OSSIM

Autor: Enrique Rodríguez Rodríguez

ossim,, monitorización

Instalación

- Descargar la ISO desde http://www.alienvault.com/opensourcesim.php?section=Downloads
- Instalar la ISO siguiendo los pasos.
- Cuando se termine la instalación actualizar el Ossim.

Mapa general de Ossim

Dashboards

- Dashboards. Información de todos las áreas y datos generales, separados en diferentes secciones.
- Risk. Visualización de riesgos de forma gráfica.

Incidents

- Alarms. Listado de alarmas con opciones para administrarlas y crear informes.
- Tickets. Los tickets son tipos de incidencias que pueden ser configuradas para detectar lo que se quiera, alarmas, anomalías u otras. Aquí también se mostrarán gráficas con datos de los tickets.
- Knowledge DB. Documentos creados por usuarios que pueden ser asociados a varios elementos como hosts, redes, incidentes, etc.

Analysis

- Gestión de la seguridad del sistema. Contiene análisis de eventos y anomalías y sus estadísticas.

Reports

- Reports. Da opciones de visualizar diferentes informes y datos sobre la red o el hosts que se quiera ver, sobre las anomalías detectadas y otros modos.

Assets

- Asset Search. Posibilidad de realizar búsquedas de hosts con múltiples filtros.
- Assets. Listado de hosts registrados con posibilidad de gestionarlos.
- SIEM Components. Sensores.

Intelligence

- Configuración de políticas, acciones y directivas.

Monitors

- Network. Tenemos muchas opciones para ver datos con diferentes gráficas de servicios o por host. Por ejemplo si entramos en la pestaña Profiles y luego en Summary –> Hosts podremos ver la lista de hosts monitorizados con sus datos, pudiendo entrar en cada uno de ellos para ver mas detalles y gráficas.
- Availability. Datos de la monitorización de los hosts dados por le nagios.
- System. Información sobre los plugins instalados y su estado y la posibilidad de activarlos o desactivarlos. Actividad de los usuarios.

Configuration

- Configuración de Ossim, sus usuarios, los plugins y las actualizaciones del software.

Tools

- Herramientas para hacer copias de seguridad, descarga de utilidades y escaneos de la red.

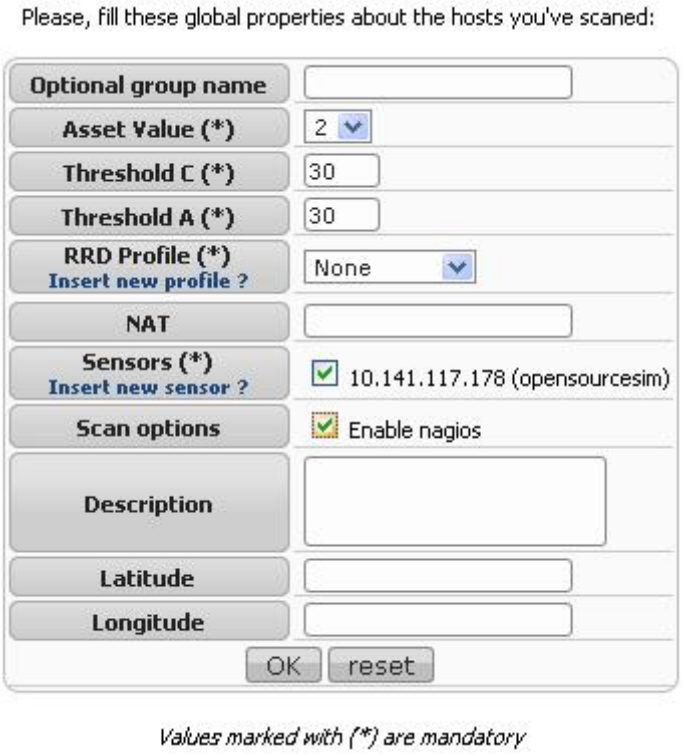
Monitorización

Lo primero que se debería realizar es una búsqueda en la red sencilla para ver que se puede encontrar. Para eso vamos a **Tools –> Net Discovery** y configuramos la búsqueda. La primera opción es la de seleccionar la red, podremos elegir una de las que viene por defecto, una que hayamos definido nosotros antes en otro apartado del Ossim o poner la red de forma manual. La forma manual se puede poner de la siguiente manera: **192.168.1.0/24**, **192.168.1.64-68** o **192.168.1.64** en el caso de que solo sea esa la dirección que se desee escanear y no un rango de direcciones. **Enable full scan** nos da la opción de escanear los servicios de las direcciones, por defecto esta **Disable**, pero se puede poner en **Fast Scan** o **Full Scan. Timing template** nos da a elegir entre los modos de escaneo, por defecto en **normal.**

