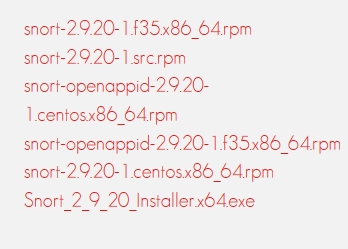
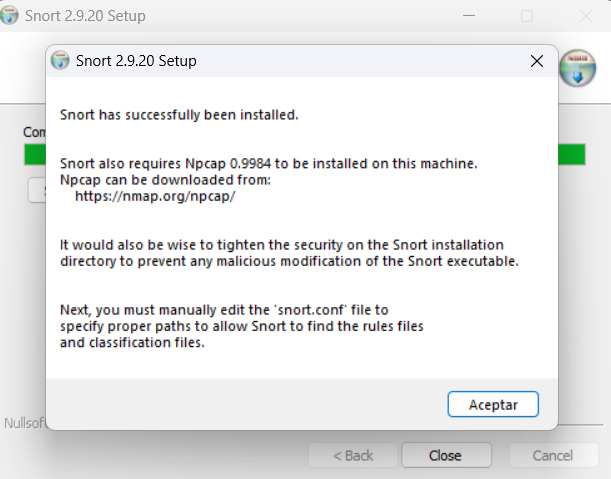
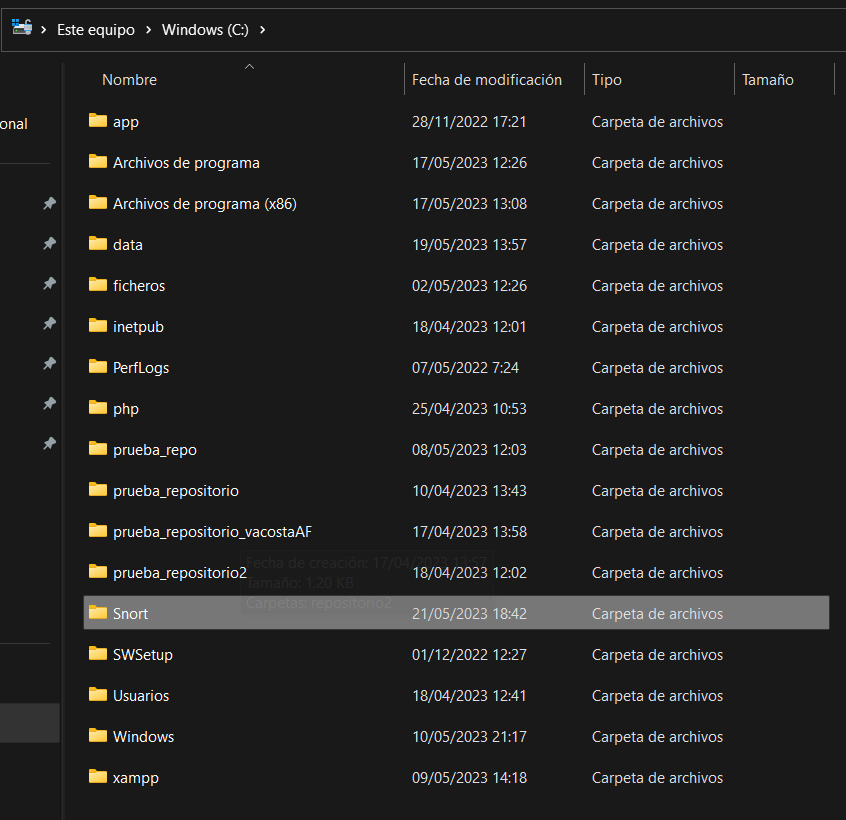
Para Instalar Snort en windows nos vamos a la dirección web [Snort Rules and IDS Software Download](https://www.snort.org/downloads) y nos bajamos la version para Windows “Snort\_2\_9\_20\_Installerx64.exe”.



