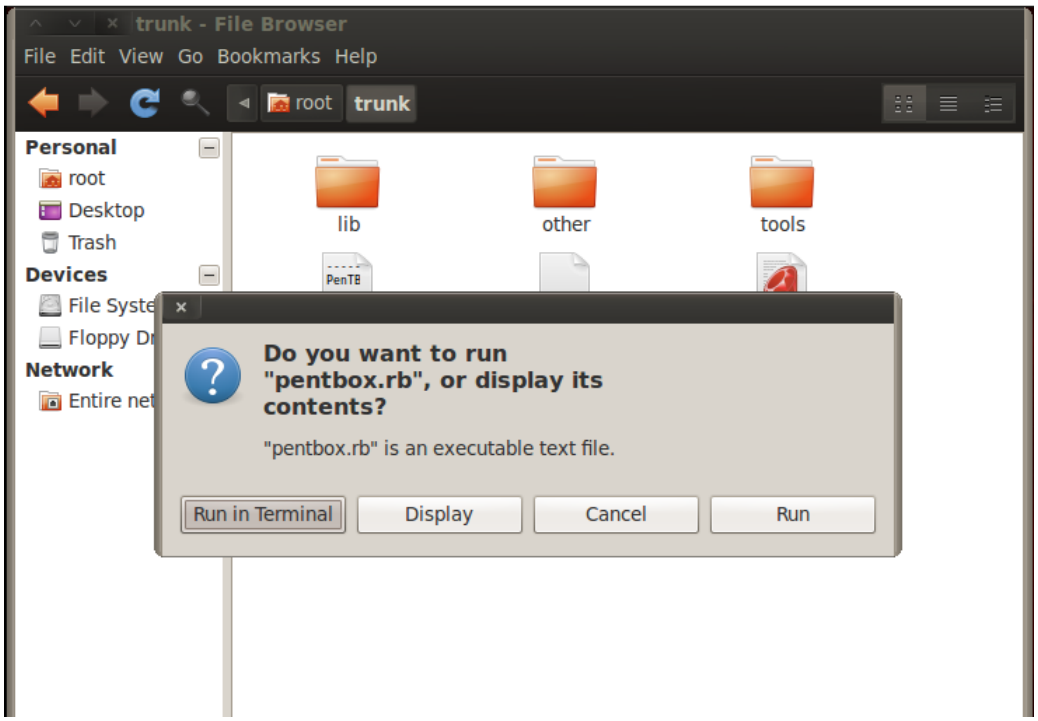
Paso 1. Descargar PenTBox de la siguiente manera:



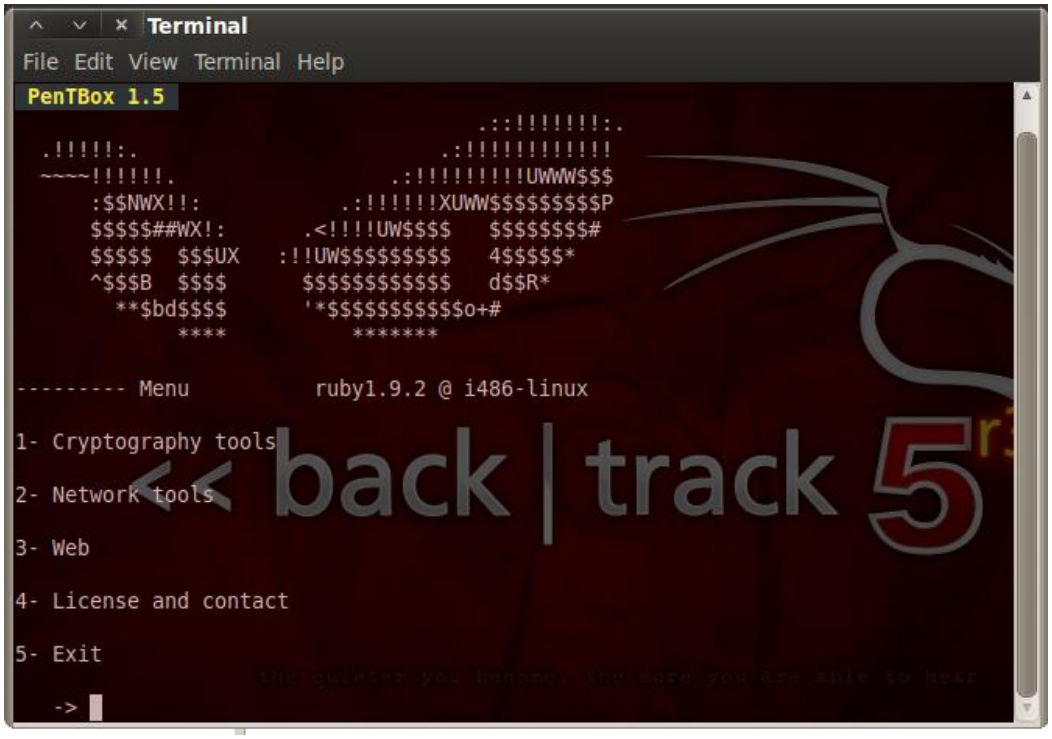
Paso 2. Ahora abrimos el navegador de archivos y buscamos la carpeta donde lo descargamos.



Paso 3. Ejecutamos el archivo **pentbox.rb** en un Terminal:



Paso 4. Aparecerá una interfaz en la consola como se ve a continuación:



Paso 5. Escogemos Network Tools (Herramientas de Red) presionando 2 y pulsando Enter.



