Laboratorio de Informática
Ingeniería de Sistemas
Escuela Colombiana de Ingeniería Julio Garavito

¿Cómo instalar la herramienta OSSEC 2.8 en Slackware 13.37?

¿Qué es OSSEC?

Es un proyecto open source, que permite monitorear y controlar los sistemas. Combina aspectos de HIDS (Host-Based intrusion detection), monitoreo de logs y manejo de incidentes.

Para más información visite: http://ossec.github.io/docs/manual/non-technical-overview.html

Requerimientos del sistema

Para poder instalar la herramienta se deben incluir paquetes que permitan compilar e instalar paquetes, los cuales se listan a continuación:

- ✓ a/
  - glibc-solibs-2.13-i486-4.txz
  - kernel-modules-2.6.37.6-i486-2.txz
- ✓ d/
  - make-3.82-i486-2.txz
  - gcc-4.5.2-i486-2.txz
  - gcc-g++-4.5.2-i486-2.txz
  - binutils-2.21.51.0.6-i486-1.txz
  - kernel-headers-2.6.37.6_smp-x86-2.txz
- ✓ k/
  - kernel-source-2.6.37.6_smp-noarch-2.txz
- ✓ l/
  - mpfr-3.0.1-i486-1.txz
  - glibc-2.13-i486-4.txz
  - glib2-2.28.6-i486-1.txz
  - glib-1.2.10-i486-3.txz
  - libmpc-0.8.2-i486-2.txz
  - libmcrypt-2.5.8-i486-1.txz
- ✓ n/
  - wget-1.12-i486-1.txz

Proceso de instalación

1. Descargar la última versión, se ejecuta el siguiente comando

   `wget -U ossec -O ossec.tar.gz` https://bintray.com/artifact/download/ossec/ossec-hids/ossec-hids-2.8.3.tar.gz

```
root@slackware:~# wget -U ossec -O ossec.tar.gz  https://bintray.com/artifact/download/ossec/ossec-hids/ossec-hids-2.8.3.tar.gz --no-check-certificate
--2017-02-28 13:36:15--  https://bintray.com/artifact/download/ossec/ossec-hids/ossec-hids-2.8.3.tar.gz
Resolving bintray.com (bintray.com)... 108.168.194.93
Connecting to bintray.com (bintray.com)|108.168.194.93|:443... connected.
WARNING: cannot verify bintray.com's certificate, issued by '/C=US/O=GeoTrust Inc./CN=GeoTrust SSL CA - G3':
  Unable to locally verify the issuer's authority.
HTTP request sent, awaiting response... 302 Found
Location: https://dl.bintray.com/ossec/ossec-hids/ossec-hids-2.8.3.tar.gz [following]
--2017-02-28 13:36:15--  https://dl.bintray.com/ossec/ossec-hids/ossec-hids-2.8.3.tar.gz
Resolving dl.bintray.com (dl.bintray.com)... 108.168.243.150
Connecting to dl.bintray.com (dl.bintray.com)|108.168.243.150|:443... connected.
WARNING: cannot verify dl.bintray.com's certificate, issued by '/C=US/O=GeoTrust Inc./CN=GeoTrust SSL CA - G3':
  Unable to locally verify the issuer's authority.
HTTP request sent, awaiting response... 302
Location: https://akamai.bintray.com/87/87c7a1904d5c08c7cff3e42bd47c055b14b08faa?__gda__=exp=1488325803~hmac=3cddc50787b94565891762aef4b18583c27718a50bd306f8b14ccb89a0b33dee&re
ition=attachment%3Bfilename%3D%22ossec-hids-2.8.3.tar.gz%22&response-content-type=application%2Fgzip&requestInfo=U2FsdGVkX18CwNdUzXVVfDTYpAJ3y1YryQWsIjWIWG-6FPPb8w1M6Dpai1ycON1
H7DZvqDl7VvABj3rdPHyEIx7ieN_8vIv-crbnkMbi5vT [following]
--2017-02-28 13:36:16--  https://akamai.bintray.com/87/87c7a1904d5c08c7cff3e42bd47c055b14b08faa?__gda__=exp=1488325803~hmac=3cddc50787b94565891762aef4b18583c27718a50bd306f8b14c
-content-disposition=attachment%3Bfilename%3D%22ossec-hids-2.8.3.tar.gz%22&response-content-type=application%2Fgzip&requestInfo=U2FsdGVkX18CwNdUzXVVfDTYpAJ3y1YryQWsIjWIWG-6FPPb
W5pmRrgolhFSiGzH7DZvqDl7VvABj3rdPHyEIx7ieN_8vIv-crbnkMbi5vT
Resolving akamai.bintray.com (akamai.bintray.com)... 23.32.201.90
Connecting to akamai.bintray.com (akamai.bintray.com)|23.32.201.90|:443... connected.
WARNING: cannot verify akamai.bintray.com's certificate, issued by '/C=NL/L=Amsterdam/O=Verizon Enterprise Solutions/OU=Cybertrust/CN=Verizon Akamai SureServer CA G14-SHA2':
  Unable to locally verify the issuer's authority.
HTTP request sent, awaiting response... 200 OK
Length: 1642095 (1.6M) [application/gzip]
Saving to: 'ossec.tar.gz'

100%[=============================================================================================================================================>] 1,642,095   2

2017-02-28 13:36:18 (2.03 MB/s) - 'ossec.tar.gz' saved [1642095/1642095]
```

