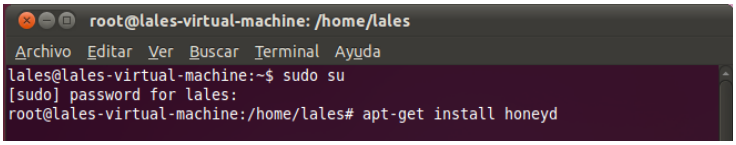
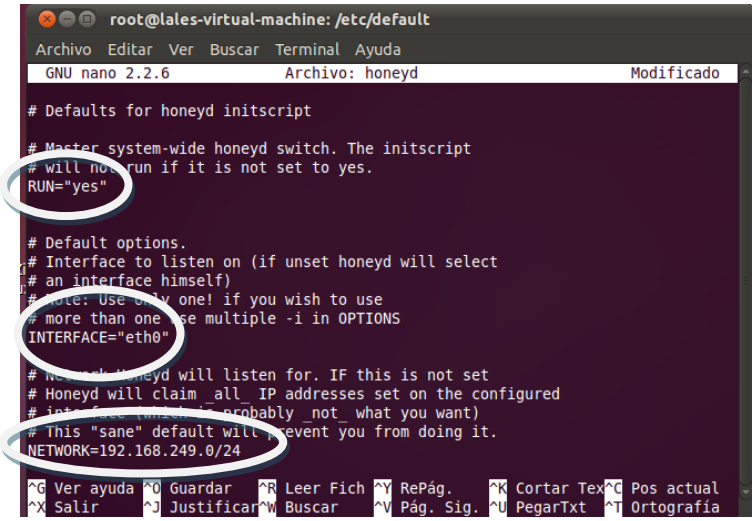
ACTIVIDAD 8 – INTENTOS DE PENETRACIÓN – TEMA 2

a) **Honeypots**. Instalación , configuración , ejecución y prueba en Windows o GNU/Linux de **honeyd** www.honeyd.org

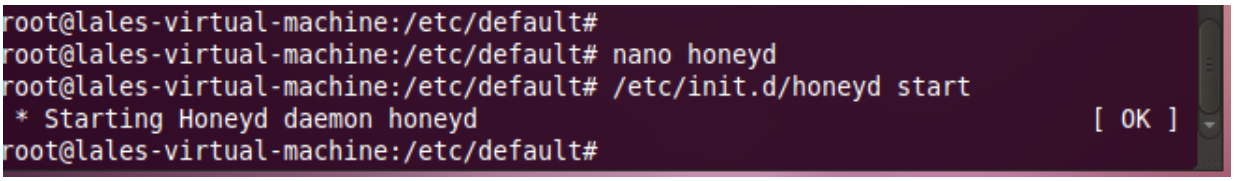
Nos descargamos la aplicación poniendo apt-get install honeyd



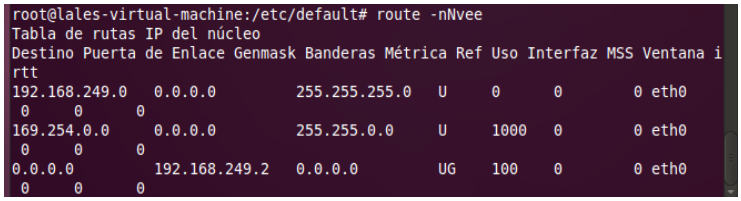
Ahora nos vamos al fichero de configuración que está en /etc/default/honeyd y lo configuramos