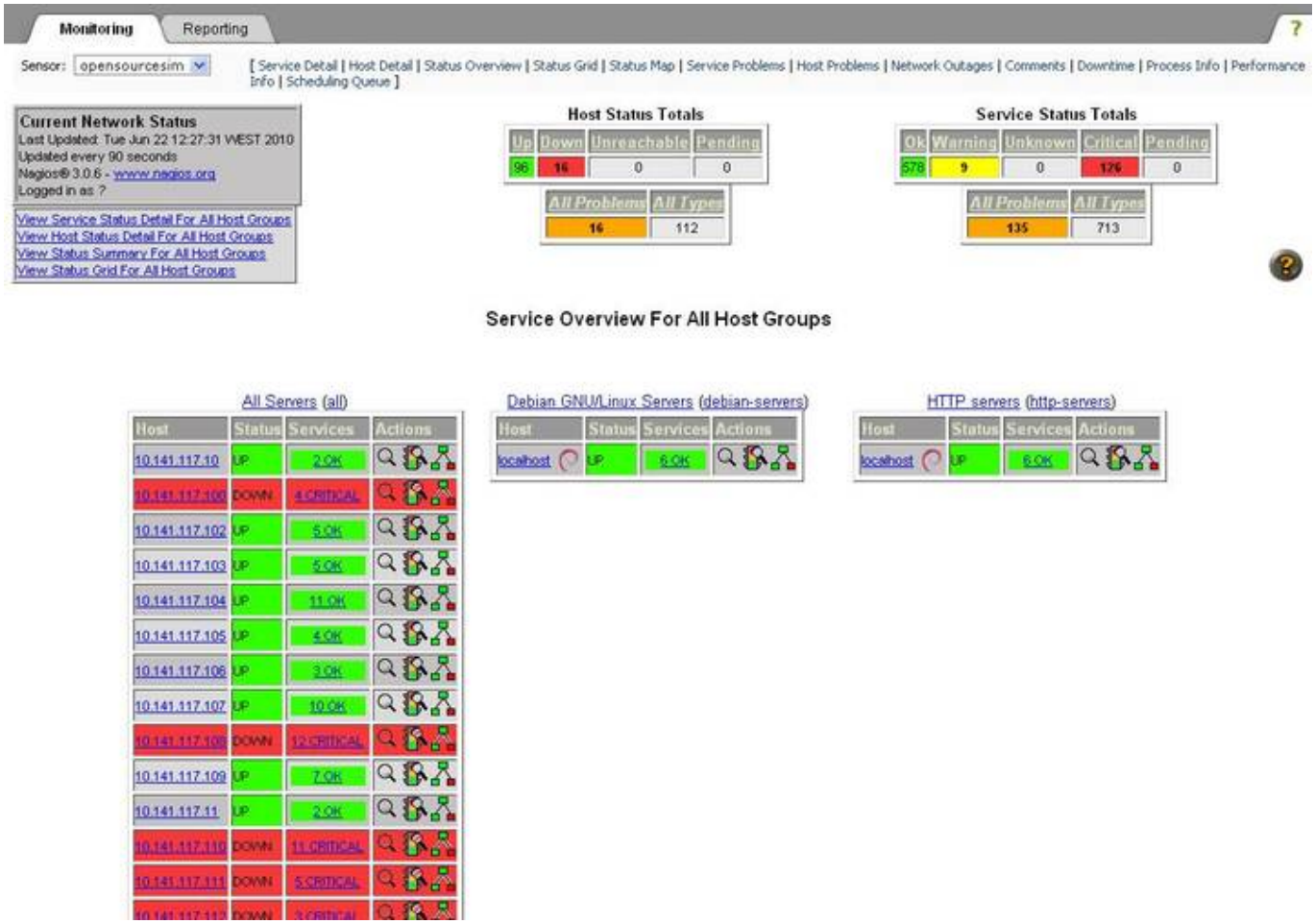
Para empezar se recomienda hacer una búsqueda general de toda el rango de direcciones, con la opción **Enable full scan** en **Disable** y el modo **normal**, para identificar todas las direcciones que tenemos disponibles. Lo siguiente sería escanear una a una las direcciones que se deseen monitorizar, con la opción **Enable full scan** en **Full Scan** y **Timing template** en **normal.** No se recomienda hacer la búsqueda de un rango de direcciones con la opción **Enable full scan** en **Full Scan** porque puede caerse el apache y no se completaría la operación.

Cuando se completa una búsqueda saldrá un mensaje: **Scan completed. Click here to show the**

results. Nos llevará de nuevo al apartado de búsqueda añadiendo al final el **Scan results.** Si interesara guardar los resultados de la búsqueda en la base de datos, marcaríamos la casilla **Insert** de los host que interesa guardar y le daríamos a **Update database values.** Nos llevara a un formulario donde se nos pedirá una serie de datos, ya unos configurados por defecto y los demás no son necesarios. La que hay que tener en cuenta es la opción **Scan options**, que por defecto está desmarcada y si no se marca este host no será monitorizado por **nagios**, cosa que interesa tener. Para terminar le daremos a **OK** y será insertado el host en la base de datos si no existía y si existía será actualizado.



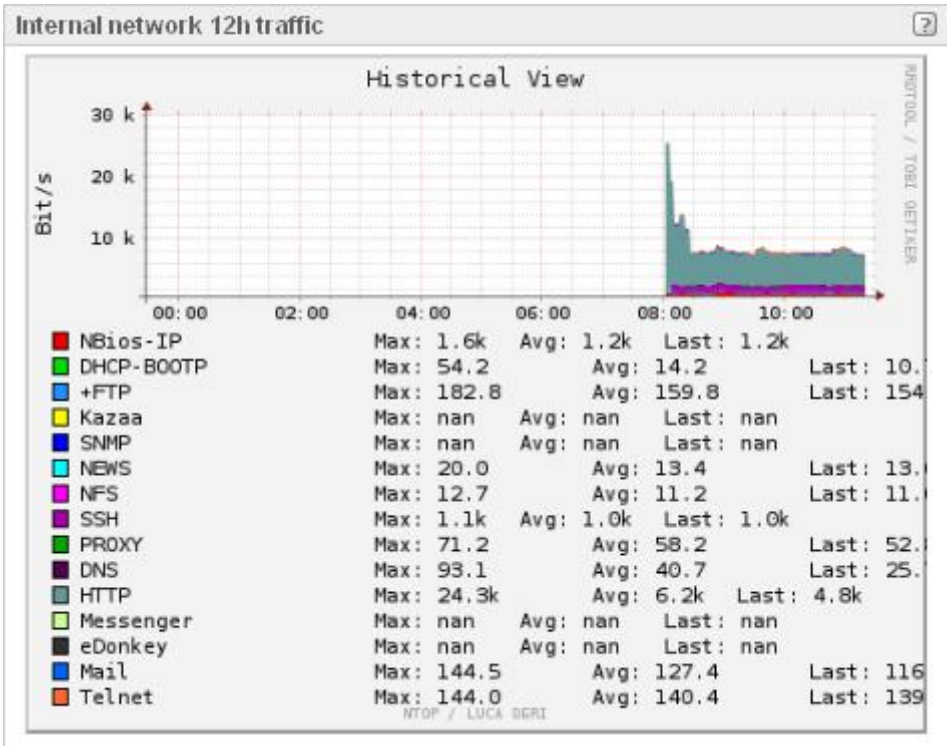
Para ver los datos de hosts, servicios y estados en los que se encuentran deberemos ir a **Monitors -> Availability** o a **Dashboards -> Dashboards** y picar sobre la imagen de la gráfica **Availability.**