2. Descomprimir el archivo y entrar a la carpeta:
   tar –xvf ossec.tar.gz
   cd ossec-hids-2.8.3/
   Deben aparecer los siguientes archivos:

```
root@slackware:~/ossec-hids-2.8.3# ls
BUGS  CONFIG  CONTRIBUTORS  INSTALL  LICENSE  README.md  active-response/  contrib/  doc/  etc/  install.sh*  src/
root@slackware:~/ossec-hids-2.8.3#
```

3. Ejecutamos el archivo install.sh

```
root@slackware:~/ossec-hids-2.8.3# ./install.sh
```

4. Cuando ejecutemos el archivo, se iniciará el proceso de instalación, como queremos instalar un agente HIDS debemos escoger las siguientes opciones:

```
root@slackware:~/ossec-hids-2.8.3# ./install.sh
which: no host in (/usr/local/sbin:/usr/sbin:/sbin:/usr/local/bin:/usr/bin:/bin:/usr/games)

  ** Para instalação em português, escolha [br].
  ** 要使用中文进行安装，请选择 [cn].
  ** Fur eine deutsche Installation wohlen Sie [de].
  ** Για εγκατάσταση στα Ελληνικά, επιλέξτε [el].
  ** For installation in English, choose [en].
  ** Para instalar en Español , eliga [es].
  ** Pour une installation en français, choisissez [fr]
  ** A Magyar nyelvű telepítéshez válassza [hu].
  ** Per l'installazione in Italiano, scegli [it].
  ** 日本語でインストールします．選択して下さい．[jp].
  ** Voor installatie in het Nederlands, kies [nl].
  ** Aby instalować w języku Polskim, wybierz [pl].
  ** Для инструкций по установке на русском ,введите [ru].
  ** Za instalaciju na srpskom, izaberi [sr].
  ** Türkçe kurulum için seçin [tr].
  (en/br/cn/de/el/es/fr/hu/it/jp/nl/pl/ru/sr/tr) [en]: en
```

```
which: no host in (/usr/local/sbin:/usr/sbin:/sbin:/usr/local/bin:/usr/bin:/bin:/usr/games)

./install.sh: line 967: clear: command not found
 OSSEC HIDS v2.8.3 Installation Script - http://www.ossec.net

 You are about to start the installation process of the OSSEC HIDS.
 You must have a C compiler pre-installed in your system.
 If you have any questions or comments, please send an e-mail
 to dcid@ossec.net (or daniel.cid@gmail.com).

  - System: Linux slackware 3.10.17
  - User: root
  - Host: slackware


  -- Press ENTER to continue or Ctrl-C to abort. --
```

