SNORT

01 COMO INSTALAR SNORT

Windows: Para instalar SNORT en Windows tenemos que irnos a la página de SNORT y descargarnos el programa .exe.

Linux: En Linux tenemos dos maneras de instalar SNORT:

1. Desde la terminal con el comando apt-get install snort
2. Llendo a la página oficial de SNORT e instalandonos los .tar.gz.

CONFIGURACIÓN 02

Mientras se nos este instalando SNORT nos saltara la configuración, en la cual tenderemos que poner el nombre de la tarjeta de red la cual queremos que nos escanee y después nos pedirá la dirección de red de nuestra LAN.

03 AÑADIR REGLAS

Dentro de la carpeta de SNORT tenemos una carpeta llamada rules y en fichero local.rules ponemos las reglas siguiendo este orden:

1. Acción de la regla
2. Protocolo
3. Dirección IP origen
4. Puerto Origen
5. Dirección de la operación: -> o <-
6. Dirección IP Destino
7. Puerto Destino
8. Opciones (tienen que ir entre paréntesis):
   msg, flags, ack, reference, classtype, sid o rev.