Y reiniciamos el servicio con /etc/init.d/honeyd start

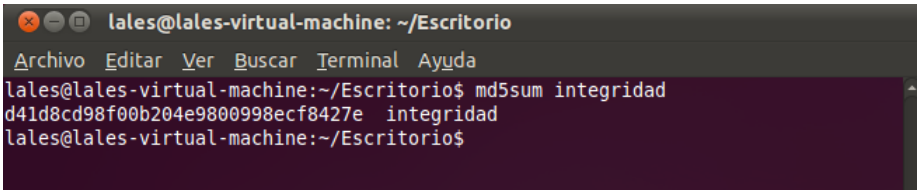


Y ahora ponemos route –nNvee y podemos ver las tablas de enrutamientos

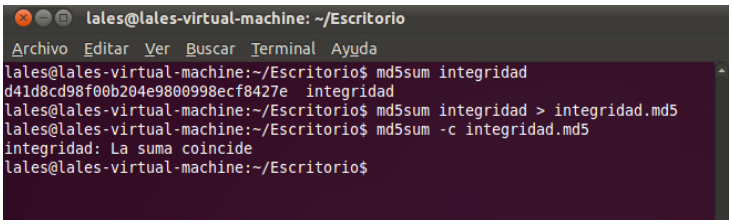


b) Sistema de detección de intrusos (IDS): HostIDS:
- Linux: Integridad de un fichero: md5sum.

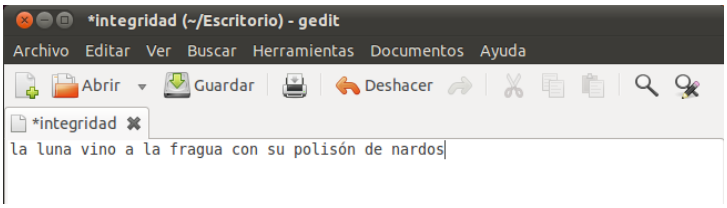
Creamos un fichero en el escritorio llamado integridad y ahora con el comando md5sum integridad, vamos a generar el hash del fichero



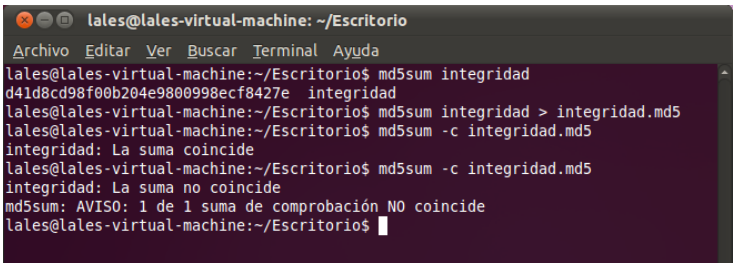
Vamos a copiar ese resultado en un fichero con extensión .md5 y vemos que la suma coincide



Ahora vamos a modificar el fichero con unas líneas

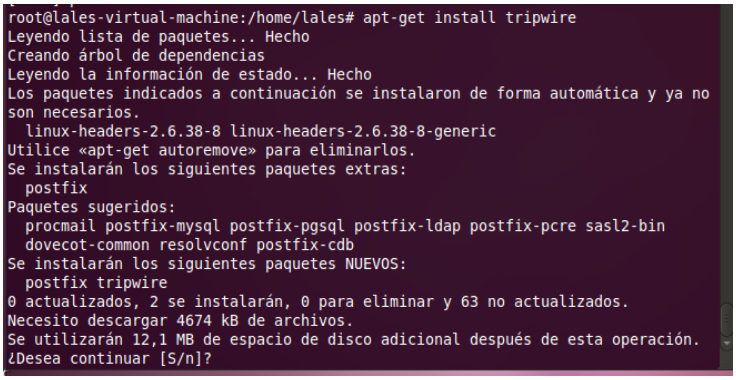


Si volvemos a ejecutar el mismo comando vemos que la integridad se ha perdido porque ya la suma no coincide