Presionamos Enter.

```
  1- What kind of installation do you want (server, agent, local, hybrid or help)? agent
```

En el siguiente paso nos preguntará la ruta en la que queremos instalar el agente, la ruta estándar en el laboratorio es /usr/local/ossec

```
2- Setting up the installation environment.

 - Choose where to install the OSSEC HIDS [/usr/local/ossec]: /usr/local/ossec
```

Aquí ponemos la IP del servidor que va a recolectar los eventos.

```
3- Configuring the OSSEC HIDS.

  3.1- What's the IP Address or hostname of the OSSEC HIDS server?:
```

```
3- Configuring the OSSEC HIDS.

  3.1- What's the IP Address or hostname of the OSSEC HIDS server?: 10.2.78.8

   - Adding Server IP 10.2.78.8

  3.2- Do you want to run the integrity check daemon? (y/n) [y]:

   - Running syscheck (integrity check daemon).

  3.3- Do you want to run the rootkit detection engine? (y/n) [y]:

   - Running rootcheck (rootkit detection).

  3.4 - Do you want to enable active response? (y/n) [y]:
```

Para las siguientes 3 opciones, damos enter para que habilite los servicios que necesita.

```
  3.5- Setting the configuration to analyze the following logs:
    -- /var/log/messages
    -- /var/log/secure
    -- /var/log/syslog
    -- /var/adm/syslog
    -- /var/adm/messages
    -- /var/log/maillog

- If you want to monitor any other file, just change
  the ossec.conf and add a new localfile entry.
  Any questions about the configuration can be answered
  by visiting us online at http://www.ossec.net .


   --- Press ENTER to continue ---
```

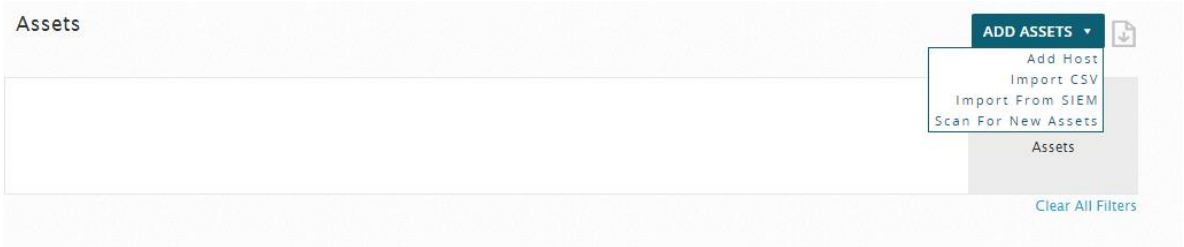
Presionamos Enter y comenzará el proceso de instalación, en caso de generarse un error se debe revisar que todos los paquetes listados anteriormente se encuentren instalados.

```
Started ossec-agentd...
Started ossec-logcollector...
Started ossec-syscheckd...
Completed.

- Configuration finished properly.

- To start OSSEC HIDS:
             /var/ossec/bin/ossec-control start

- To stop OSSEC HIDS:
             /var/ossec/bin/ossec-control stop

- The configuration can be viewed or modified at /var/ossec/etc/ossec.conf


   Thanks for using the OSSEC HIDS.
   If you have any question, suggestion or if you find any bug,
   contact us at contact@ossec.net or using our public maillist at
   ossec-list@ossec.net
   ( http://www.ossec.net/main/support/ ).

   More information can be found at http://www.ossec.net

   ---  Press ENTER to finish (maybe more information below). ---
```

