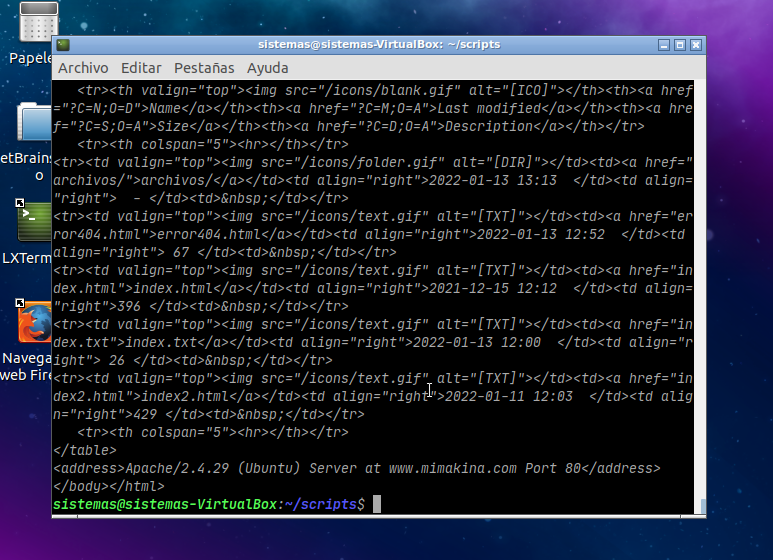
Nuevo ejercicio: Vamos a hacer peticiones desde un cliente a un servidor, para leer el archivo de log de acceso.

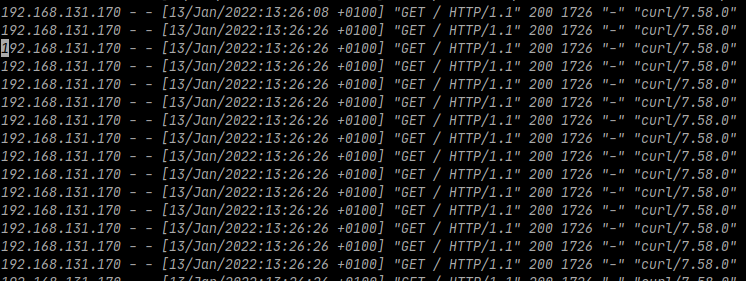
1º → Creamos un bucle y hacemos 500 peticiones desde el cliente al servidor. El bucle se crea y ejecuta en el cliente.



INSTALO CURL, que no está, pongo al cliente en la misma red, le pongo como DNS el servidor y ejecuto el script y que trabaje.

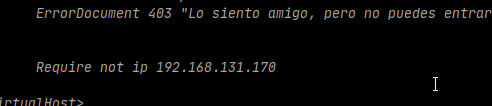


Entonces ahora miro el archivo de log del servidor.



Efectivamente, me ha hecho las 500 peticiones.

Entonces lo que tenemos que hacer es bloquear la IP para evitar que haga esto y que no nos haga un DdoS.



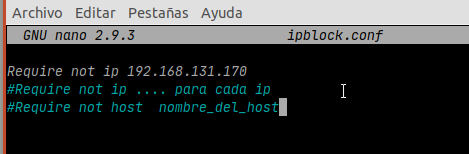
Añadimos esta línea y probamos.

No funciona, solucionar

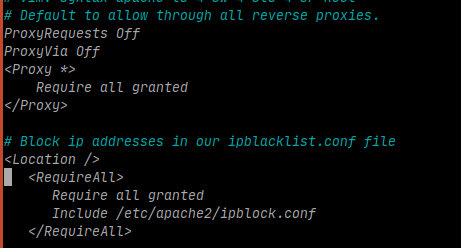
He conseguido solucionar el problema.

Para crear una lista de bloqueados tenemos que seguir los siguientes pasos:

1º → Creamos un archivo en el cual vamos a guardar las IPS, o dominios, o host, que queremos bloquear. En este caso solo una.