Paso 6. Ahora seleccionamos la opción **Honeypot** presionando 3 y pulsando Enter.



Paso 7. Ahora seleccione la segunda opción (Configuración manual) pulsando 2 y Enter. Le solicitará el número de puerto a abrir, introducimos el 80.



Paso 8. Ahora nos solicitará introducir un mensaje falso que aparecerá cuando alguien intente acceder al host a través del puerto 80.



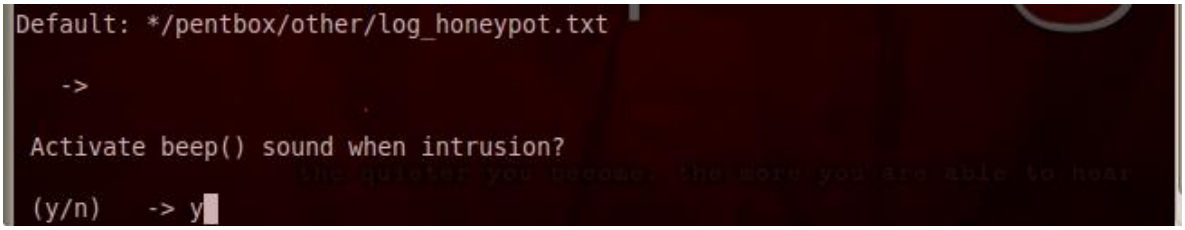
Paso 9. Ahora nos preguntará si deseamos llevar un registro (log) de los intrusos que intentaron acceder.



Paso 10. Ahora podremos introducir un nombre para el archivo de registro o bien presionar enter para dejar el nombre por defecto (log_honeypot.txt)

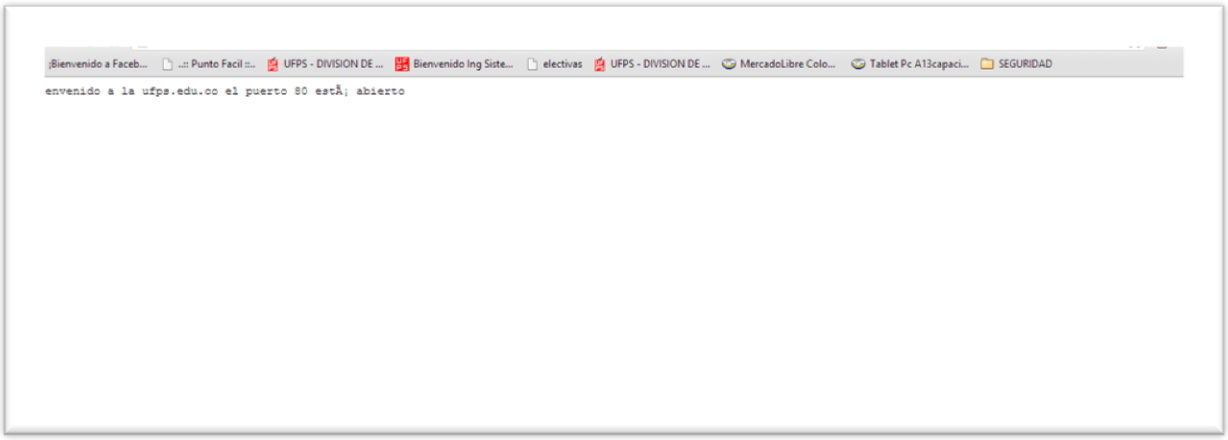


Paso 11. Nos preguntará si deseamos que se reproduzca un sonido cada vez que se detecte un intruso.

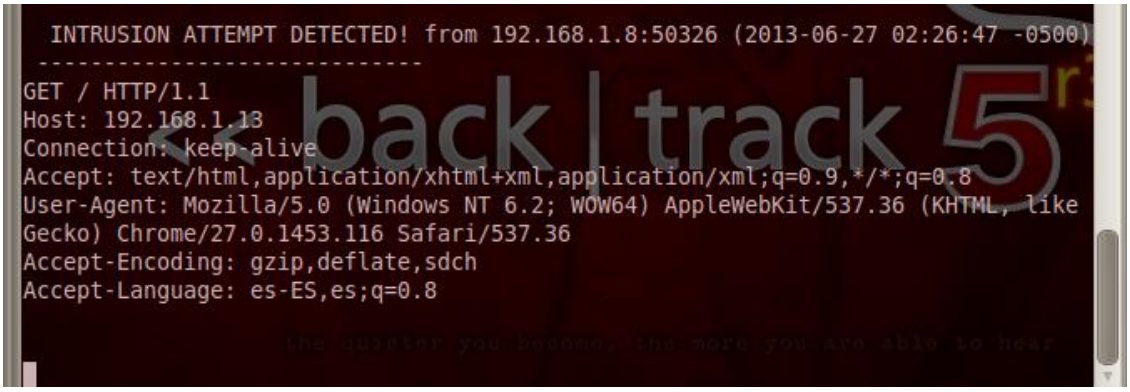


Con estos sencillos pasos el honeypot está listo para funcionar.

Paso 12. Probando el servicio. Desde cualquier navegador accedemos a la máquina donde esté configurado el honeypot a través de la ip y el puerto 80, aunque no es necesario colocar este último porque los navegadores lo toman por defecto para http:



Paso 14. Revisar en el host donde se encuentra el honeypot funcionando para asegurarse que fue detectado el intento de acceso:



BIBLIOGRAFÍA

http://cyberquotient.blogspot.com/2013/01/how-to-make-small-honey-pot-on-backtrack.html