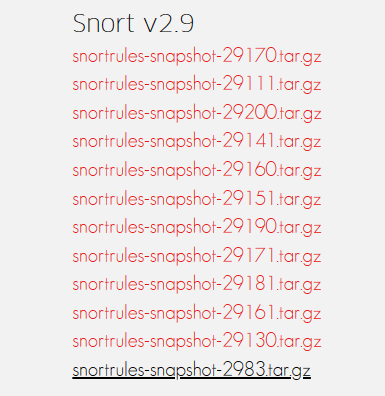
Una vez descargado lo instalamos y seguimos las instrucciones del instalador.



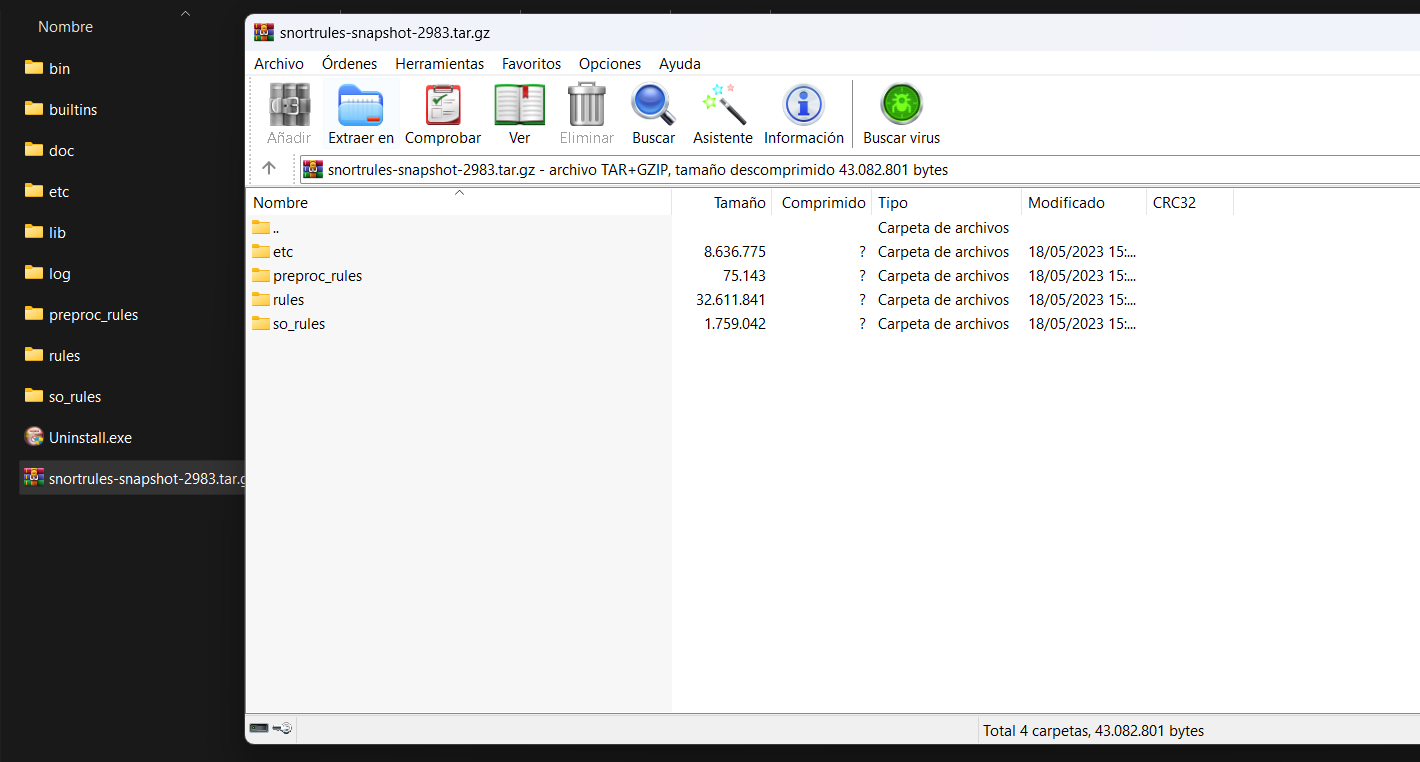
Se te creara la carpeta “Snort” en “C:”.