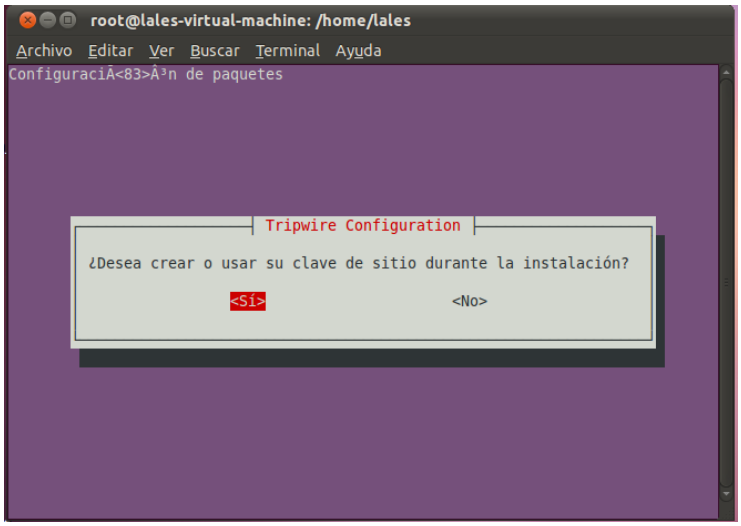


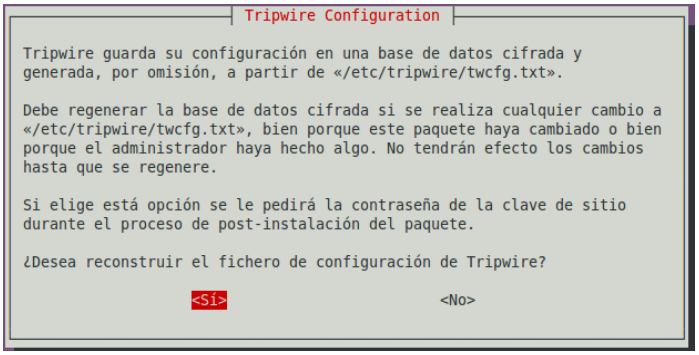
- Linux: Integridad de un sistema de ficheros: trypwire

Vamos a instalar trypwire, para ello ponemos apt-get install tripwire

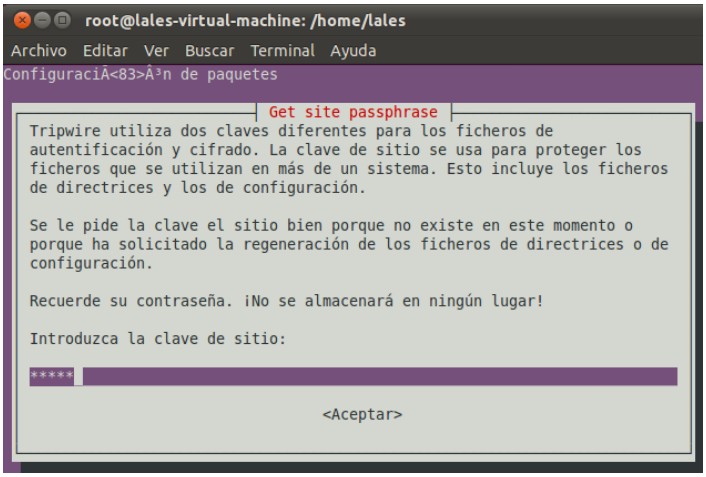


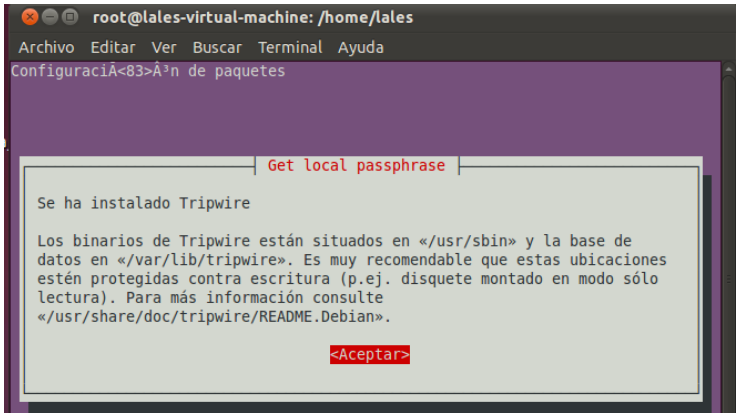
Nos sale un asistente, que vamos a ir dejando por defecto las opciones que nos da