2º → Una vez creado, tenemos que decirle a apache que cargue este archivo y que se active la directiva de bloqueo. Esto lo tenemos que hacer en apache.conf



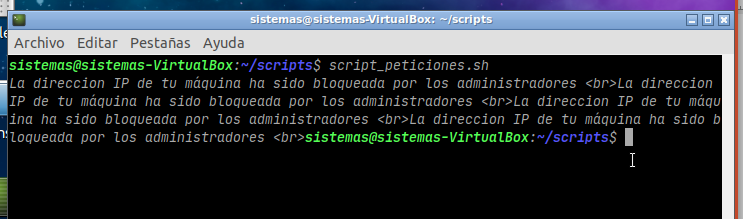
Vamos por partes porque he hecho un copypaste.

La parte de proxy es para permitir que funcione vía proxy, para nuestro ejercicio podríamos omitirlo.

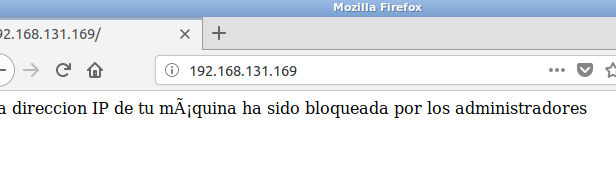
La parte que nos interesa es la segunda. Indicamos la localización de nuestra web que queremos bloquear, esto es por si queremos bloquear TODA la web, o solo alguna página especifica de la web.

Acto seguido permitimos a todo el mundo, y añadimos la directiva include archivo.conf, esto lo que hace es cargar nuestro archivo, y como tenemos puesto que las Ips X no tengan acceso, pues no cargaran.

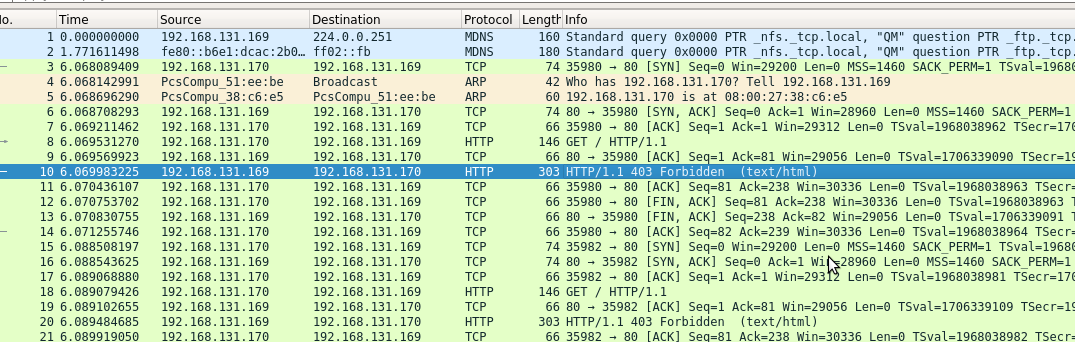
3º → Reiniciamos el servicio y probamos. Entramos al cliente y lanzamos el script del otro día, pero solo con 3-4 peticiones para no saturar.



Como podemos ver, salta el Error 403 tantas veces como peticiones hemos realizado.

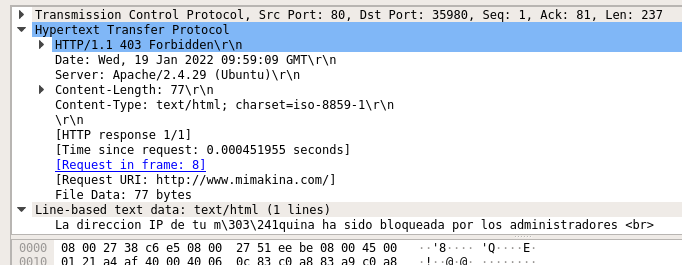
Y si accedo vía web pasa lo mismo.

4º → Vamos a lanzar las peticiones, pero escuchando en el servidor con wireshark



aparecen las solicitudes del cliente, y podemos ver en la parte de info que pone 403 forbidden, esto es que ha saltado la directiva de bloqueo.

Si abrimos esa tarma para ver el contenido



Aquí podemos ver el error 403, la web que prohibe, y el texto en plano.