Indice

[IDS 1](#_Toc507269129)

[Snort Linux 1](#_Toc507269130)

[Suricata windows 9](#_Toc507269131)

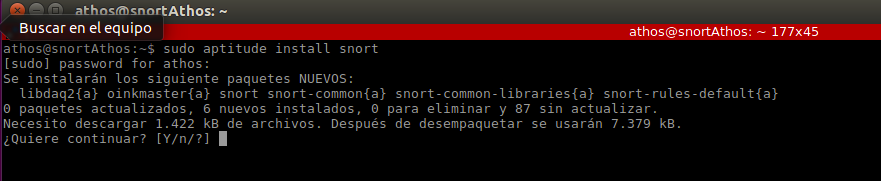
# IDS

Un ids es un sistema de detección de intrusos. Monitoriza la red para buscar ciertos patrones, y genera alertas que luego podremos comprobar para ver si algún tipo de ataque se esta produciendo.

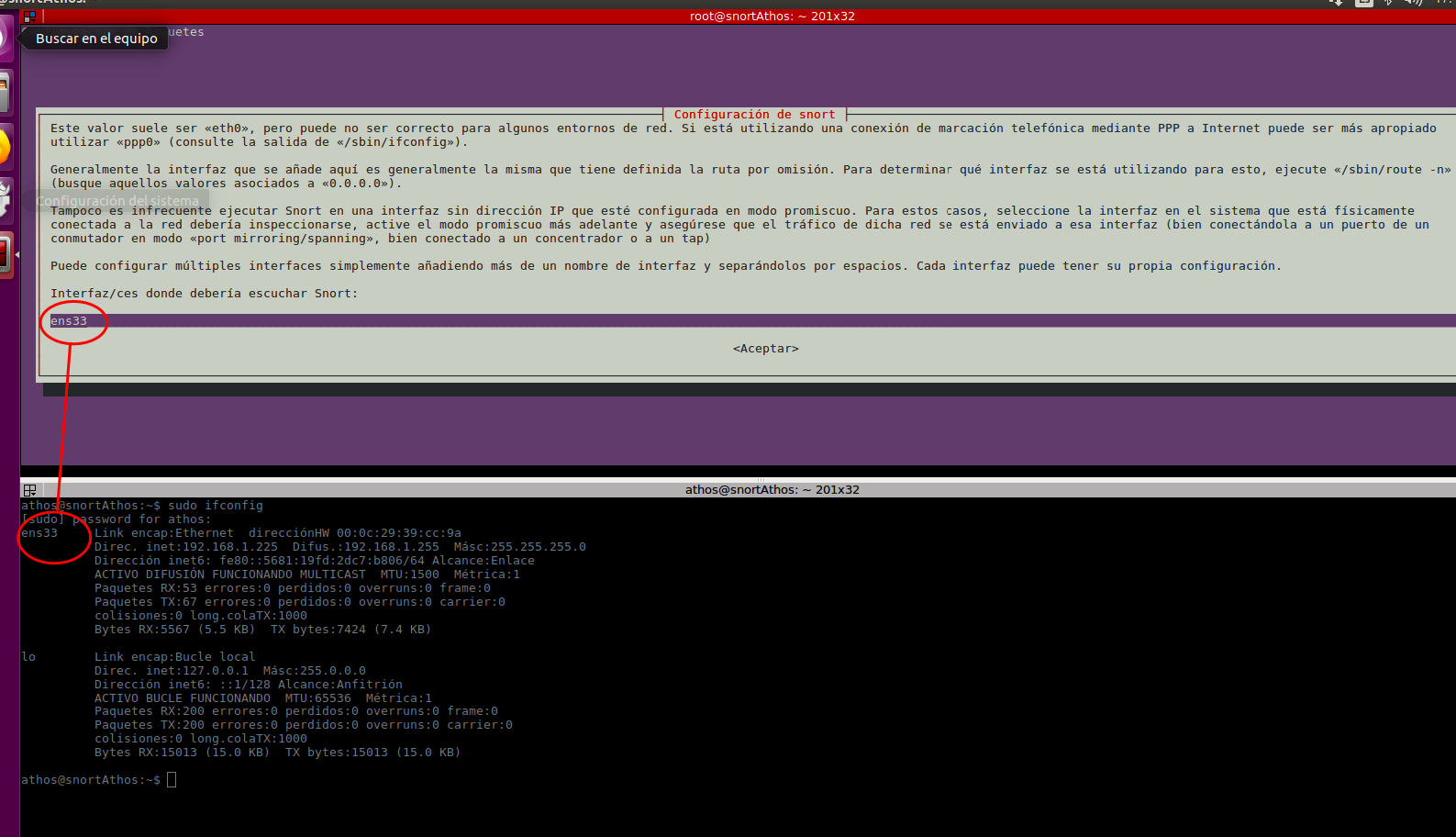
En esta practica vamos a probar dos, Snort en Linux y Suricata en windows. Ambos programas son multiplataforma y podemos usarlos tanto en Linux como en windows. Usaremos diferentes sistemas operativos para dar un poco de variedad a este documento.

# Snort Linux

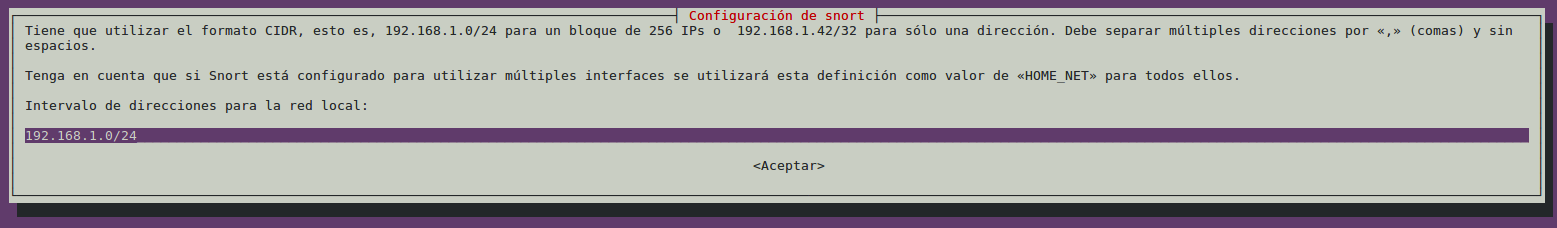
Instalamos Snort con el siguiente comando:



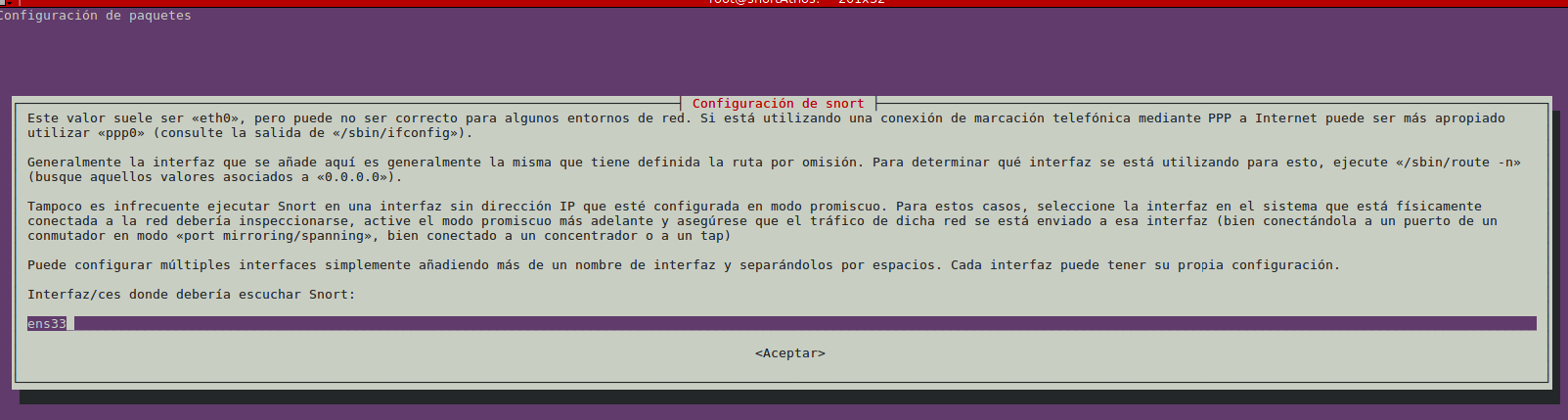
Comprobamos cual es el nombre de nuestra tarjeta de red y lo introducimos en el asistente de configuración de snort