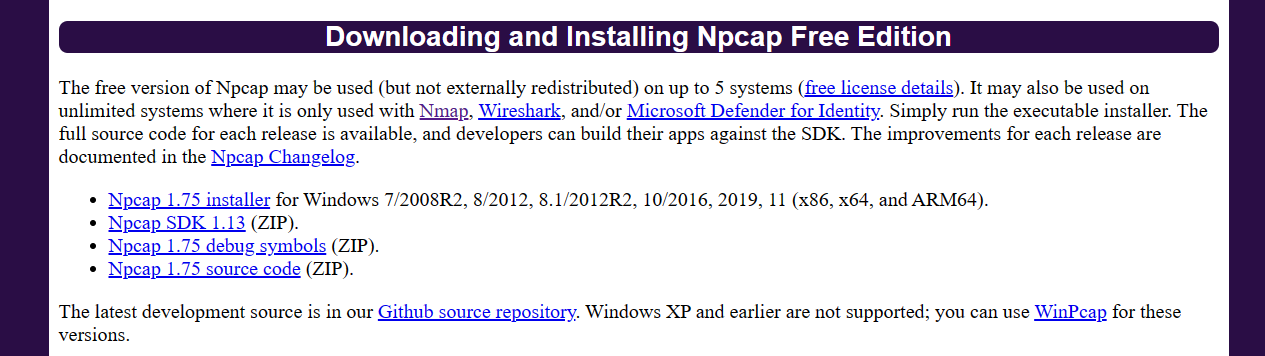
Ahora hay que bajarse las reglas desde la misma página para que el programa funcione:



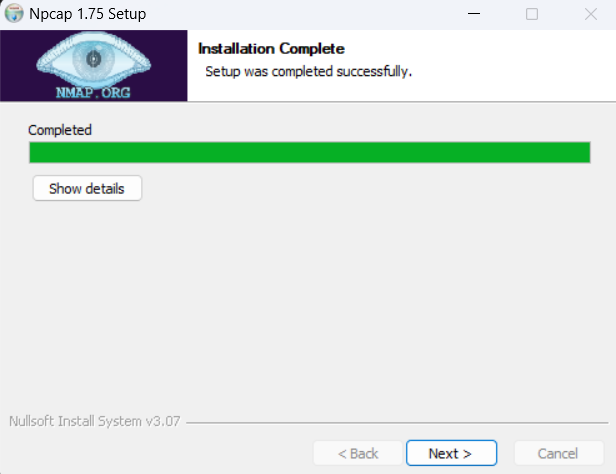
Es posible que al tratarse de reglas de detección de intrusiones de un falso positivo del antivirus, lo desactivamos temporalmente y bajamos el archivo. Lo descomprimimos en la carpeta raíz del programa y sobrescribimos si es necesario:



Ahora tenemos que descargarnos el programa “Npcap” desde [Npcap: Windows Packet Capture Library & Driver](https://npcap.com/#download):

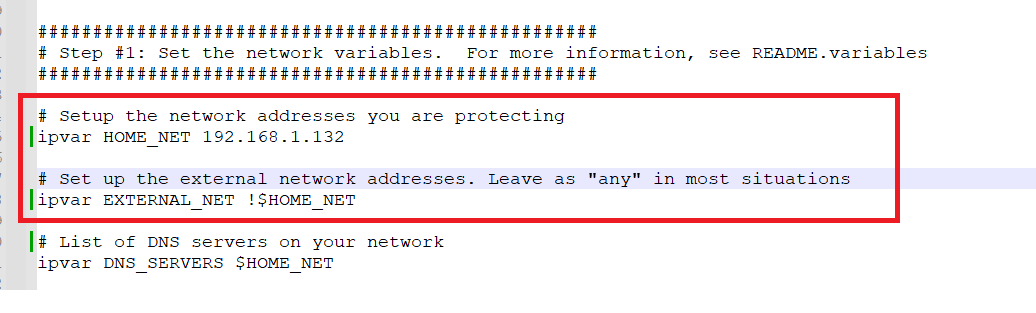


Lo instalamos:

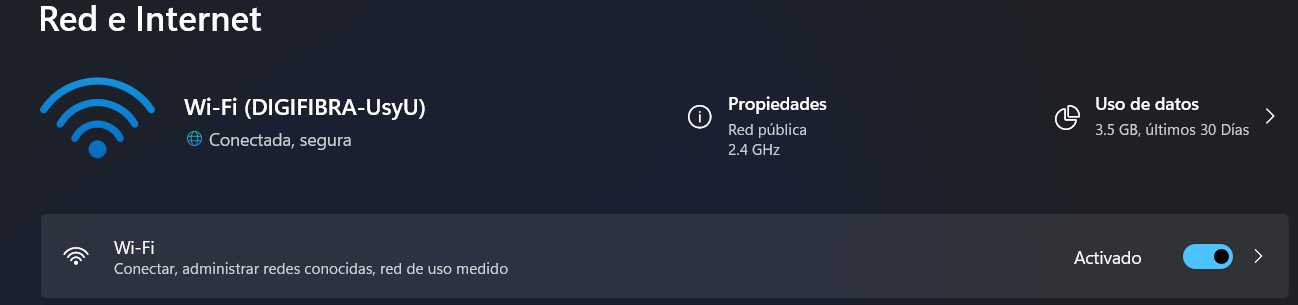


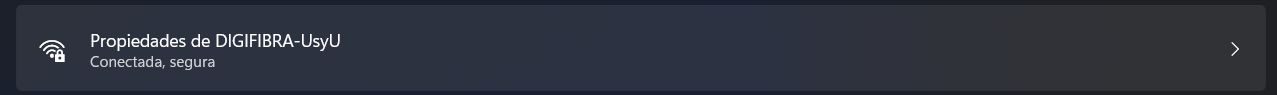
Ahora toca reiniciar el pc. Después nos vamos a la carpeta de “Snort” en “C”, abrimos la carpeta “etc” y buscamos el archivo “snort.cong” el cual podemos abrir con cualquier editor de textos como Notepad++.

Ahí que buscar primero la configuración de red de internet. Buscar el paso numero 1 y en la primera línea poner la ip de la maquina con la que experimentar y en la segunda línea poner “!$HOME\_NET” sin comillas para indicar como redes externas cualquiera menos la de tu pc.



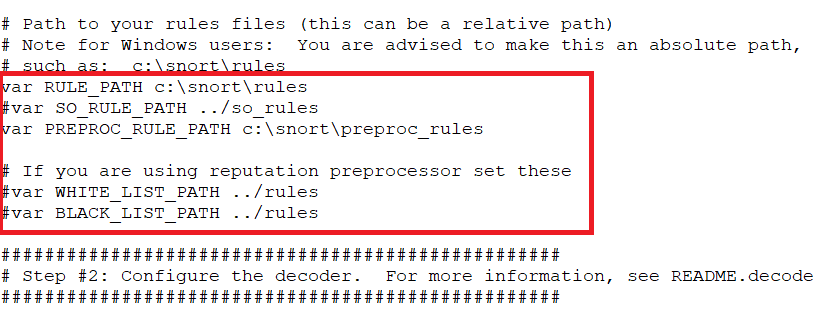
Para saber tu ip puedes ir a configuración de red y buscar tu dispositivo con acceso a internet, en mi caso el wifi y en propiedades encontraras la ipv4 que es la que necesitaremos.



