# Bitácora Instalación Suricata sobre Raspbian

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. 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