Ahora nos pregunta que red queremos monitorizar.

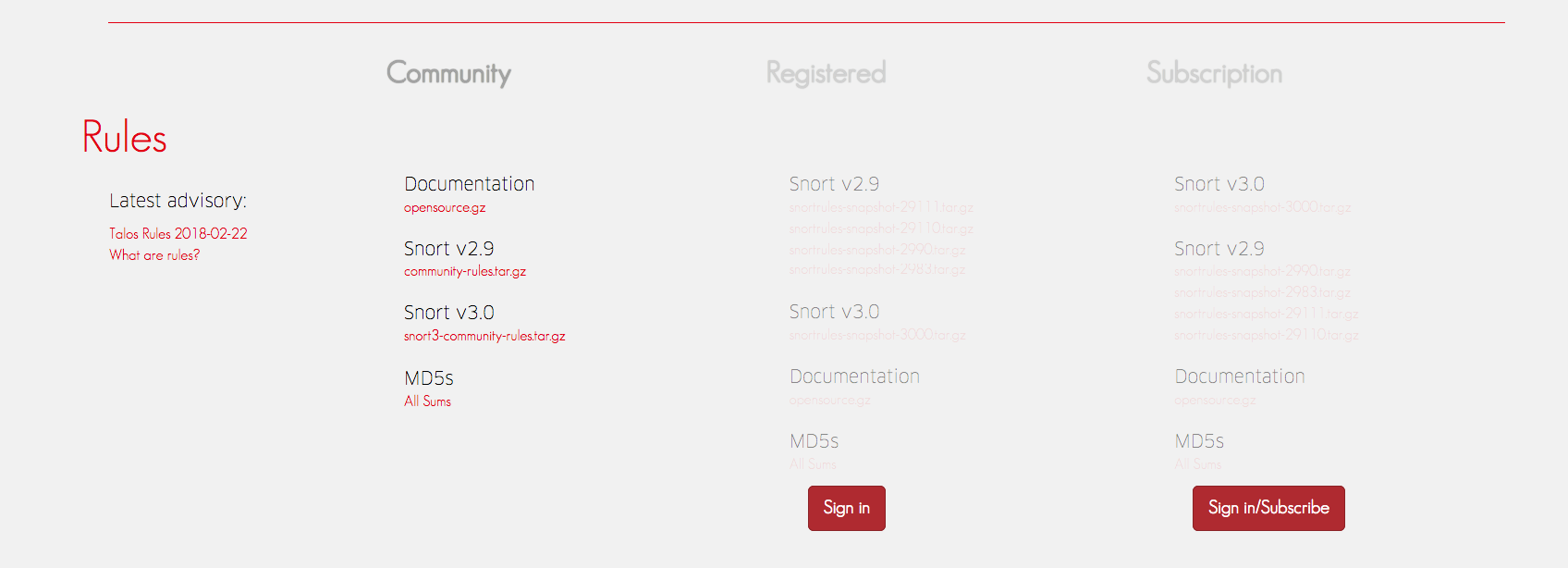


Nos vuelve a preguntar donde debería escuchar snort



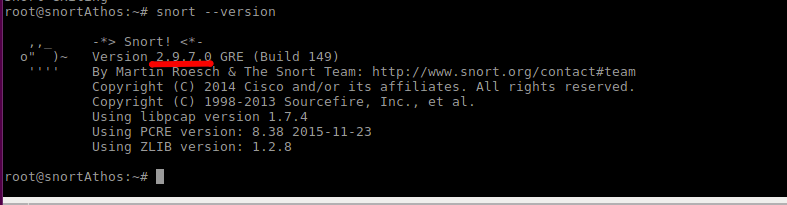
Ahora vamos a establecer las reglas que debe aplicar snort. Para esto podemos ir a la pagina de snort y descargar las reglas de la comunidad, o podríamos crear nuestras propias reglas.

Vamos a la pagina de snort y miramos en la sección de descargas a ver que encontramos.

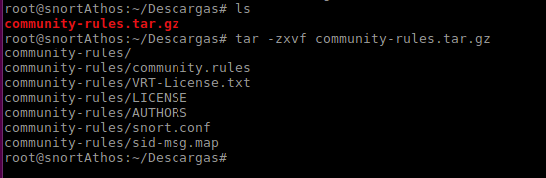


Vemos que tenemos reglas para la versión 2.9 de snort y para la versión 3.0.

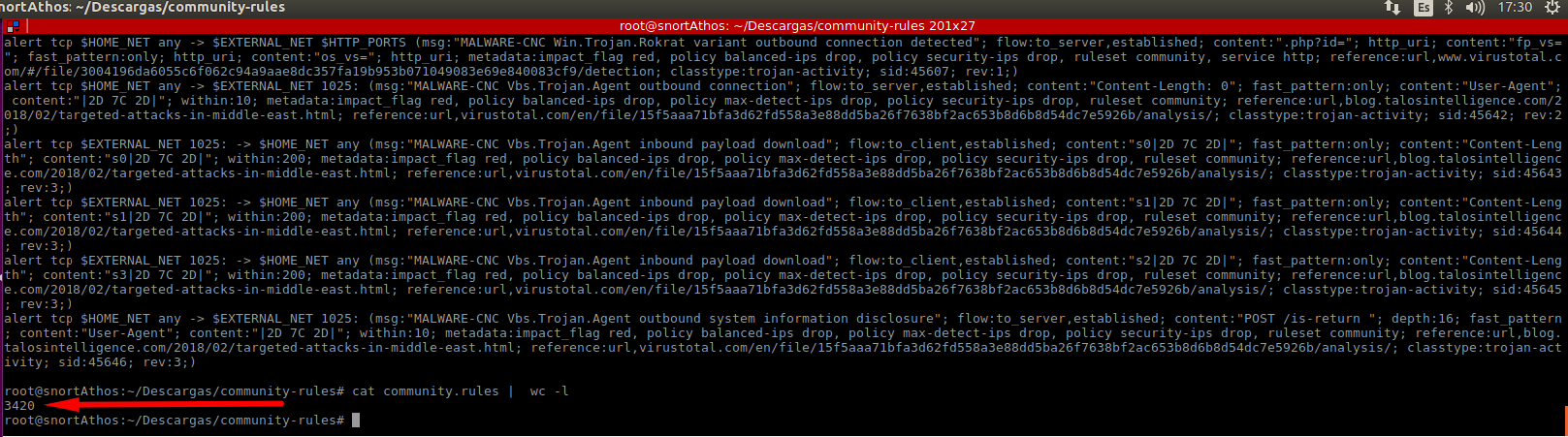
Vamos a comprobar que versión de snort tenemos instalada en nuestra maquina.