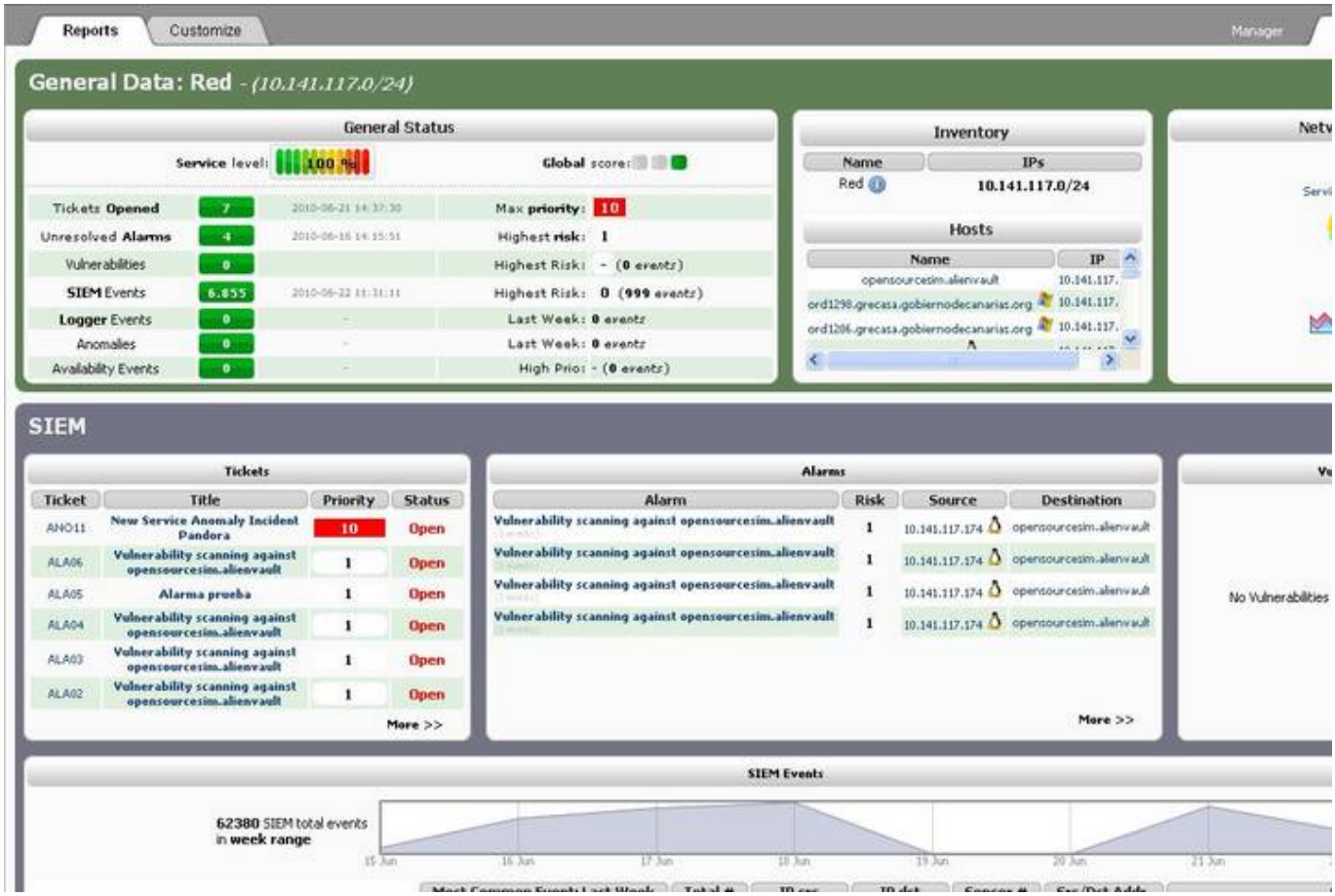
Si hay un error en la monitorización de alguno de los hosts, puede dar error en el nagios y puede que no muestre nada, en ese caso mirar que hosts son los que fallan y eliminar los servicios o hosts que sean necesarios para seguir con el funcionamiento normal del nagios.