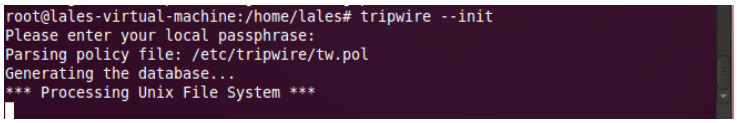


Nos pide una contraseña, vamos a poner inves

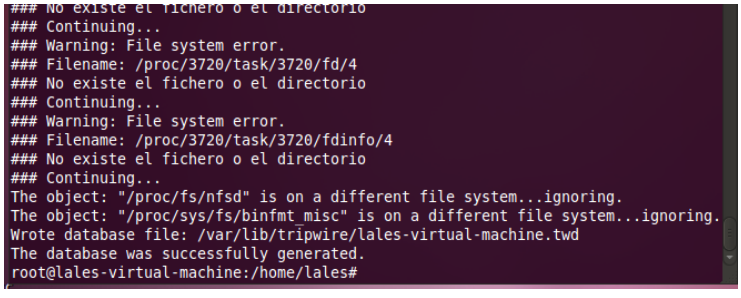




Ahora vamos a crear la base de datos con el comando tripwire –init



Y nos las crea correctamente



Una vez creado el archivo de configuración tendremos que crear un archivo de políticas, cuando lanzamos este comando luego nos pedirá nuestra contraseña. Nos creamos una base de datos para que se almacene todo lo del programa tripwire.

```
root@lales-virtual-machine:/home/lales# twadmin -m P /etc/tripwrite/twpol.txt
### Error: File could not be opened.
### Filename: /etc/tripwrite/twpol.txt
### No existe el fichero o el directorio
### Exiting...
root@lales-virtual-machine:/home/lales#
```

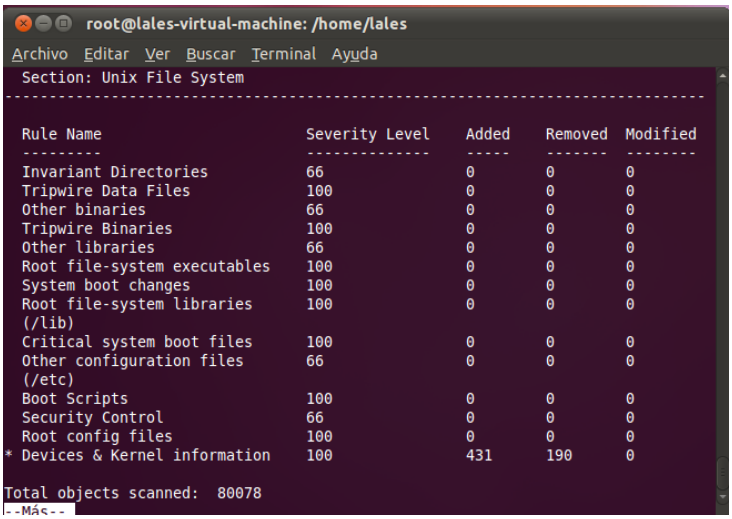
Y volvemos a poner el comando tripwire –init

```
### Continuing...
### Warning: File system error.
### Filename: /proc/3737/task/3737/fdinfo/4
### No existe el fichero o el directorio
### Continuing...
The object: "/proc/fs/nfsd" is on a different file system...ignoring.
The object: "/proc/sys/fs/binfmt_misc" is on a different file system...ignoring.
Wrote database file: /var/lib/tripwire/lales-virtual-machine.twd
The database was successfully generated.
```