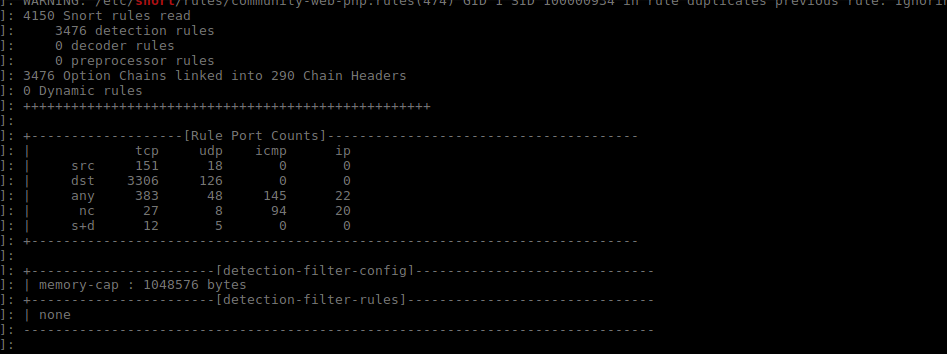
Como tenemos la versión 2.9 vamos a descargarnos esas reglas.



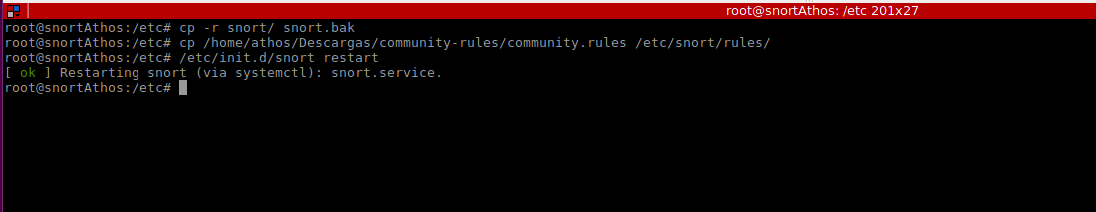
Como podemos ver en la siguiente imagen, snort (o su comunidad) nos provee de un gran numero de reglas que podemos aplicar, estas reglas son las habituales que suele necesitar un ids, así que vamos a aplicarlas



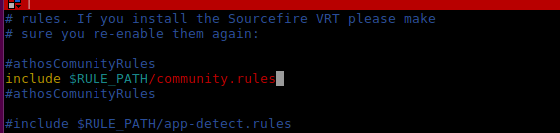
Antes de aplicar las reglas que nos hemos descargado, reiniciamos snort y miramos en el archivo /var/log/syslog las líneas cuyo contenido es snort para ver las reglas que esta aplicando



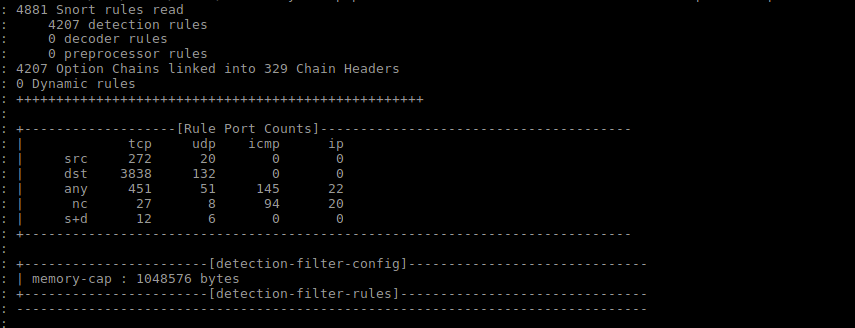
Ahora vamos a introducir nuestro archivo de reglas de la comunidad en la carpeta /etc/snort/rules, pero antes haremos una copia de seguridad de toda la carpeta /etc/snort por si acaso.



En el archivo de configuración snort.conf, añadimos la regla que acabamos de copiar al directorio rules

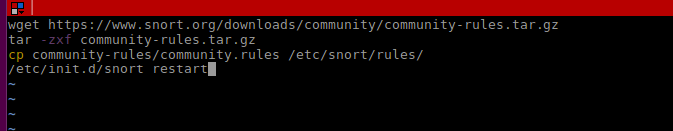


Y volvemos a mirar el syslog con cat /var/log/syslog |grep snort



Esta vez, tenemos 4881 reglas en vez de 4150.

Si quisiéramos automatizar la actualización de las reglas creadas por la comunidad podríamos crear un script parecido a este

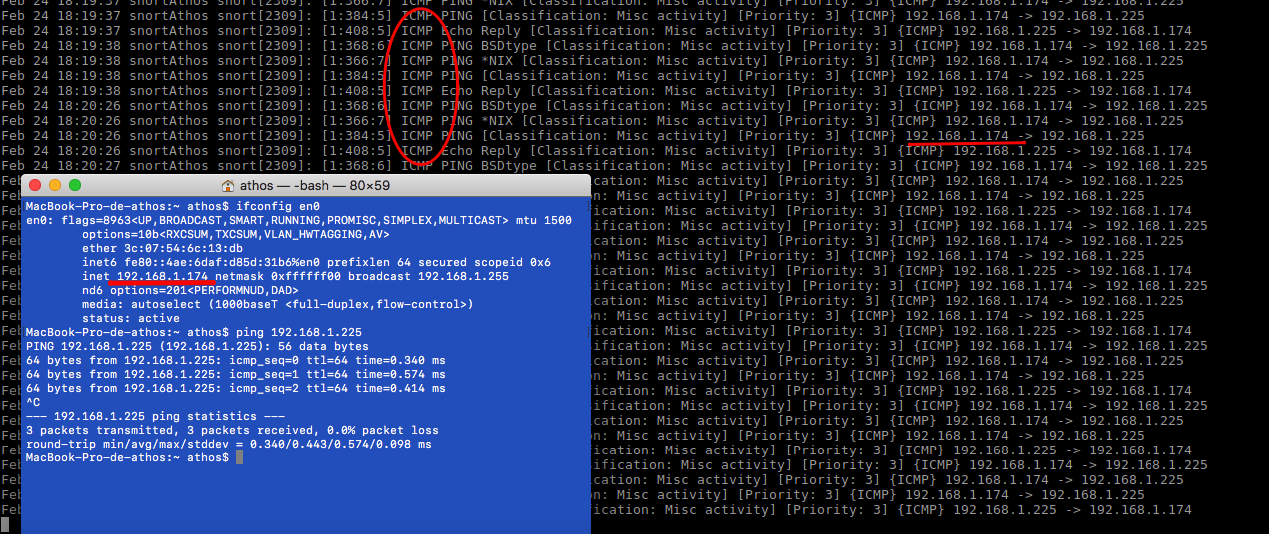


Y añadirlo a una tarea de cron para que se ejecutase de forma periódica.

Modificamos el archivo snort.conf y añadimos la siguiente línea para poder ver los logs en texto plano en el log syslog y empezamos a hacer pruebas



Primero vamos a hacer un ping



Como vemos, desde otra maquina, hacemos pings, y el snort lo detecta.