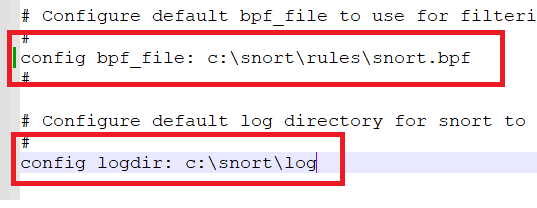




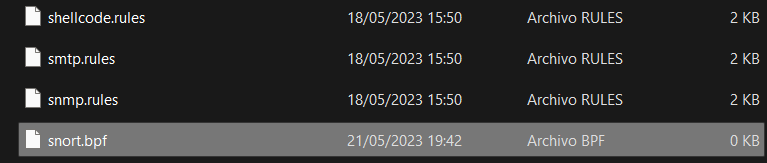
Después bajas hasta el final del paso uno y modificar las líneas indicadas de la siguiente forma:



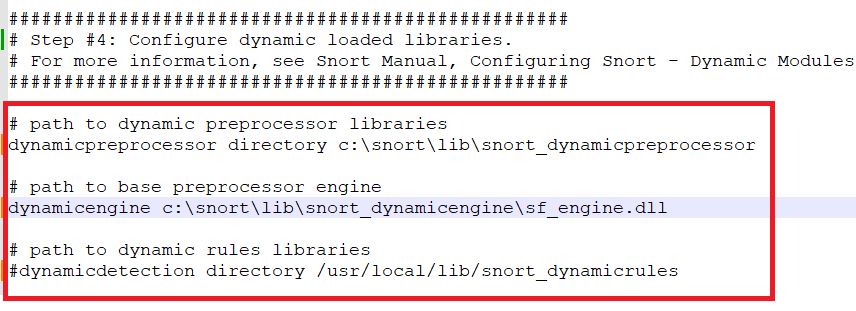
Bajar casi hasta el final del paso 2 y modificar la siguiente línea:



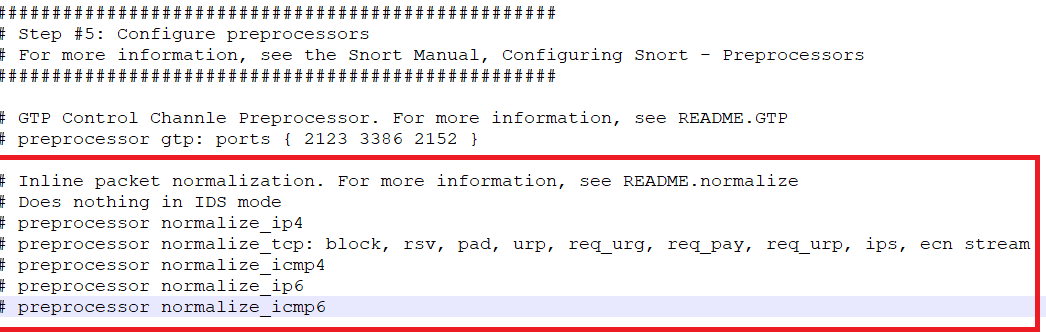
Ir a la ruta escrita en la primera fila modificada y crear ese archivo para que snort no nos de errores.



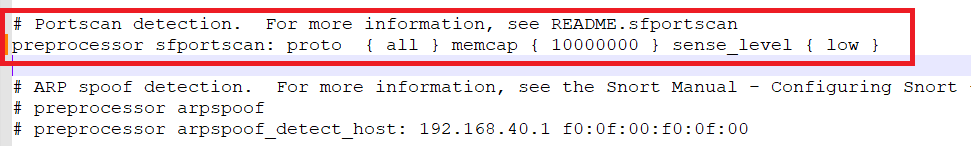
En el paso 4 más abajo modificar las dos primeras líneas y la última comentarla entera con “#”.



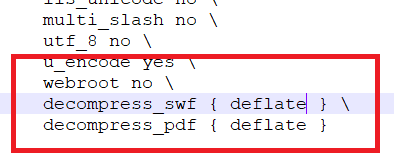
En el paso 5 comentar esas líneas porque Windows no las utiliza:



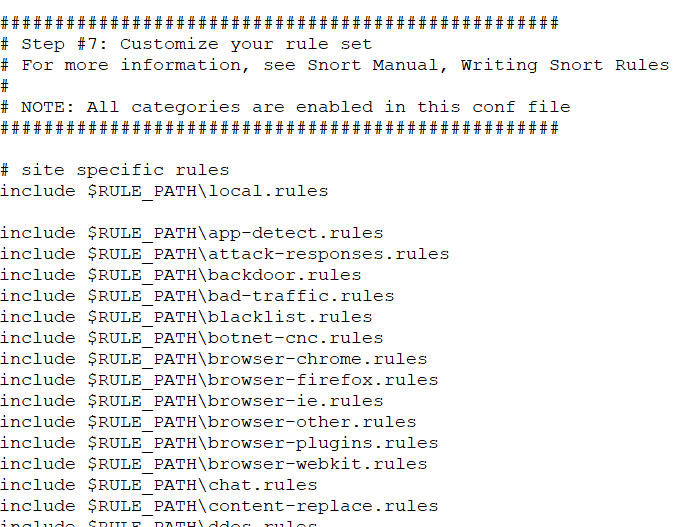
Más abajo en el mismo paso 5 activar las líneas de detección de puertos quitándole el “#”:



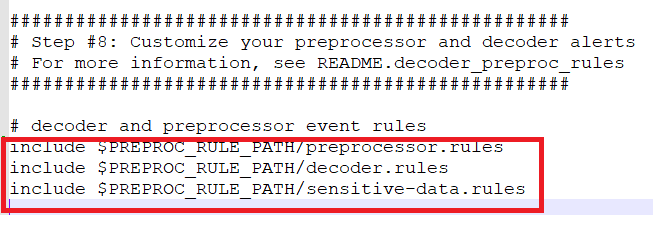
A continuación buscar la línea “decompress\_swf { deflate lzma } \” con Ctrl F y quitarle el “lzma” ya que Windows no utiliza ese método de compresión, quedando así:



En la sección 7 hay que cambiar todas las “/” por “\” son muchas asique es conveniente ayudarte con el editor en vez de hacerlo manualmente.