Ahora generamos un informe para ver si registra las modificaciones

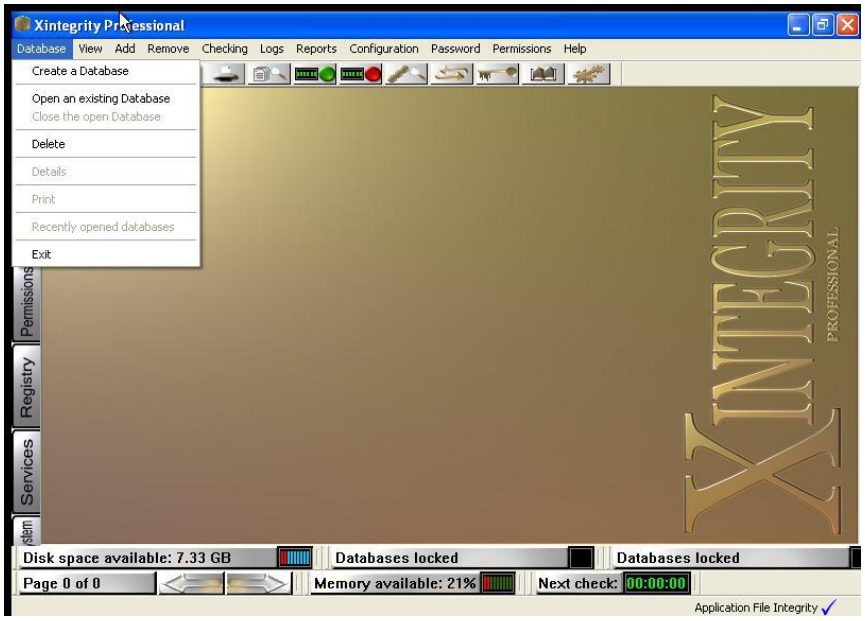
```
root@lales-virtual-machine:/home/lales# tripwire --check | more
Parsing policy file: /etc/tripwire/tw.pol
*** Processing Unix File System ***
Performing integrity check...
```

```
root@lales-virtual-machine: /home/lales
Archivo  Editar  Ver  Buscar  Terminal  Ayuda

Open Source Tripwire(R) 2.4.1 Integrity Check Report

Report generated by:          root
Report created on:            Mon Apr 16 03:06:14 2012
Database last updated on:     Never

================================================================================
Report Summary:
================================================================================

Host name:                    lales-virtual-machine
Host IP address:              127.0.1.1
Host ID:                      None
Policy file used:             /etc/tripwire/tw.pol
Configuration file used:      /etc/tripwire/tw.cfg
Database file used:           /var/lib/tripwire/lales-virtual-machine.twd
Command line used:            tripwire --check
```