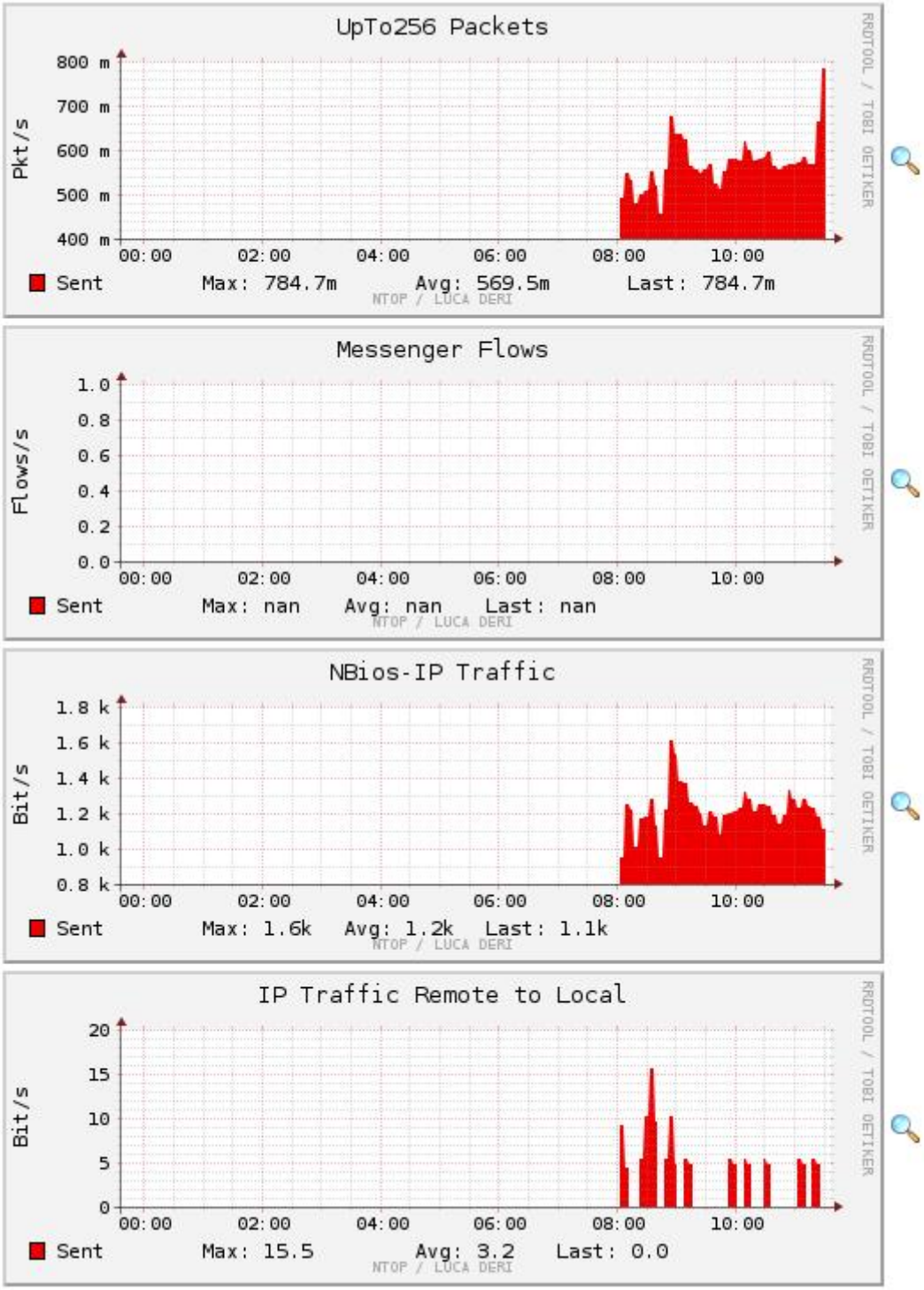
Visualizar datos de la red

Dashboards -> Dashboards -> Network. Aquí se nos muestra alguna de las gráficas sobre datos de red. En alguna podremos picar y entrar para ver mas detalles.

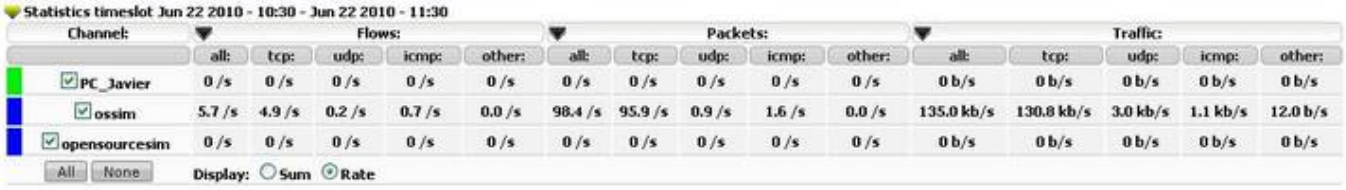


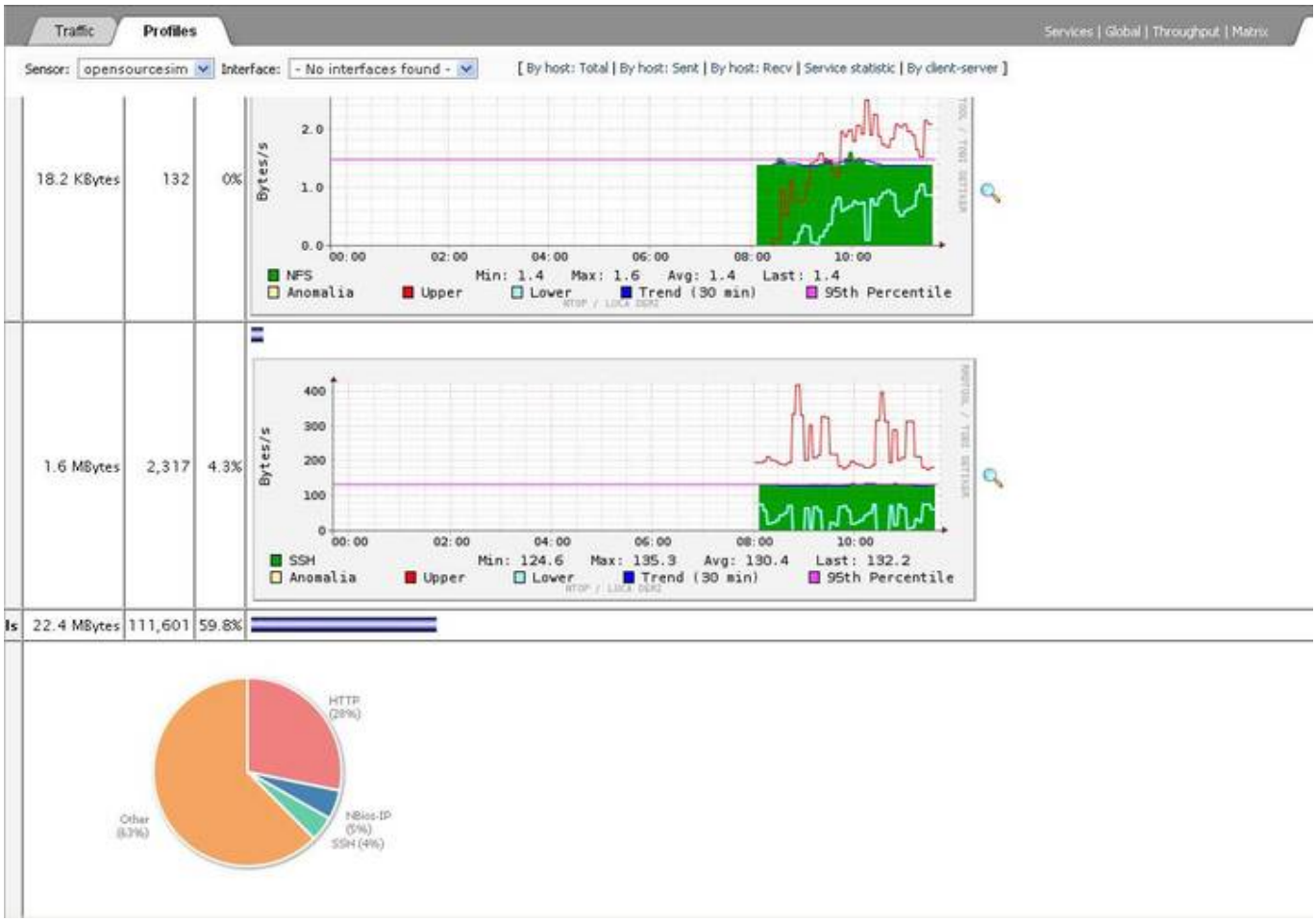
Reports –> Reports nos permite ver informes detallados. Si queremos ver el estado de la red, introducimos la red y le damos a **generate**. En **General Status** veremos la información general de la red. **Inventory** nos da el nombre de la red y la lista con todos los hosts. **Network Traffic** contiene una gráfica de la distribución de los servicios y los detalles del tráfico en la red, que incluye múltiples gráficas sobre servicios procesos. En **SIEM** tenemos los datos sobre los Tickets, las Alarmas, las Vulnerabilidades y los Eventos.