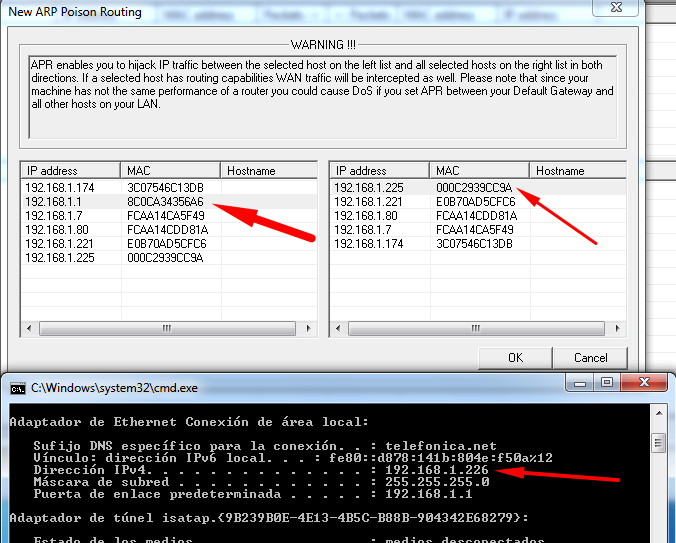
Ahora vamos a intentar hacer un arp spoofing con cain y abel.

En la siguiente imagen, podemos comprobar las ips de cada uno de los dispositivos involucrados en la poc.

192.168.1.1 router

192.168.1.225 victima (con snort corriendo)

192.168.1.226 atacante (ejecutando cain&abel)



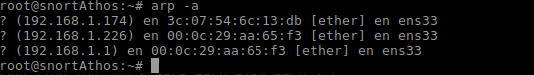
Nuestro snort, no detecta un intento de envenenamiento arp, así que tendremos que poner una regla para que lo detecte.

Haciendo una búsqueda en el archivo de configuración por arp encontramos lo siguiente

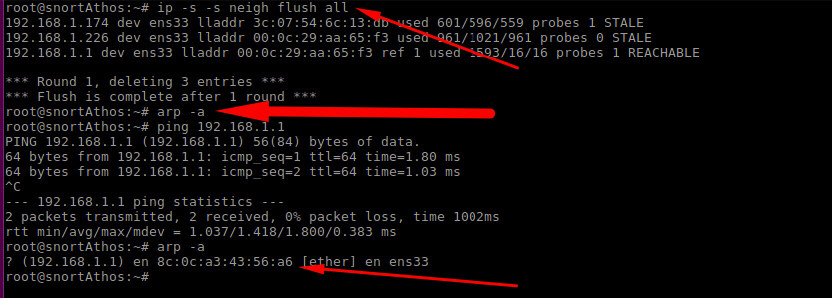


Vemos que hay una regla comentada, así que vamos a editarla y vemos que pasa.

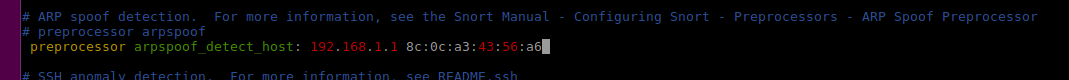
Cuando voy a mirar en la maquina snort cual es la ip REAL del router para añadirlo a nuestra regla, me doy cuenta de que del intento anterior, tenemos la tabla arp envenenada



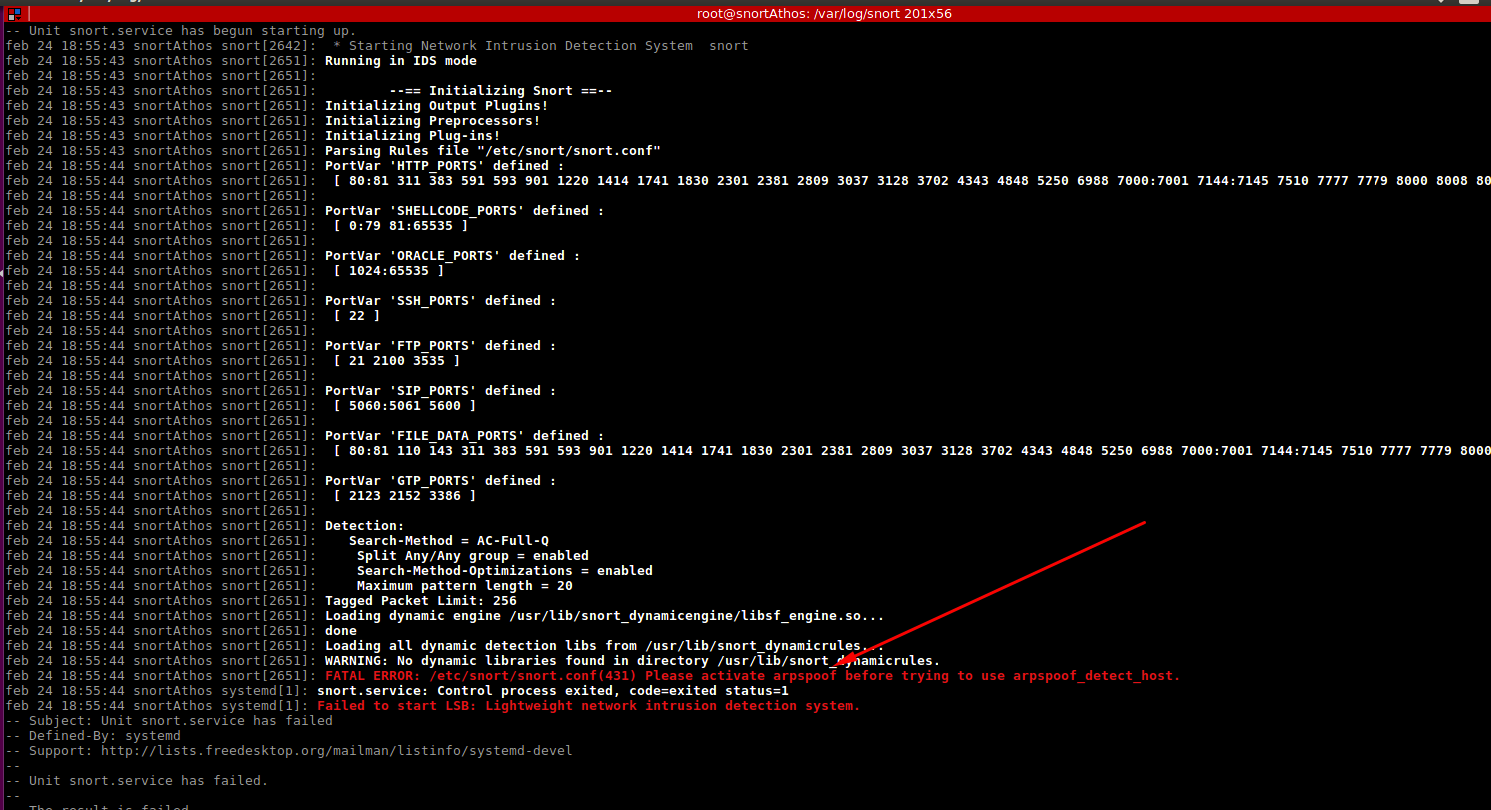
Así, que vamos a eliminar toda la tabla arp y haremos un ping al router para obtener la mac real y añadirla a nuestra regla



Ahora que ya tenemos la mac real de nuestro router, guardamos la regla y reiniciamos snort

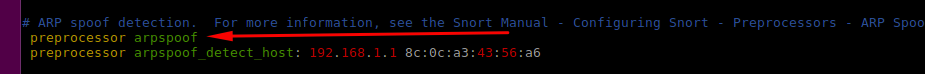


Al reiniciar snort, nos da un error



Nos dice que tenemos que activar arpspoof antes de usar arpspoof\_detect\_host

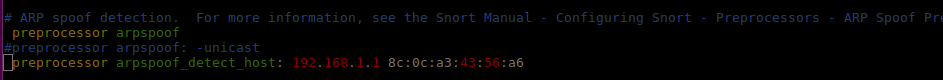
Así que revisamos el archivo de configuración y vemos que nos habíamos dejado de descomentar esa línea. Al final lo tenemos que dejar como en la siguiente imagen



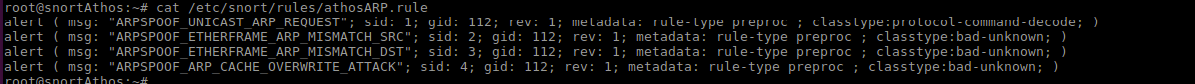
Reiniciamos snort, y vamos a volver a hacer la prueba de envenenamiento arp.