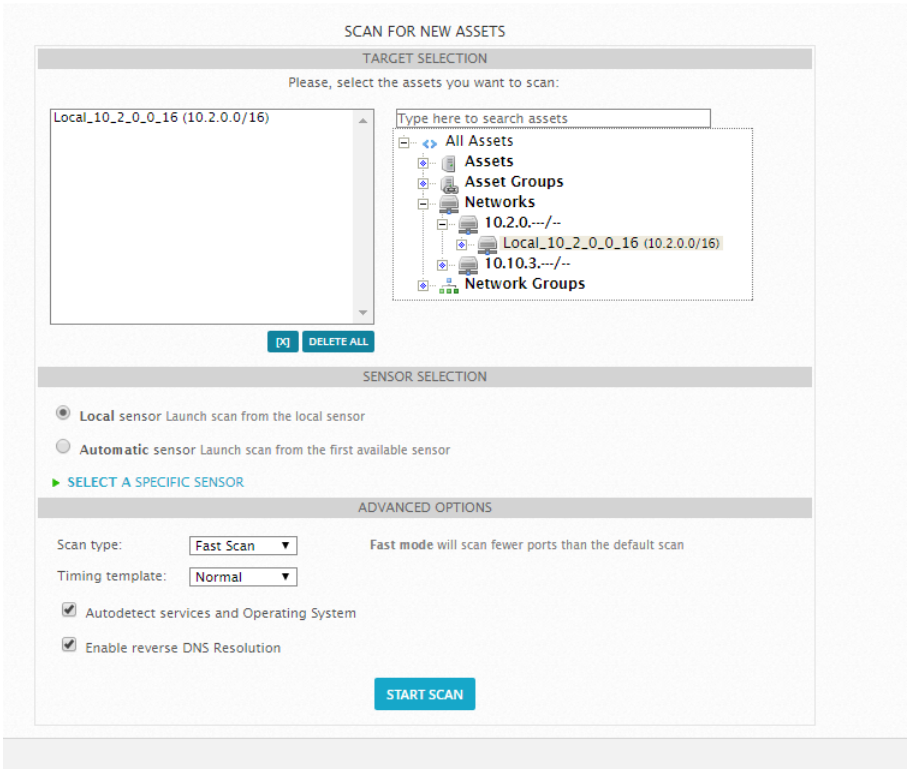
Si la instalación se completó con éxito, se debe mostrar el mensaje anterior.

Conectar el servidor a la plataforma OSSIM

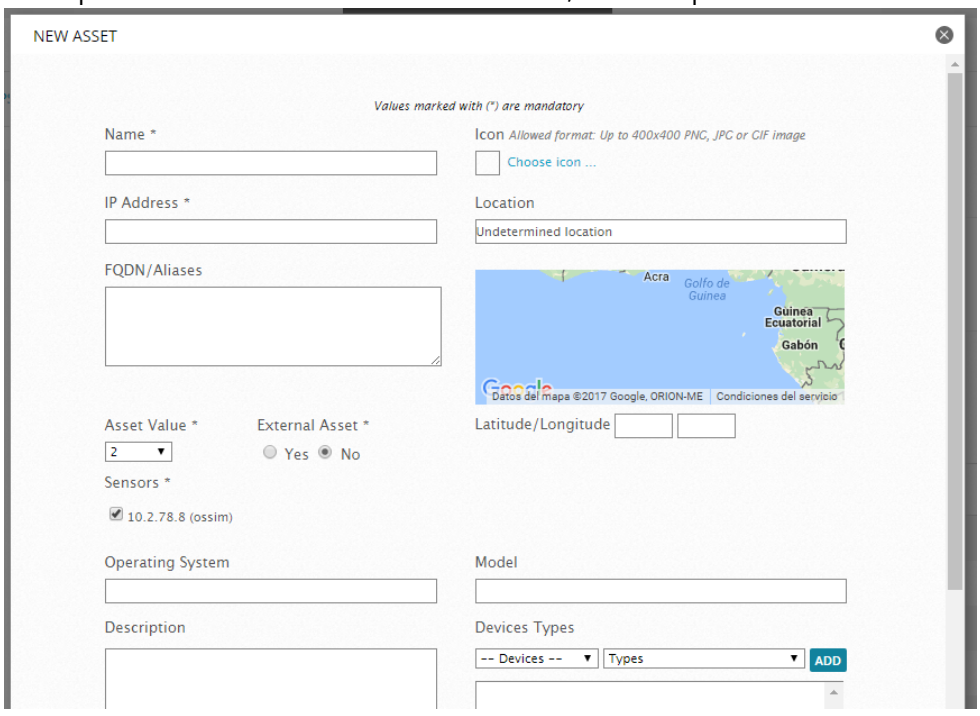
1. Generamos la llave en la plataforma OSSIM. Para ello nos dirigimos a la pestaña Enviroment->Assets & Groups. Aparecerá un listado de activos conectados a la plataforma, en caso de que no aparezca en el menú:



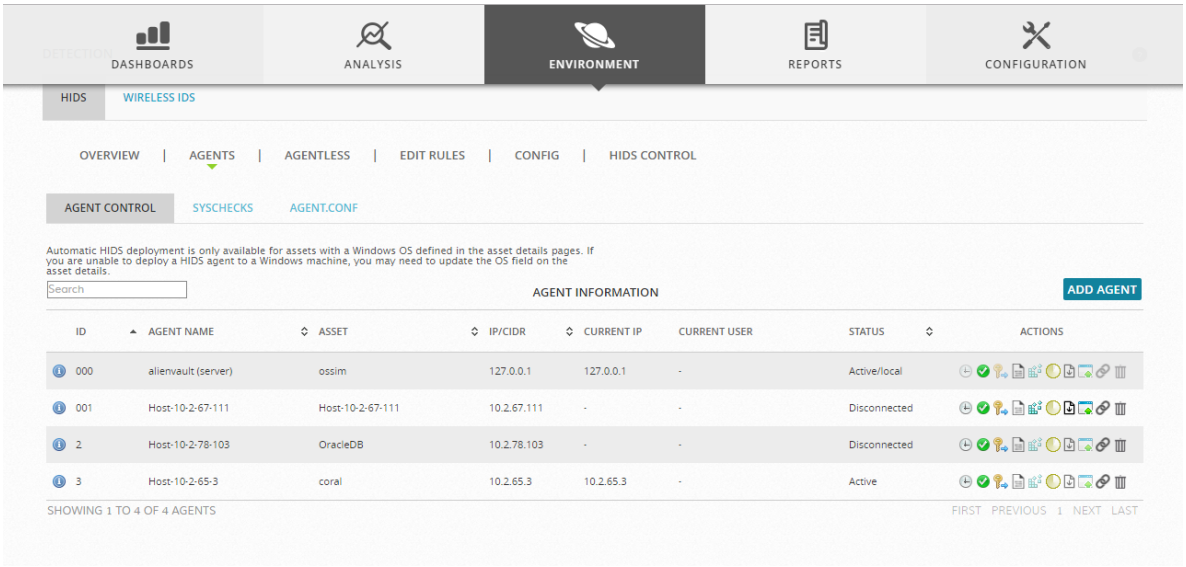
Nos dirigimos a Scan For New Assets en caso de que se quiera escanear la red, eligiendo qué activo queremos escanear en el menú lateral:



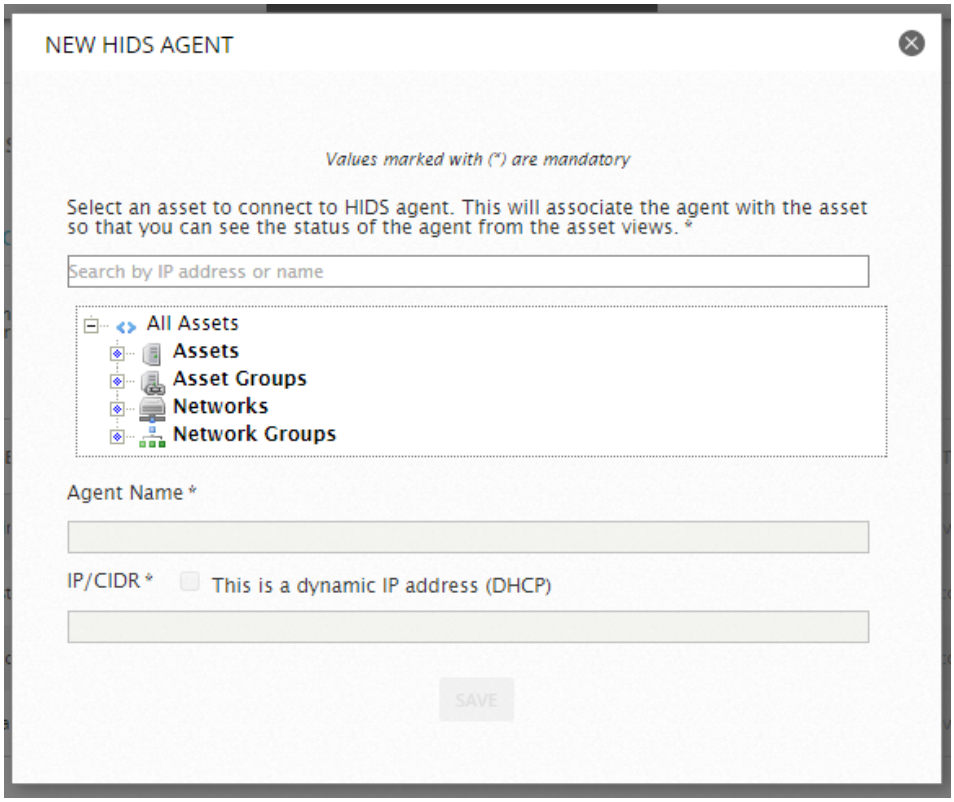
O lo podemos añadir manualmente, en la opción Add Host:



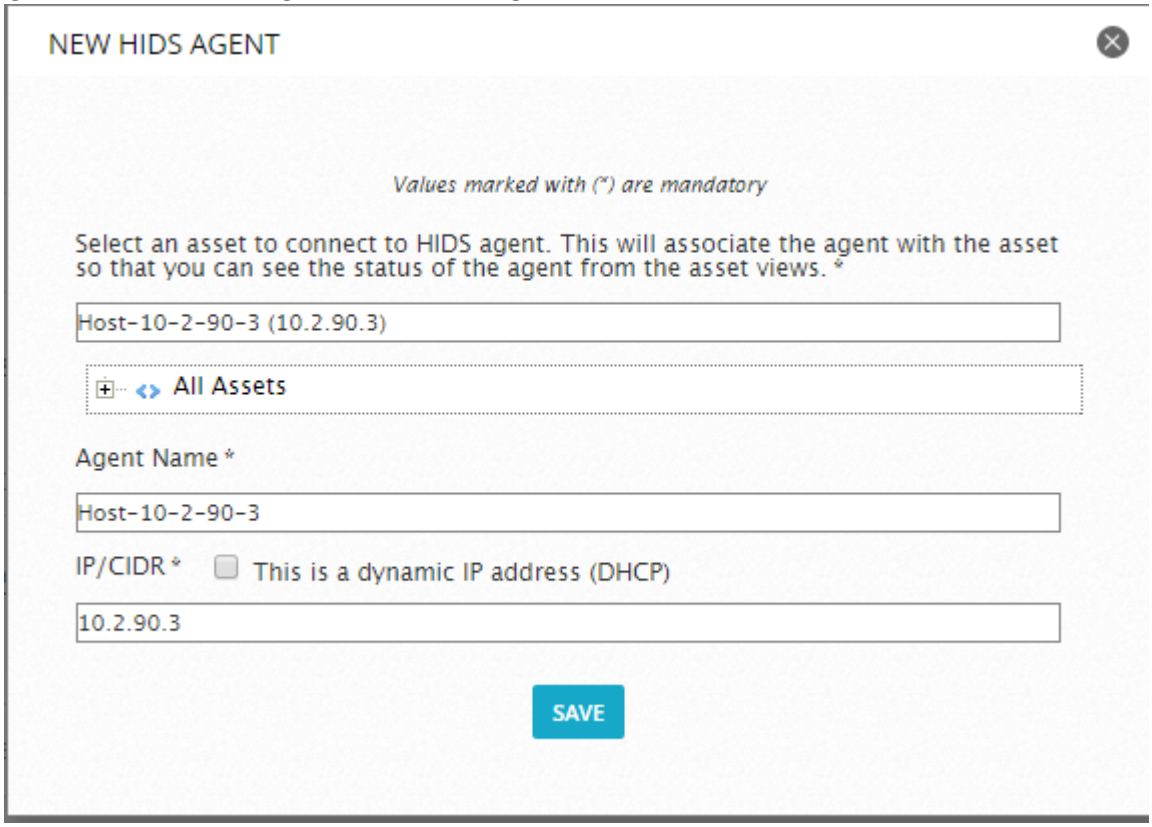
Nos dirigimos al menú Enviroment->Detection->Agents