Si vamos por el apartado **Monitors -> Network**, en la pestaña **Traffic** veremos una gran cantidad de gráficas y en la pestaña **Profiles** tendremos gráficas con otros datos y opciones.



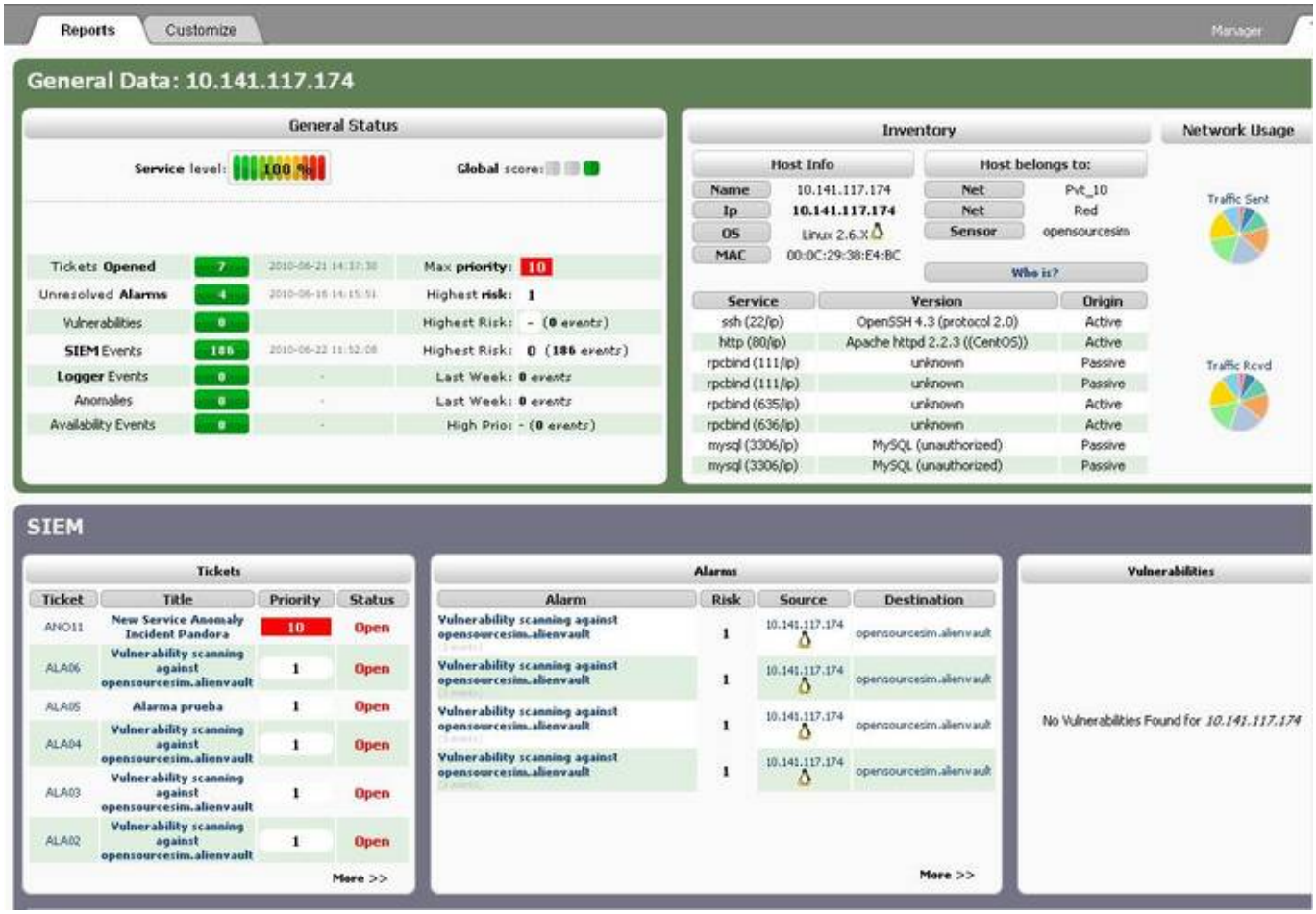


En **Assets -> Asset Search** podremos buscar los host pertenecientes a una red determinada, y si lo hacemos desde la pestaña **Advanced** tendremos mas opciones de búsqueda. En **Assets -> Assets**

–> Networks se pueden crear, modificar o borrar redes y también se le pueden dar nombres para identificarlas. Desde aquí se puede activar o desactivar el nagios para toda una red.