Bueno, pues seguimos sin que esto funcione, así que lo vamos a configurar de otra forma.

La configuración de la imagen anterior la vamos a cambiar por la siguiente



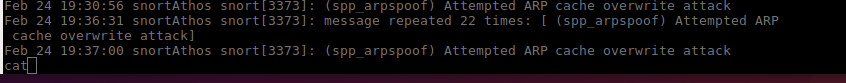
También crearemos un nuevo fichero con las siguientes reglas.



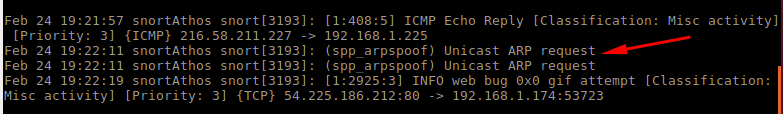
Y en el archivo de configuración cargaremos el nuevo archivo de reglas

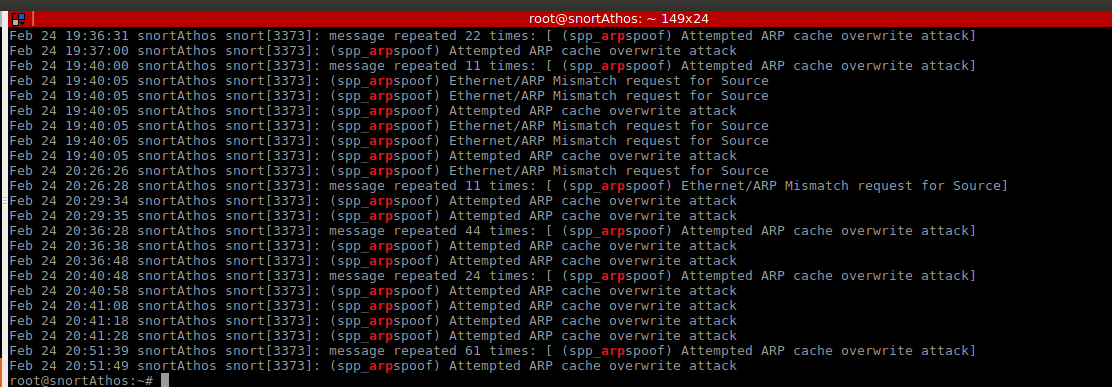
ç

Ahora reiniciamos el snort y volvemos a probar

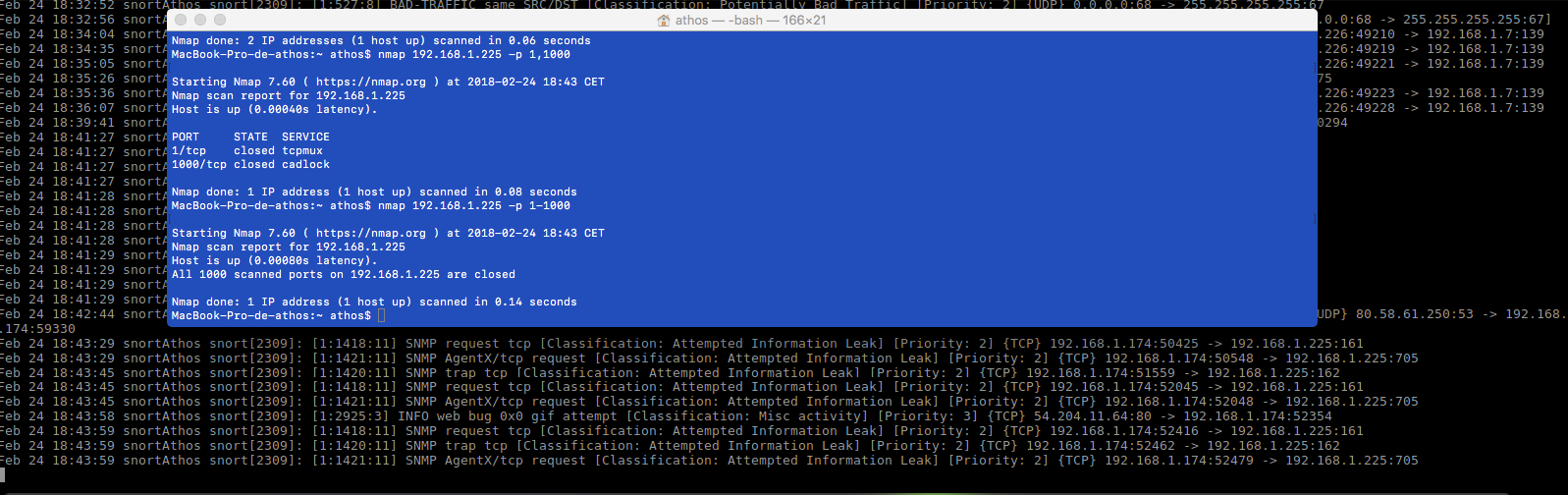


Ahora si que vemos que detecta los ataques de arp spoofing





Vamos a hacer un escaneo de puerto con nmap para ver si esto lo detecta snort.