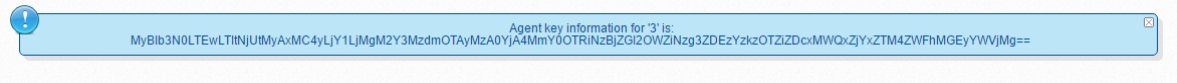
2. Damos click en el botón ADD AGENT y aparecerá la siguiente ventana:



En esta ventana buscamos la ip del activo que acabamos de agregar, y automáticamente pondrá los campos correspondientes a la IP y el nombre del agente. Damos click en el botón Save y se guardará la configuración del agente HIDS.



3. Copiamos la llave generada haciendo click en el botón  aparecerá un diálogo con la llave que se debe utilizar para conectar el servidor con la plataforma:



Configurar llave de la plataforma OSSIM en el servidor Slackware

1. Nos dirigimos a la ruta donde está instalado OSSEC (/usr/local/ossec/bin):

```
root@slackware:/usr/local/ossec/bin# ls
agent-auth*     ossec-agentd*   ossec-execd*         ossec-lua*   ossec-syscheckd*
manage_agents*  ossec-control*  ossec-logcollector*  ossec-luac*  util.sh*
```

2. Ejecutamos el script manage_agents:

```
root@slackware:/var/ossec/bin# ./manage_agents


****************************************
* OSSEC HIDS v2.8.3 Agent manager.     *
* The following options are available: *
****************************************
   (I)mport key from the server (I).
   (Q)uit.
Choose your action: I or Q: _
```

Seleccionamos la opción "I" y escribimos la llave generada:

```
* Provide the Key generated by the server.
* The best approach is to cut and paste it.
*** OBS: Do not include spaces or new lines.

Paste it here (or '\q' to quit):
```

Nos aparece el menú anterior y seleccionamos la opción "Q".

3. Corremos el script de inicio del agente:

```
./ossec-control start
```

```
root@slackware:/usr/local/ossec/bin# ./ossec-control start
Starting OSSEC HIDS v2.8.3 (by Trend Micro Inc.)...
Started ossec-execd...
2017/03/09 13:23:20 ossec-agentd: INFO: Using notify time: 600 and max time to reconnect: 1800
Started ossec-agentd...
Started ossec-logcollector...
Started ossec-syscheckd...
Completed.
root@slackware:/usr/local/ossec/bin#
```

Con estos pasos ya quedará conectado el servidor a la plataforma OSSIM.

Versión actual **1.2**		
Autor	María Alejandra Blanco Uribe	
Fecha de creación	02/03/2017	
Modificaciones		
Responsable	**Fecha**	**Cambio**
María Alejandra Blanco Uribe	09/03/2017	Cambios en las rutas de archivos y comandos a ejecutar.
David Rivera	21/04/2021	Se aplica una corrección al manual y a su vez sufre pocos cambios.