# Bitácora Instalación Suricata sobre Raspbian

## Instalación Suricata IoT

1. Lista que librerías para instalar sobre SO:

sudo apt-get -y install libpcre3 libpcre3-dbg libpcre3-dev \

build-essential autoconf automake libtool libpcap-dev libnet1-dev \

libyaml-0-2 libyaml-dev pkg-config zlib1g zlib1g-dev libcap-ng-dev libcap-ng0 \

make libmagic-dev libjansson-dev

wget https://github.com/OISF/libhtp/archive/0.5.21.tar.gz

tar -xzvf 0.5.21.tar.gz

cd libhtp

./autogen.sh

./configure

make

make install

ldconfig

1. Descargar comprimido de Suricata:

git clone https://github.com/decanio/suricata-IoT.git

1. Entrar a la carpeta de suricata:

cd suricata-3.1

1. Instalar:

./autogen.sh

./configure && make && make install-full

ldconfig

1. Copiar archivos de configuración:

mkdir /var/log/suricata

mkdir /etc/suricata

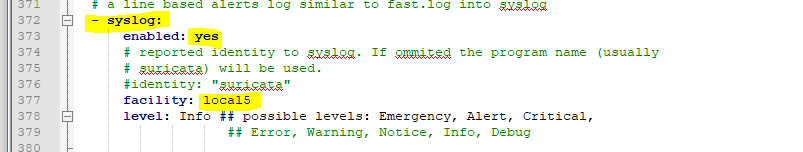
mkdir /etc/suricata/rules

cp classification.config /etc/suricata

cp reference.config /etc/suricata

cp suricata.yaml /etc/suricata

1. Habilitar el envió de alertas al servicio syslog para enviar alertas a OSSIM, editar archivo “suricata.yaml”:



1. Incluir el envió de alertas de Suricata que tiene como prefijo “local5” por el servicio Syslog, incluir la siguiente línea en el archivo /etc/rsyslog.conf:

[\*.local5@ip\_servidor\_OSSIM:puerto](mailto:*.local5@ip_servidor_OSSIM:puerto)

1. Reiniciar servicio rsyslog:

sudo service rsyslog restart

1. Bajar reglas (por defecto se bajan por Oinkmaster):

apt-get install oinkmaster

editar el archivo oinkmaster.conf: /etc/oinkmaster.conf

adicionar línea:

url = <http://rules.emergingthreats.net/open/suricata/emerging.rules.tar.gz>

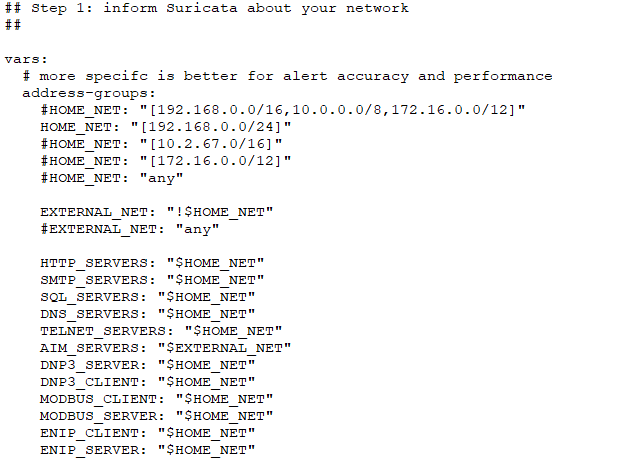
comando: oinkmaster -C /etc/oinkmaster.conf -o /etc/suricata/rules

