**Instalación Snort3 en server CentOS Stream 8**

Se han instalado los siguientes paquetes:

epel-release, libpcap-devel, pcre-devel, libdnet-devel, hwloc-devel, openssl-devel, zlib-devel, luajit-devel, pkgconf, libmnl-devel, libunwind-devel, libnfnetlink-devel, libnetfilter\_queue-devel, hyperscan hyperscan-devel, xz-devel libuuid-devel, libsafec libsafec-devel, gperftools-devel, perl-LWP-UserAgent-Determined perl-Net-SSLeay perl-LWP-Protocol-https perl-SysSyslog perl-Archive-Tar

Se ha instalado la última versión de libDAQ y Flatbuffers

Snort está instalado en /usr/local/snort/bin/snort (**/usr/local/snort/bin/snort –V** para comprobar la versión).

Los archivos de configuración se encuentran en:

* /usr/local/snort/etc/snort/snort.lua
* /usr/local/snort/etc/snort/snort\_defaults.lua

Las reglas se encuentran en /usr/local/snort/rules/ , donde están los distintos archivos de reglas, que se encuentran todas juntas en un mismo archivo llamado snort.rules

Las listas blanca y negra se encuentran en /usr/local/snort/Intel/

La AppID (odp) se encuentra en /usr/local/snort/appid

Se ha instalado el módulo para alertas rápidas, que son almacenadas en /var/log/snort/

Se ha instalado como servicio la última versión de PulledPork, que permite que la reglas se actualicen, así como un timer para que se active automáticamente de forma periódica cada noche a las 00:10.

El OinkCode para la descarga de reglas es el siguiente:  
- 648d0cfc6cbf9735d349c3457d40c408687f6357

Para iniciar Snort, se utiliza el siguiente comando:

**/usr/local/snort/bin/snort -c /usr/local/snort/etc/snort/snort.lua –R /usr/local/snort/rules/snort.rules -i enp4s0 -A alert\_fast -s 65535 -k none**

De esta forma, Snort empezará a registrar las conexiones que se realicen a través de la interfaz, que en este caso es **enp4s0**, y guardará la información en /var/log/snort/

Se ha credo el servicio snort.service , que es ejecutado por el también creado usuario snort:snort

La instalación y configuración se han hecho siguiendo la siguiente guía:

<https://snort-org-site.s3.amazonaws.com/production/document_files/files/000/003/977/original/Snort_3_GA_on_CentOS_8_Stream.pdf>