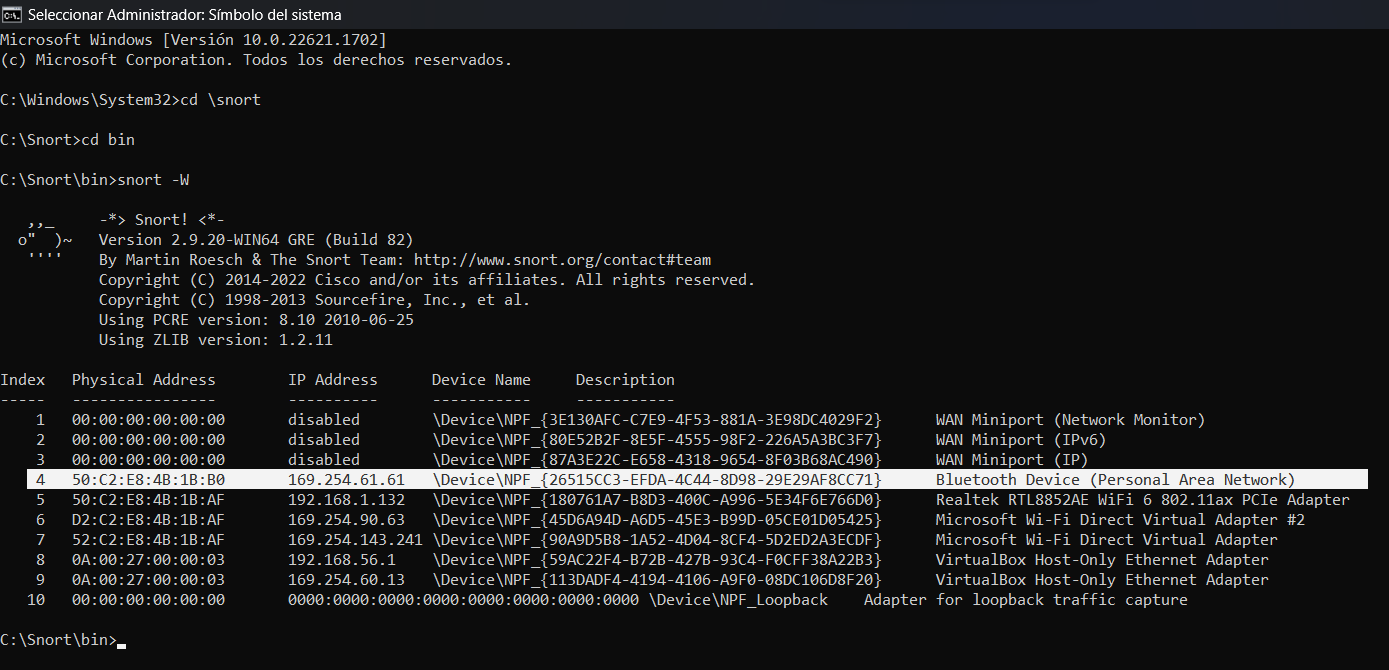


Sección 8: Quitar las “#” de las tres reglas que hay.



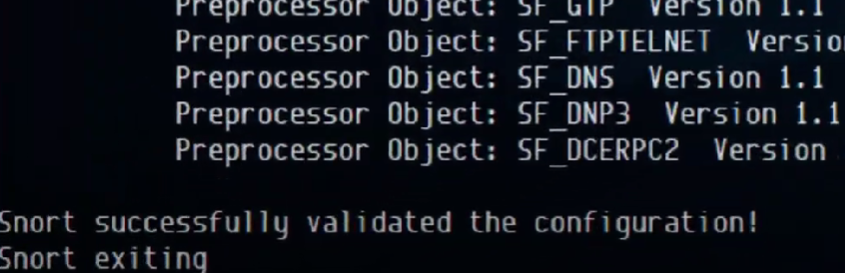
Ya terminamos la configuración.

Abrir la terminal de Windows (cmd) como administrador y hacemos lo siguiente.

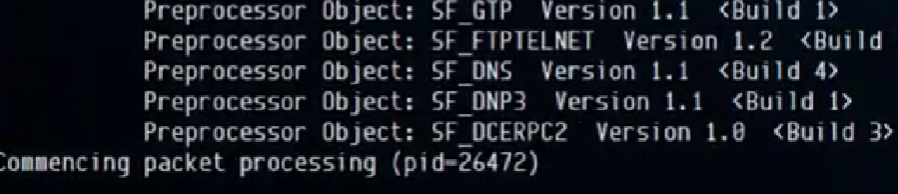


Aquí debería aparecer el dispositivo con el que nos conectamos a internet buscando la ip que buscamos y escribimos al principio lo encontraremos.

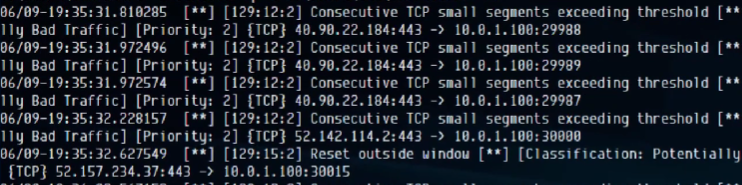
A continuación, escribimos “snort -c c:\snort\etc\snort.conf -T -i 4” sin comillas y el 4 es el número de interfaz de red del dispositivo que buscamos justo antes por lo que en cada caso variará y pulsamos intro. Debería validarnos la configuración.

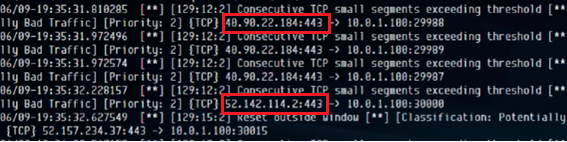


A continuación, escribimos “snort -A console -c c:\snort\etc\snort.conf -T -i 4” sin comillas



Esto nos indica que snort está ya escuchando. Enseguida se nos llenará la pantalla de información que no nos es útil asique escribimos, “snort -A console -q -c c:\snort\etc\snort.conf -T -i 4” para que solo nos salga la información que buscamos:





Estas IPs son de dispositivos que están mandando paquetes de información en nuestra misma red por lo que son posibles intrusos. Ahora habría que coger y apuntarlas y decidir que hacer con ellas como por ejemplo bloquearlas.