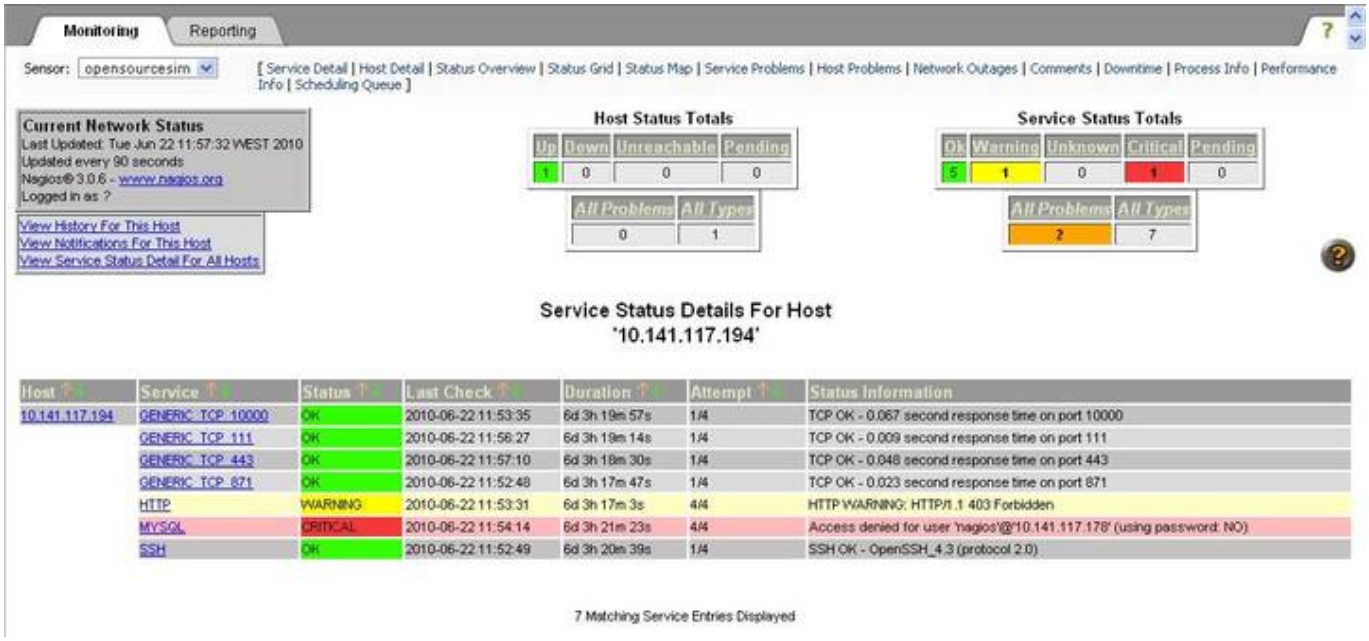
Visualizar datos de hosts

Reports –> Reports nos ayuda a buscar el host que queremos ver introduciendo su dirección ip y dándole a **generate**. En **General Status** veremos la información general del host. **Inventory** nos da toda su descripción como su nombre, el sistema operativo, los servicios que tiene y datos sobre ellos. En **SIEM** tenemos los datos sobre los Tickets, las Alarmas, las Vulnerabilidades y los Eventos sobre este host.

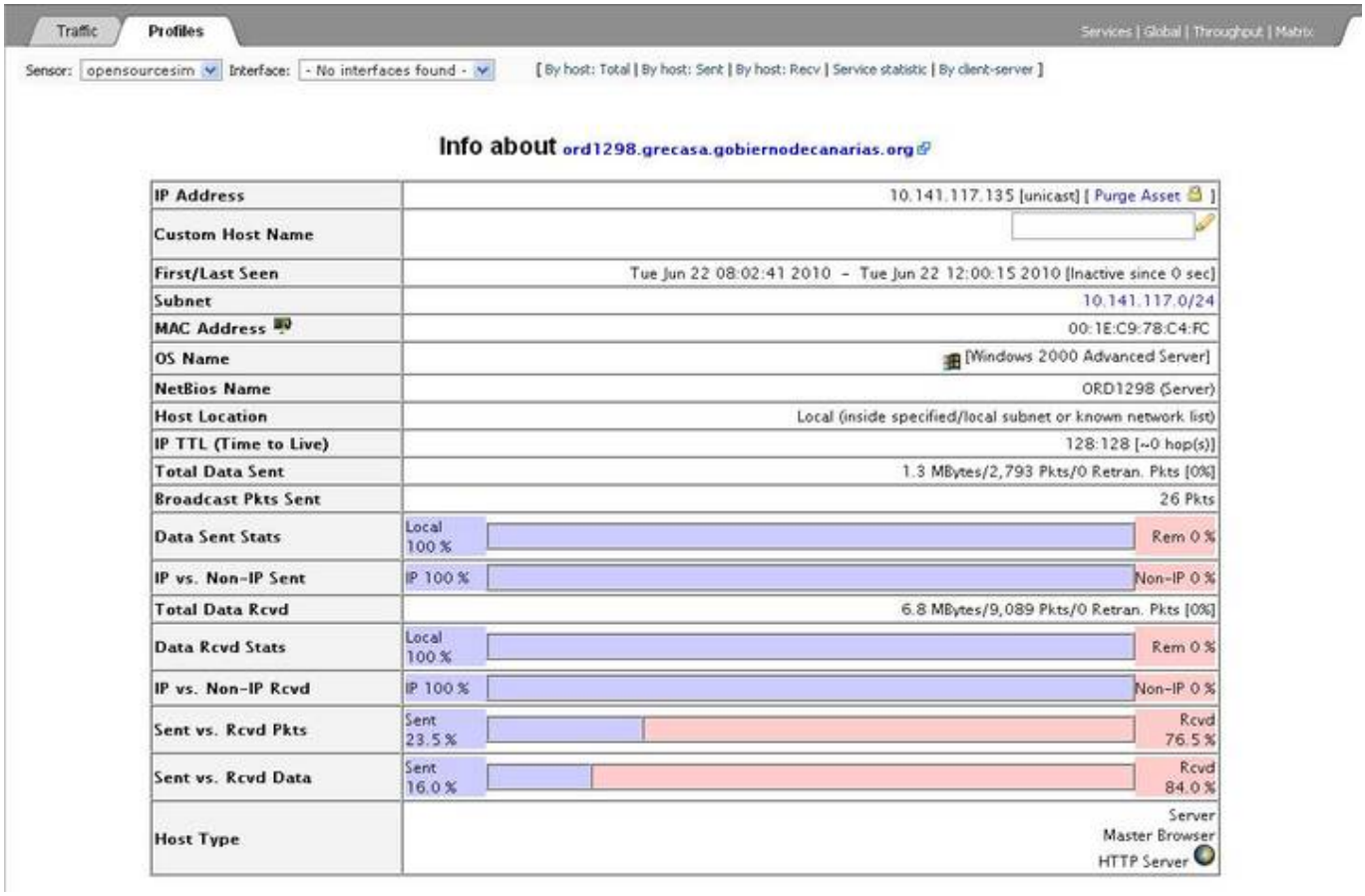


Assets –> Assets contiene la lista de hosts identificados. Si entramos en alguno de ellos nos llevará a sus detalles como en **Reports**.