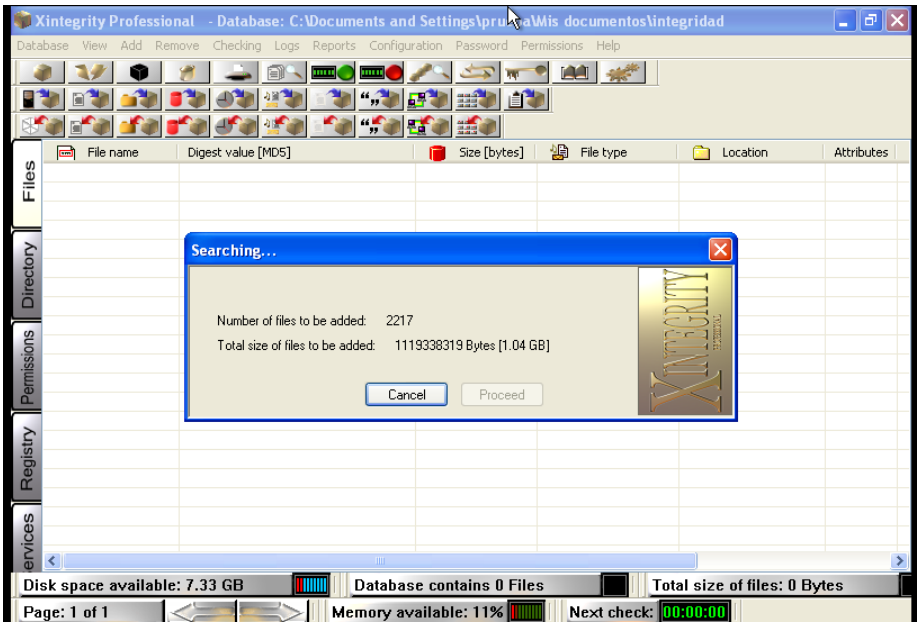


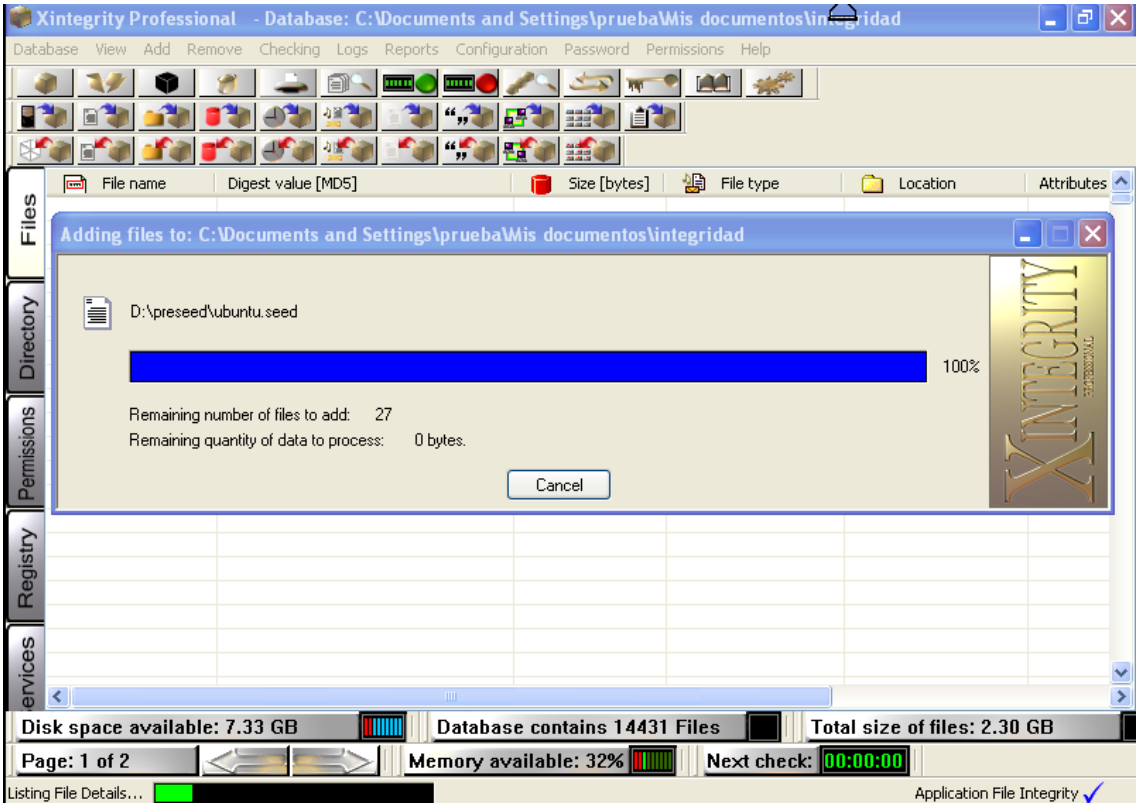
- Windows: Integridad del sistema de ficheros mediante Xintegrity.

Nos descargamos el programa Xintegrity y en la pantalla principal creamos una base de datos