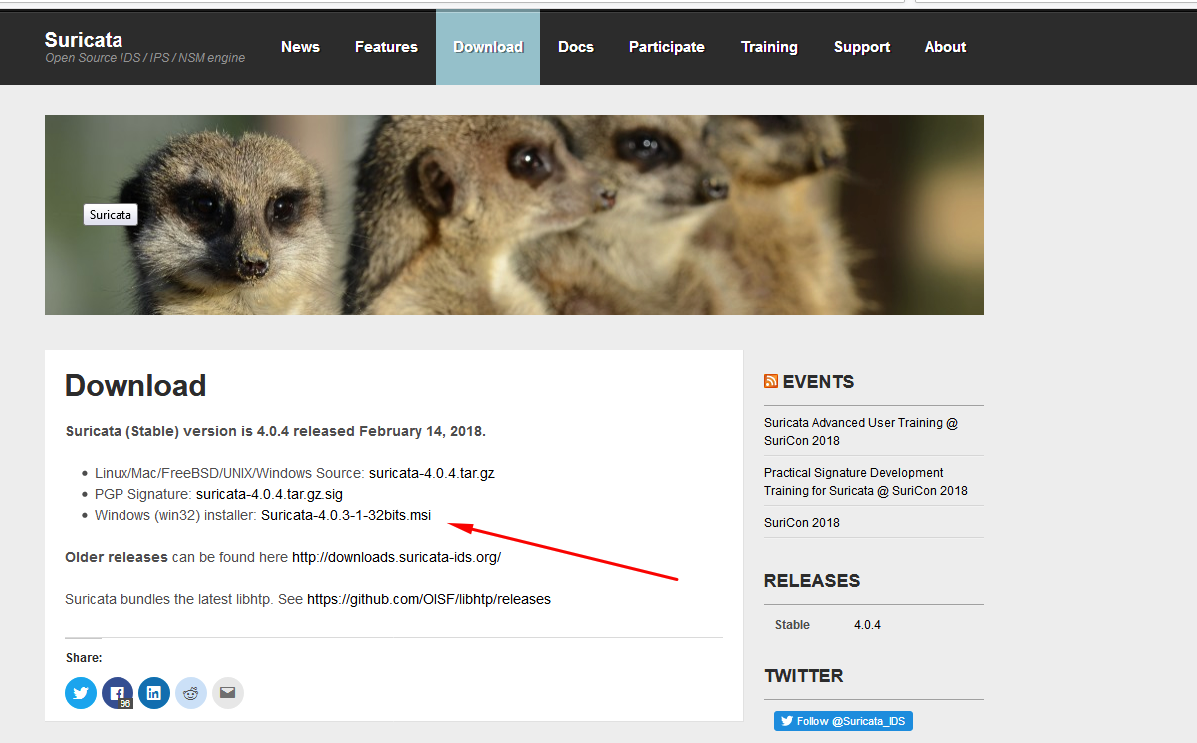


Y como podemos ver, si que detecta el escaneo de puertos, catalogándolo como intento de obtención de información.

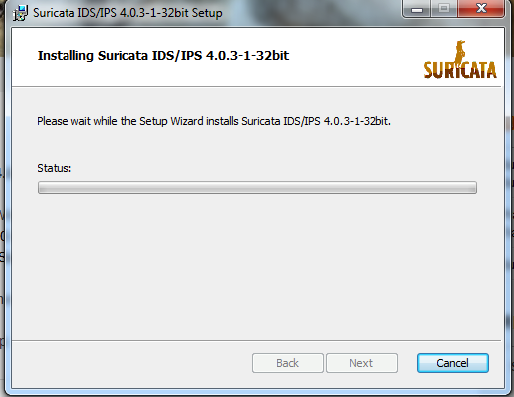
# Suricata windows

Vamos a probar otro ids. Esta vez utilizaremos suricata y lo probaremos en windows.

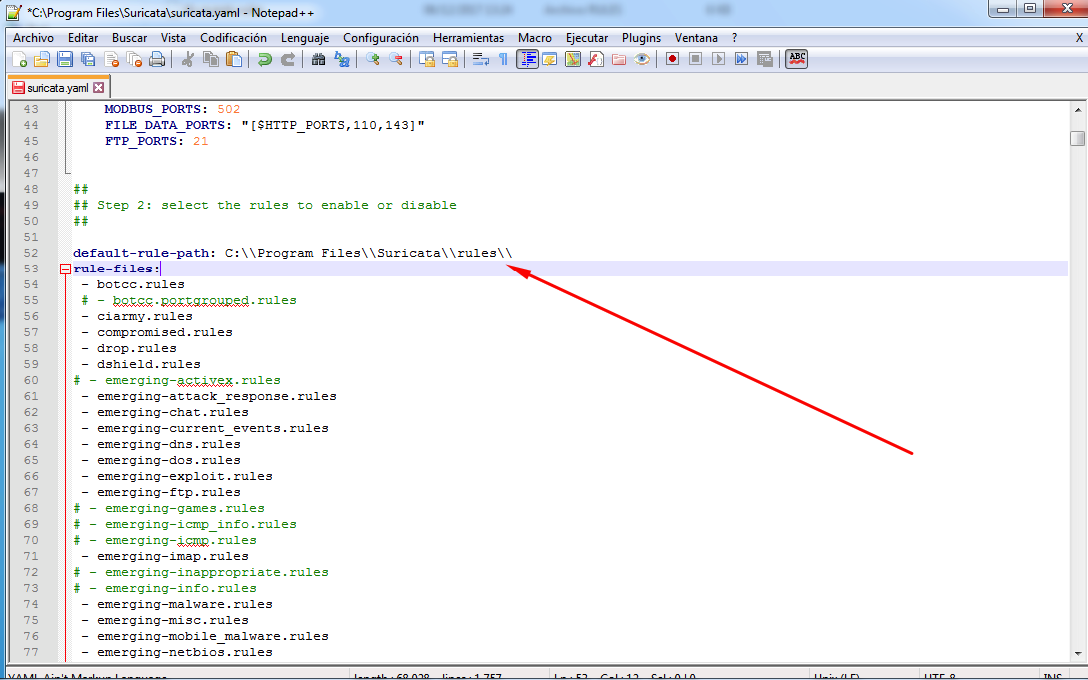
Vamos a su pagina oficial y lo descargamos



La instalación es como cualquier programa normal.