En **Monitors –> Availability** tenemos la monitorización de los servicios hecha por nagios. Tiene varias opciones de agrupamiento y si hacemos click sobre un host podremos ver sus detalles. Desde aquí se puede hacer que deje de monitorizarlo. Dentro de la pestaña Reporting podemos crear informes sobre el host que se elija.



Si vamos por **Monitors –> Network** en la pestaña **Profiles** nos saldrá otras opciones. Entrando en **Summary –> Hosts** obtendremos la lista de los hosts. Entrando en ellos podremos ver mas información y gráficas.



Tickets

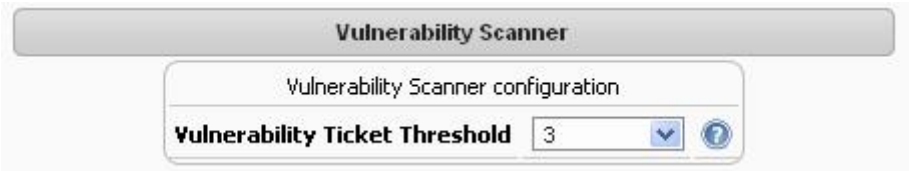
Introducción

Los tickets son tipos de incidencias que pueden ser configuradas para detectar lo que se quiera, alarmas, anomalías u otras.

Configuración general

Si se quiere que un ticket se abra automáticamente cuando se genera una alarma tenemos que tener la opción **Automatic Ticket Generation** habilitada, se encuentra en **Configuration –> Main.**

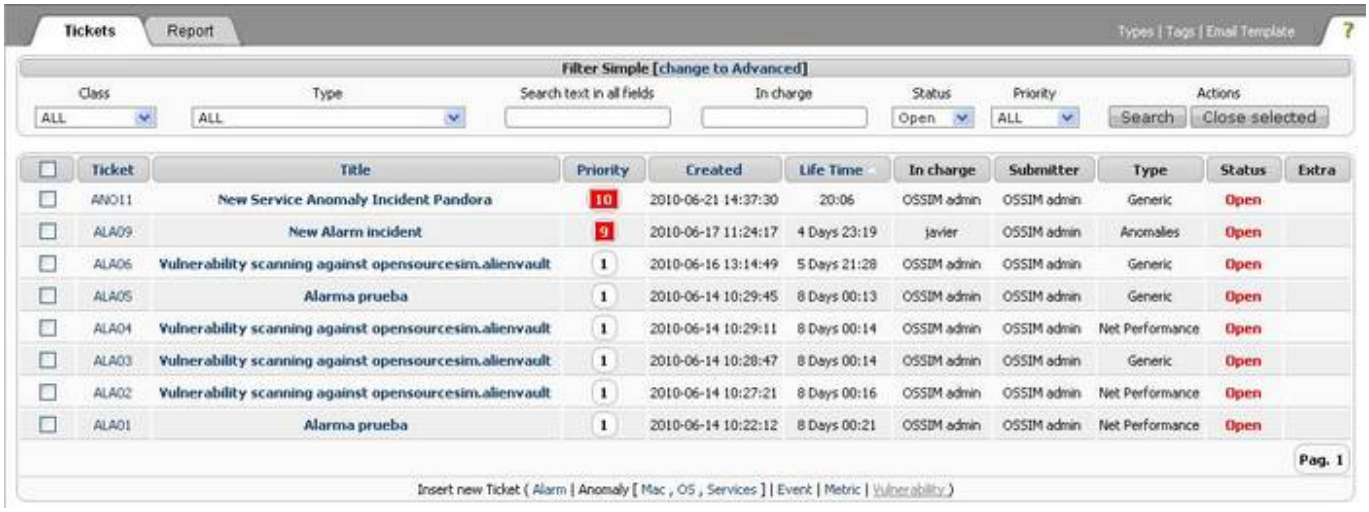
Cada vez que se encuentre una vulnerabilidad en el escaneo de un host se abrirá automáticamente un ticket. Se puede configurar el riesgo mínimo que tiene que tener una vulnerabilidad antes de que el ticket se abra. Para configurarlo ir a **Configuration –> Main** en el apartado **Vulnerability Scanner.**



Si el valor es demasiado bajo creará muchos tickets después de cada exploración de vulnerabilidad, con valor 3 o 4 sólo se abrirán tickets de vulnerabilidad reales, y no cuando sean identificados los servicios en la red.

Crear un ticket

Para crear un nuevo ticket vamos a **Incidents –> Tickets** y en la parte inferior se encuentra **Insert new Ticket** y los posibles tipos de ticket que se pueden crear.