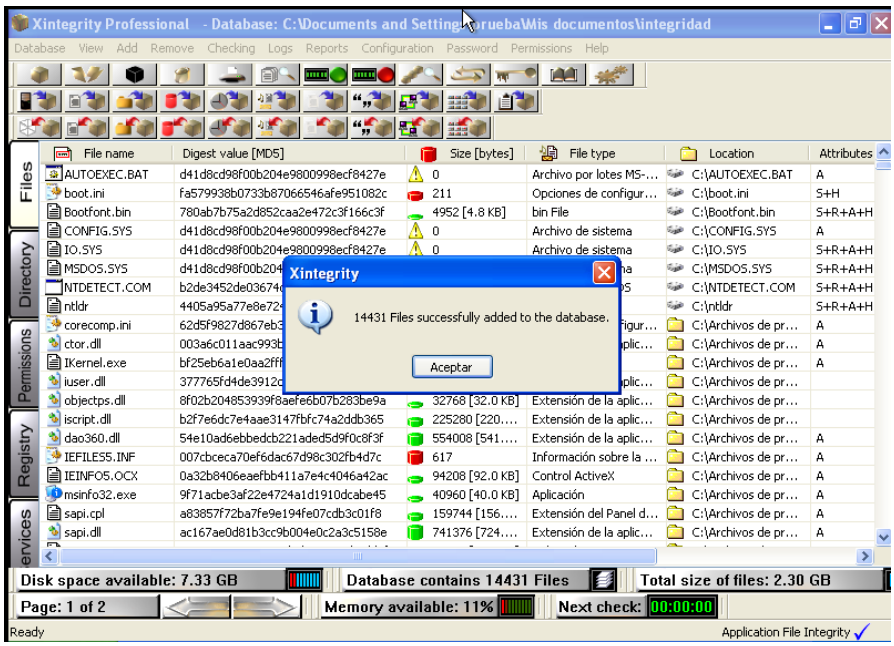


A continuación añadimos los archivos a nuestra base de datos





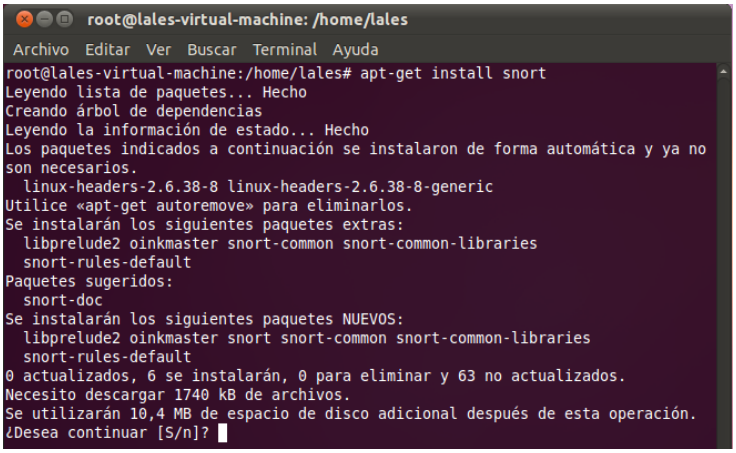
Y nos da correctamente todos los archivos que se han creado en la base de datos



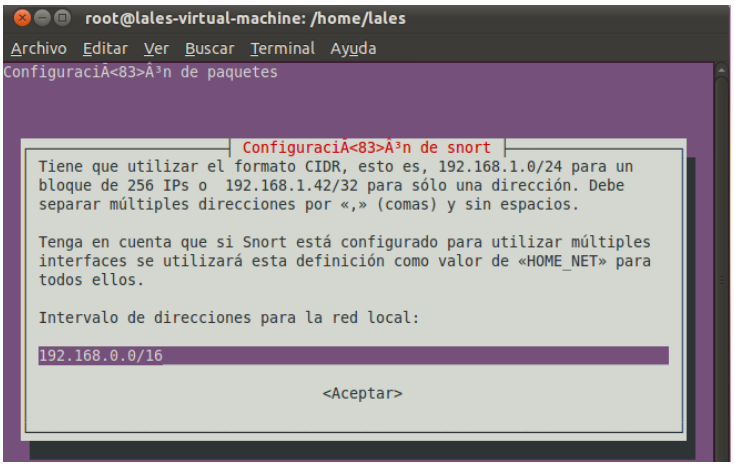
c) Sistema de detección de intrusos (IDS): Net IDS:
- Instala y configura Snort en GNU/Linux.