1. Correr Suricata:

suricata -c /etc/suricata/suricata.yaml -i eth0 --init-errors-fatal

## Archivo de configuración suricata.yaml

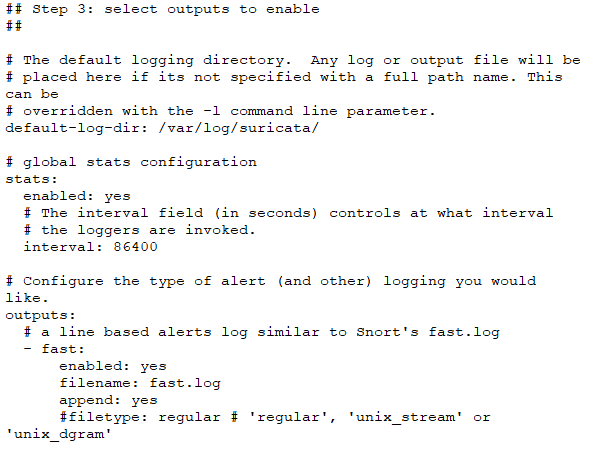
El archivo de configuración de Suricata IoT es el archivo llamado suricata.yaml, este contiene los parámetros para correr el suricata, las partes principales de este archivo están en la configuración de la red, en donde se identifica la red local y la red externa, y las reglas que se quieren aplicar.



En esta parte del archivo de configuración suricata.yaml sirve para configurar las propiedades de la red en donde está el dispositivo centinela, en tal caso, se define la variable de “HOME\_NET”, en donde se coloca el identificador de red y la máscara, como lo muestra la imagen, de igual modo, se puede configurar otro tipo de variable en donde se encuentran algunos servicios de red como el servidor HTTP o el DNS.



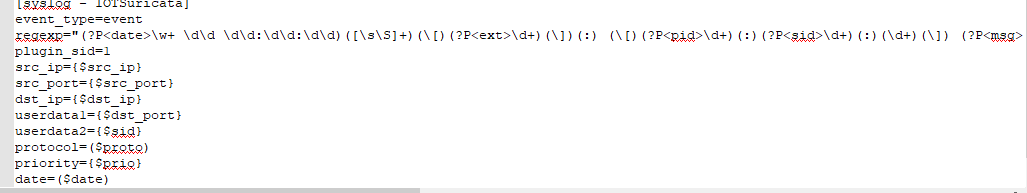
En este punto del archivo de configuración suricata.yaml permite escoger las reglas que van a ser revisadas por el software Suricata, en este punto se debe ver que cada archivo de reglas tiene un esquema de nombre\_del\_archivo.rules, en donde el nombre describe el paquete de reglas de se evalúan. Por otro lado, también se configura la ubicación en donde se encuentran las reglas, esta configuración se ve en la asignación de la variable “default-rule-path”.



Por último, en esta parte del archivo de configuración suricata.yaml permite configurar las diferentes salidas de reportes de alertas o avisos que emite el sistema, como muestra la imagen permite configurar un archivo de estadísticas, al colocar el campo de “enables” en “yes” se toma que se quiere un archivo de reporte de estadísticas cada cierto tiempo definido en la variable “Interval”. Todos estos archivos de reportes se pueden consultar en la ruta colocada en la variable de “default-log-dir”.

## Archivo plugin para OSSIM.

El archivo de plugin para OSSIM es el archivo llamado SuricataIoT.cfg, este archivo contiene las especificaciones de la expresión regular que permite al OSSIM entender los eventos generados por esta herramienta.



Con este archivo de plugin el sistema OSSIM reconoce los mensajes del protocolo syslog que tienen específicamente el formato determinado por la expresión regular ya mencionada, de tal forma que nos permite obtener información importante para determinar el tipo de tráfico malicioso, para ello OSSIM permite declarar variables tomadas de la expresión regular las cuales son las siguientes:

* src\_ip, esta variable contiene la ip fuente del tráfico identificado como malicioso.
* src\_port, esta variable contiene el puerto fuente del tráfico malicioso.
* dst\_ip, esta variable contiene la ip de destino del tráfico malicioso.
* userdata\_1, esta variable contiene el puerto destino del tráfico malicioso.
* userdata\_2, esta variable contiene el número de identificación de la regla Suricata que se envía.
* priority, esta variable contiene el número de prioridad definida en la regla Suricata del tráfico malicioso.

## Probar Suricata

1. Para probar Suricata corremos el comando en la terminal:

suricata -c /etc/suricata/suricata.yaml -i eth0 --init-errors-fatal

1. Una vez comience a correr el mismo sistema empieza a examinar los paquetes de la red en busca que coincida con alguna regla.
2. De haber un paquete que coincida con alguna regla de Suricata y se genere una alerta Suricata, el sistema automáticamente lo enviará al servidor OSSIM y lo entenderá como un mensaje de alerta Suricata.