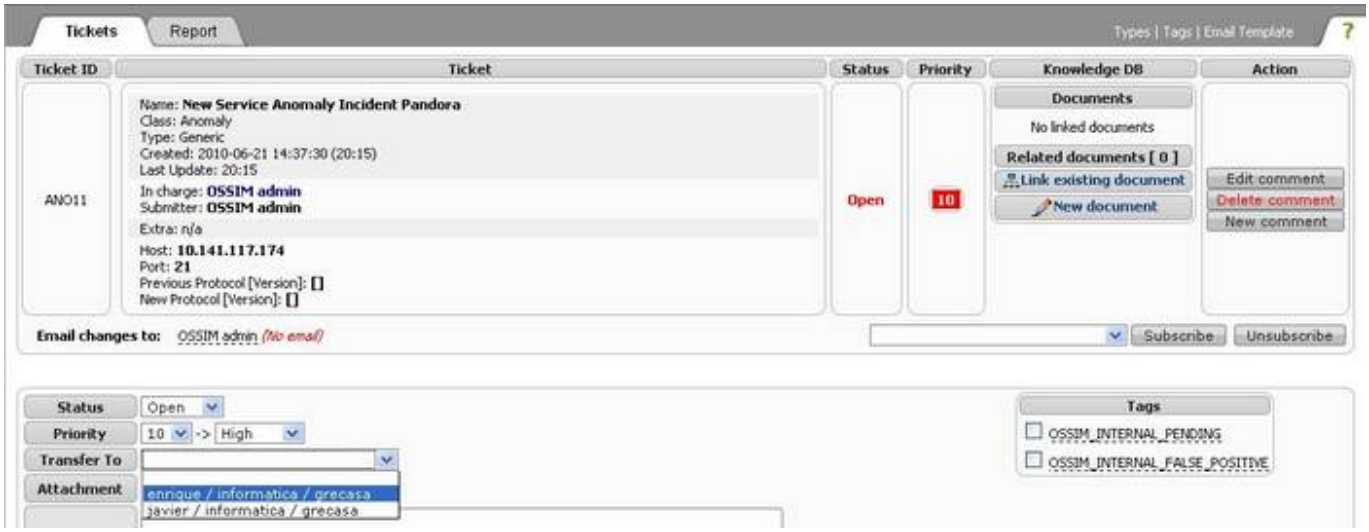


Modificar un ticket

Para modificar un ticket lo abrimos picando en su nombre o en su id en **Incidents –> Tickets.**

- **Vincular documentos.** En **Incidents –> Knowledge DB** podemos tener guardados documentos. Estos documentos pueden ser vinculados a tickets, por ejemplo un documento que explica como quitar un troyano conocido, un mapa de red o la lista de personas con las que hay que contactar cada vez que hay un determinado problema. Para vincular uno de estos documentos vamos a la opción **Link existing document** dentro del ticket al que se quiera vincular.

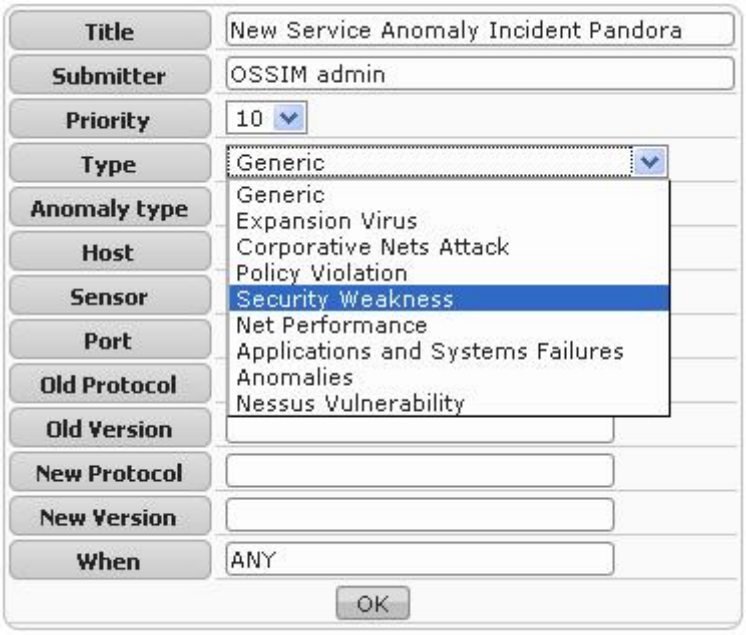
- **Transferir ticket.** Cuando un usuario crea un ticket puede transferírselo a otro usuario con la opción **Transfer to** dentro del ticket que se quiera transferir.



- **Adjuntar archivo.** A un ticket se le puede adjuntar algún archivo con la opción **Attachment.**
- **Subscribirse.** Con la opción **Subscribe/Unsubscribe** podremos recibir correos o dejar de recibirlos cada vez que cambia algo en el ticket. El formato del correo se puede modificar en la opción **Email Template** en la parte superior derecha.

- **Cerrar un ticket** Para cerrar o reabrir un ticket, cambiaremos la opción **Status** al estado en que se quiera tener, y se rellenarán los campos para explicar el motivo, por ejemplo puede ser cerrado porque se creó por un falso positivo y de esta manera no se abrirá en el futuro por este motivo.
- **Clasificarlos.** Para clasificar los tickets se pueden usar los tipos, que ya vienen definidos por defecto o pueden ser creados o modificados. Para crear, modificar o borrar algún tipo está la opción **Types** en la parte superior derecha. Para cambiar el tipo de un ticket ya creado tendremos que darle a la opción **Edit comment** dentro del ticket.

Ticket type	Description	Actions
Generic	--	--
Expansion Virus	--	[Modify] [Delete]
Corporative Nets Attack	--	[Modify] [Delete]
Policy Violation	--	[Modify] [Delete]
Security Weakness	--	[Modify] [Delete]
Net Performance	--	[Modify] [Delete]
Applications and Systems Failures	--	[Modify] [Delete]
Anomalies	--	[Modify] [Delete]
Nessus Vulnerability	--	--
Add new type		



- **Etiquetas.** Las etiquetas pueden agregar información al ticket de forma rápida. Para agregar nuevas etiquetas lo haremos en la opción **Tags**, en la parte superior derecha. Vienen dos etiquetas por defecto: **OSSIM_INTERNAL_PENDING.** Si esta etiqueta se fija, el escáner de vulnerabilidad no se abrirá de nuevo el mismo ticket. **OSSIM_FALSE_POSITIVE.** Si esta etiqueta está activa, la vulnerabilidad se marcará como un falso positivo y no se volverá a abrir en un futuro análisis.

Errores

No carga la página. Puede ser que el apache esté caído. Reiniciar el servidor apache:

```
# /etc/init.d/apache2 start
```

Referencias

- http://www.openredes.com/category/alienvault-usm-ossim/manuales-ejemplos-alienvault-usm-ossim/
- http://ossim.net/dokuwiki/doku.php?id=user_manual:incidents:tickets
- página principal http://www.ossim.net/
- Descargar desde http://www.ossim.com/home.php?id=download
- foro http://www.ossim.net/forum/
- turoriales http://www.alienvault.com/blog/dk/ossim/tutorials/index
- http://windowsitpro.com/article/articleid/99992/analyze-network-events-with-ossim-toolset.html