www.snort.org

Instalamos con apt-get install snort

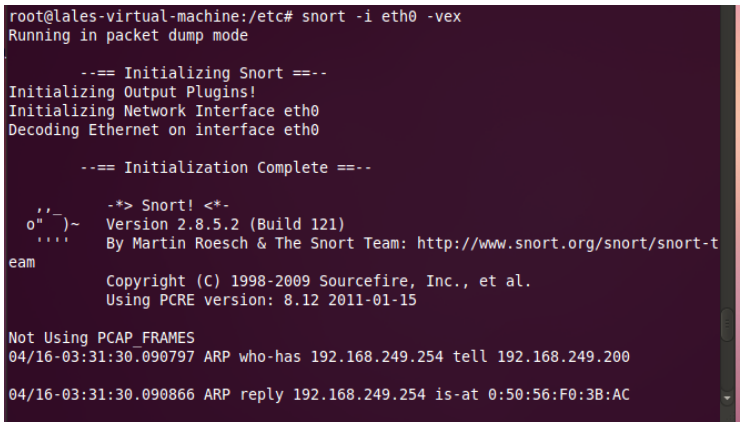


Durante la instalación nos pide el intervalo de direcciones para la red local

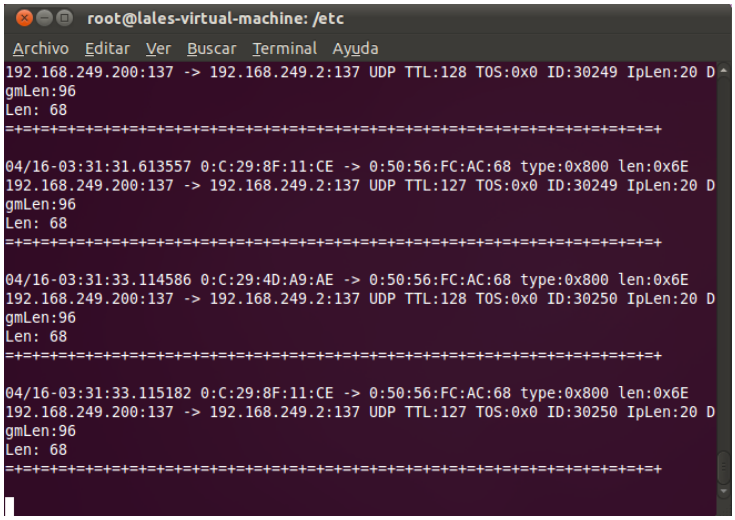


Ahora ponemos el comando para ejecutar snort, para ello ponemos

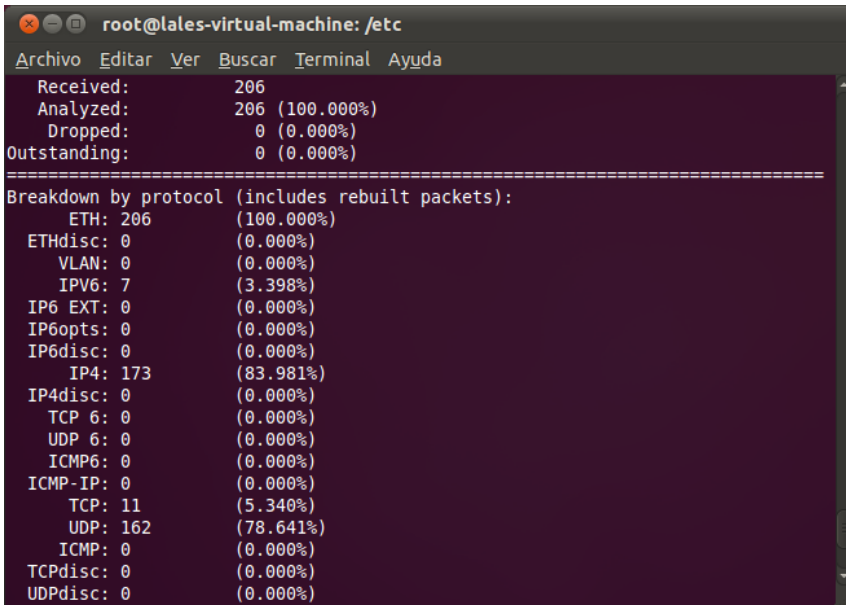
Snort –i eth0 –vex



Y nos aparecen las escuchas que ha hecho



Al final nos muestra un resumen de todas las escuchas que ha hecho



MARÍA ÁNGELES PEÑASCO SÁNCHEZ – ACTIVIDAD 8 – TEMA 2 – SAD