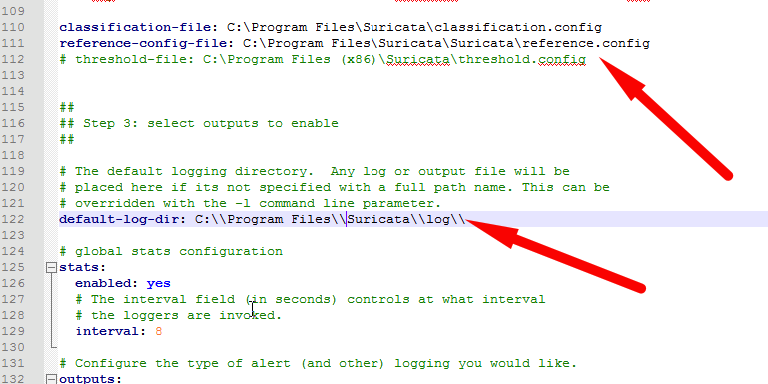


Lo primero que vamos a hacer es editar el archivo de configuración

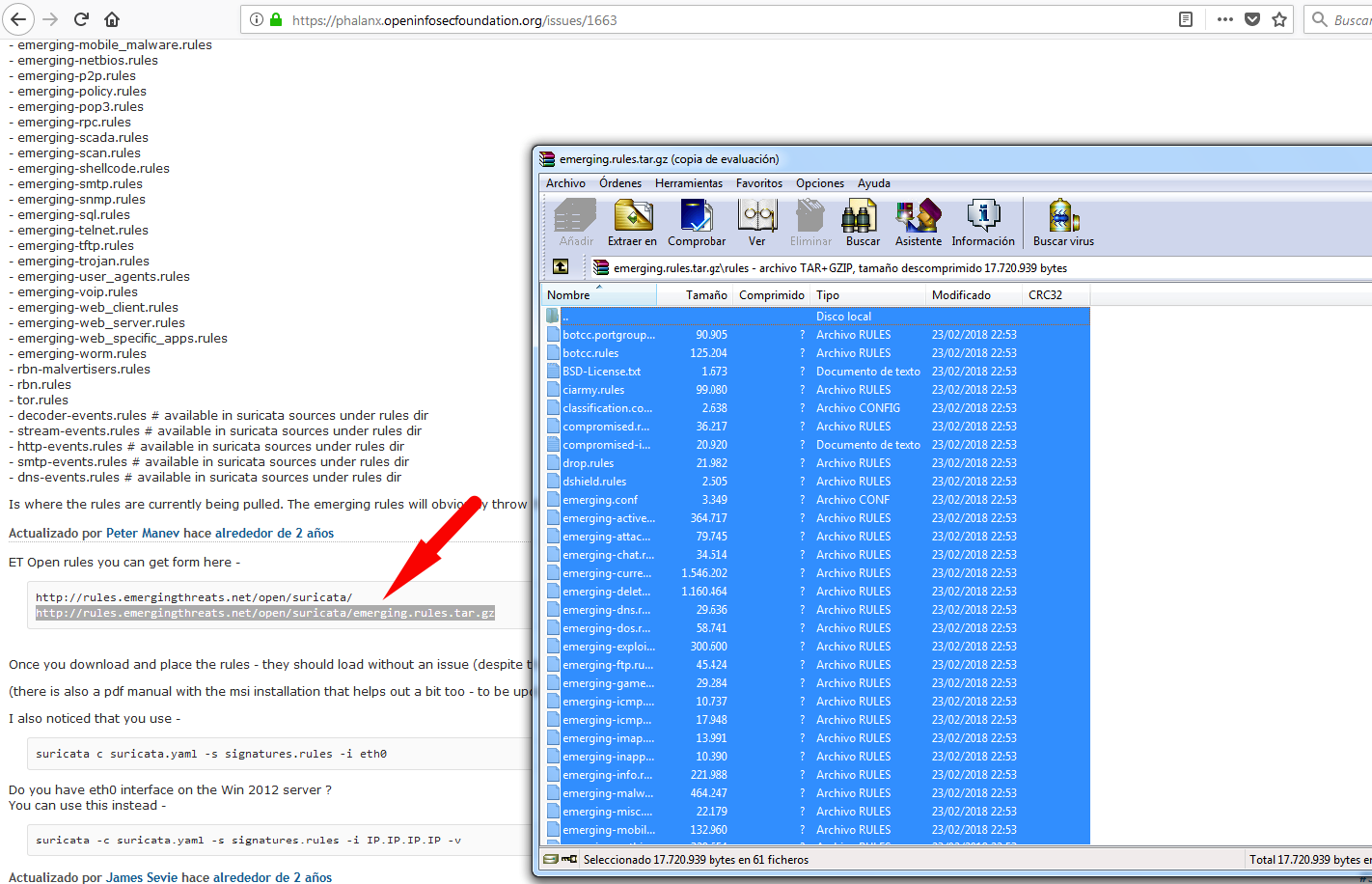


Cambiaremos la directiva default-rule-path y pondremos la correcta como se ve en la imagen (por defecto venia la ruta mal)

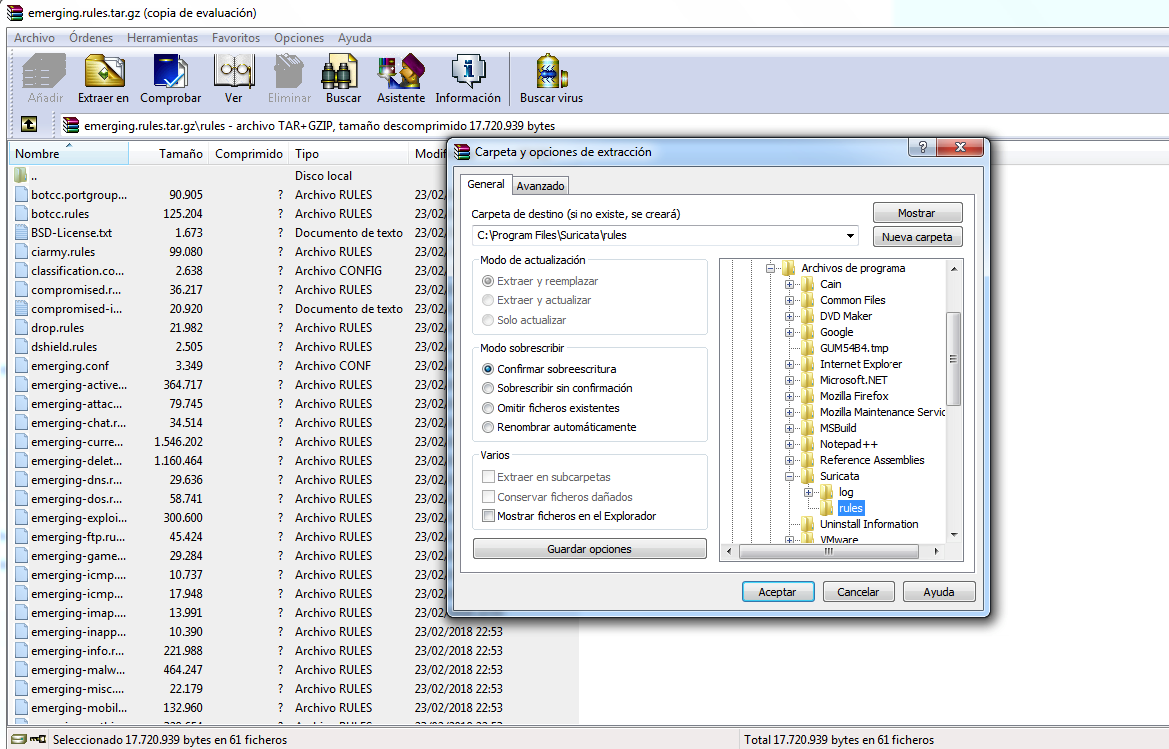
También modificaremos estas dos rutas



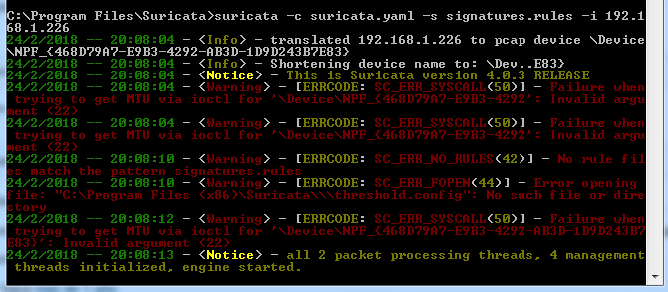
Después de configurar las rutas de forma correcta, podemos optar por descargarnos reglas que están a disposición de la comunidad.

Podemos verlo en las siguientes imágenes

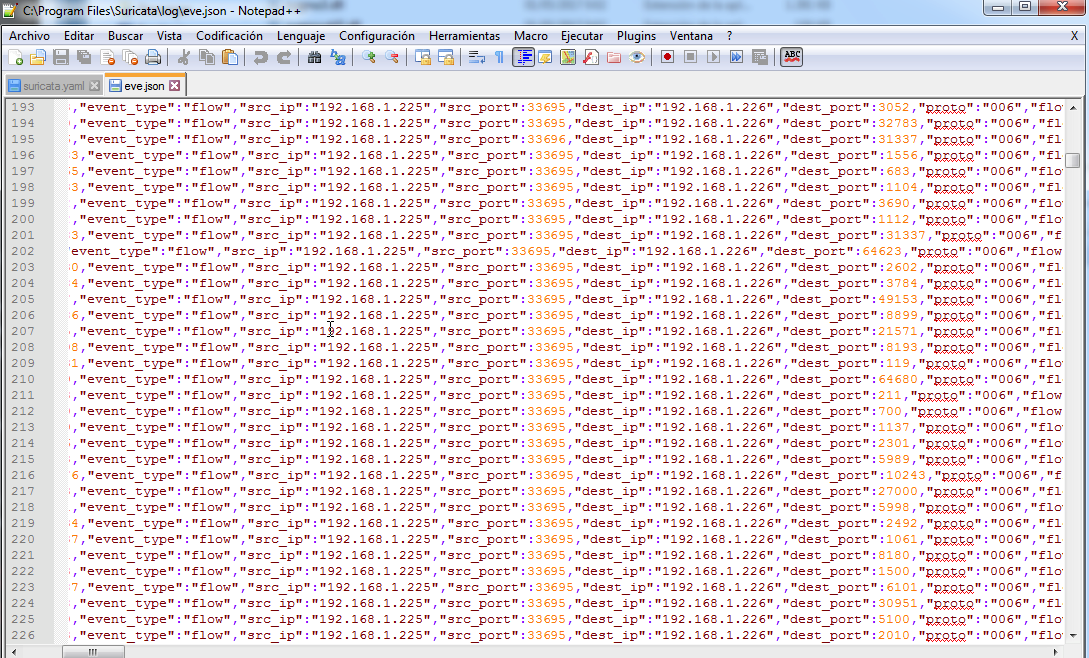
Lo descomprimimos en nuestra carpeta de reglas



Una vez hecho esto, arrancaremos suricata como se ve en la imagen

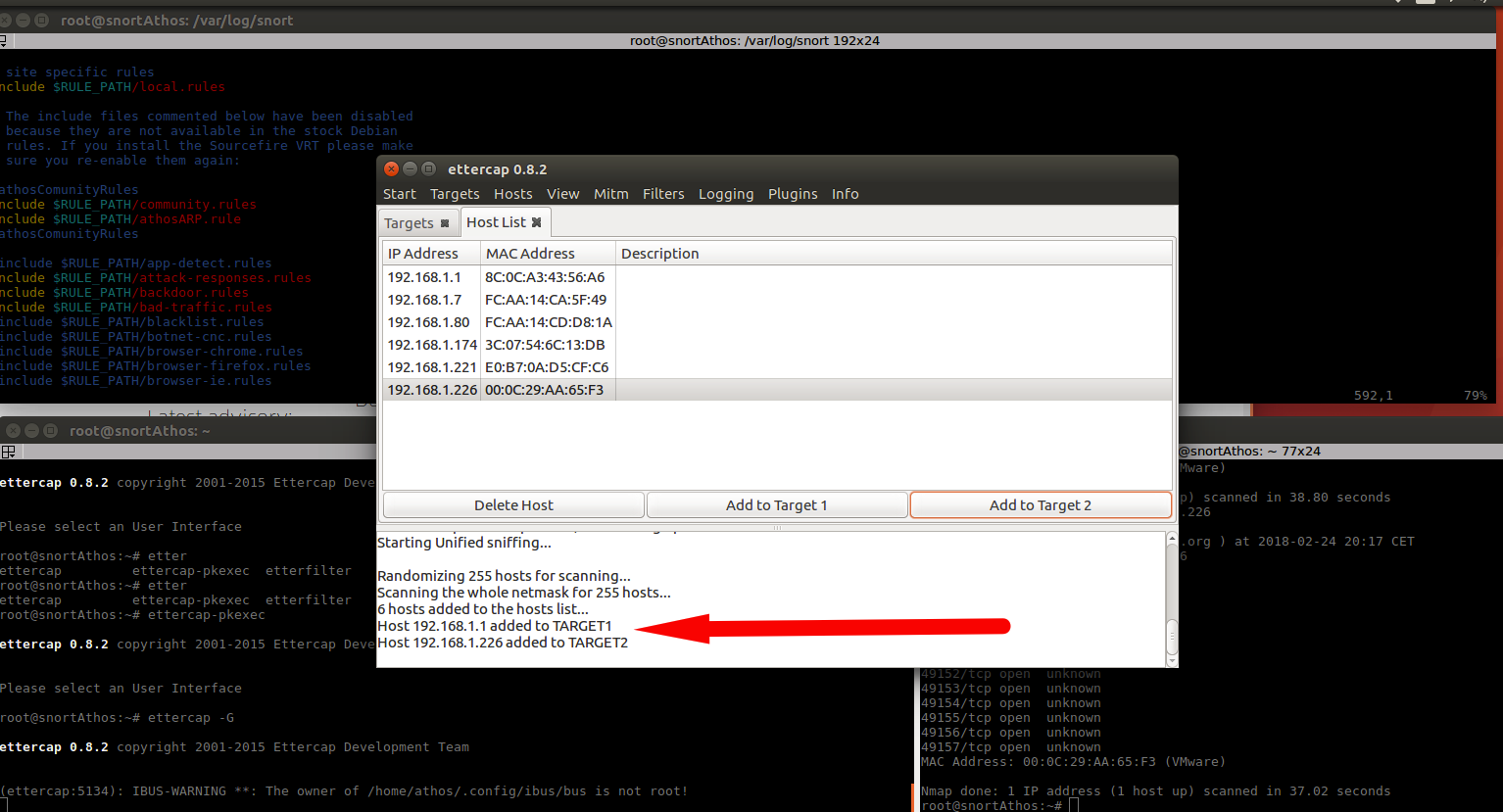


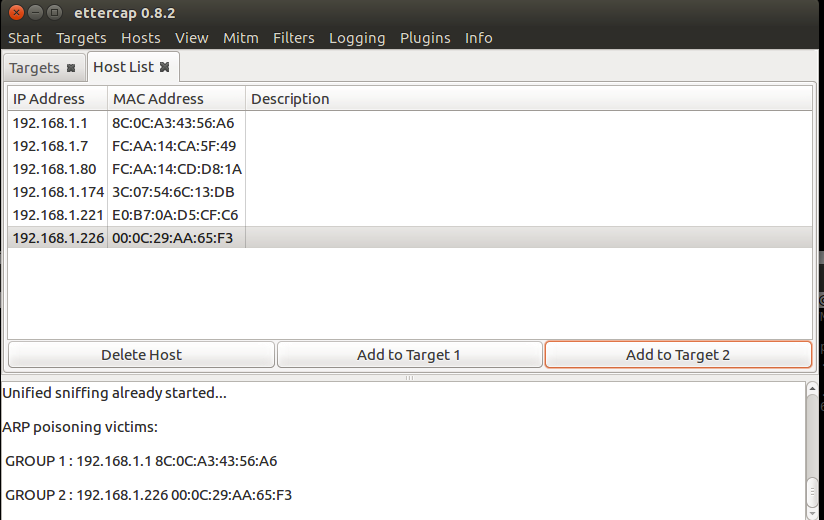
Realizamos un nmap y vemos los logs de suricata



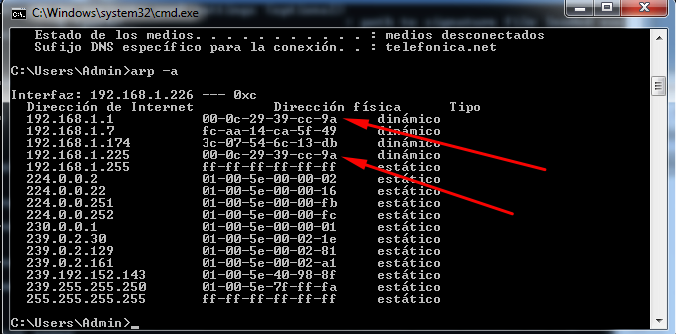
Como se puede ver, una lista interminable de consulta a diferentes puertos.

Ahora, vamos a intentar hacer un mitm con ettercap. Seleccionamos los targets





Como se ve el ataque se ha realizado correctamente



Suricata no ha detectado el ataque de arp poisoning, sólo es cuestión de añadir una regla como hicimos con snort.