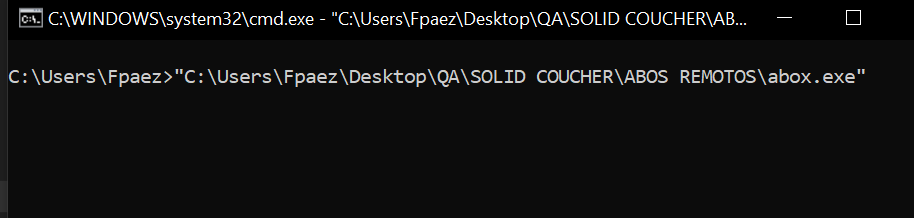
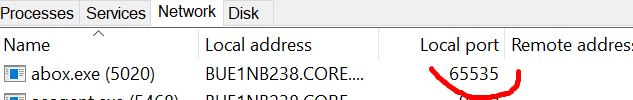
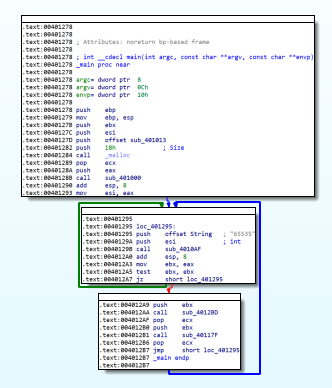
Ahora nos vamos a enfrentar al ABOX, y al ejecutarlo vemos que no imprime ningún mensaje.



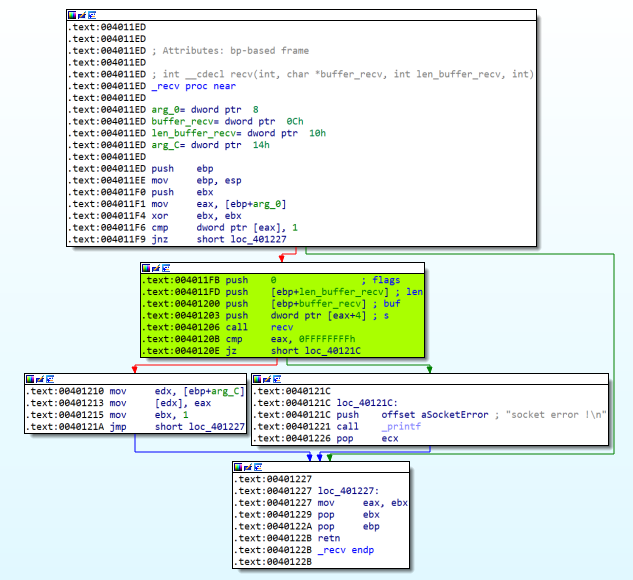
Con **Proccess Hacker** vemos el puerto que está escuchando



Vamos abrirlo en **IDA,** este es todo el árbol inicial:

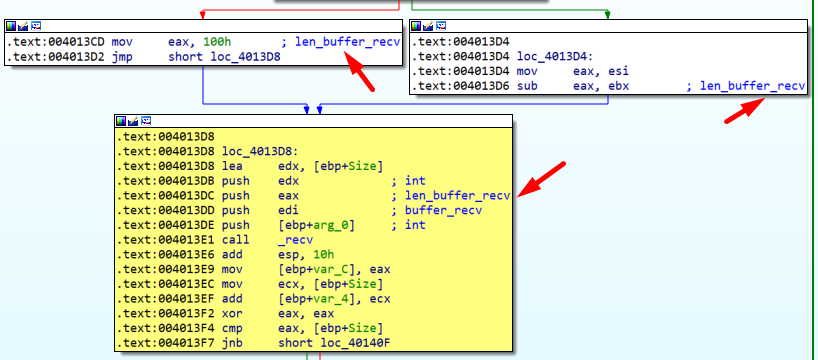


Ahí veo el puerto que se pone a la escucha, voy a buscar la función **recv** directamente.

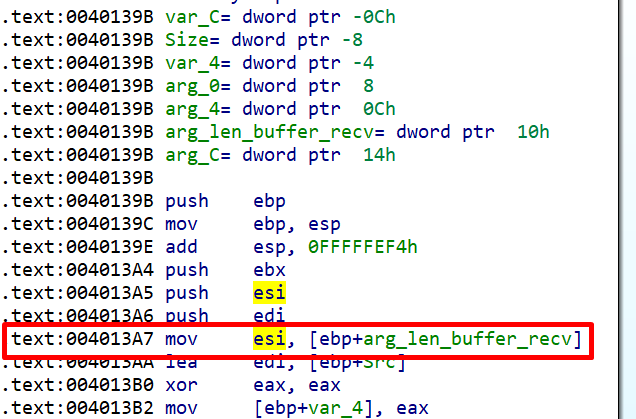


Vayamos a donde es llamado todo este bloque que contiene el **recv**

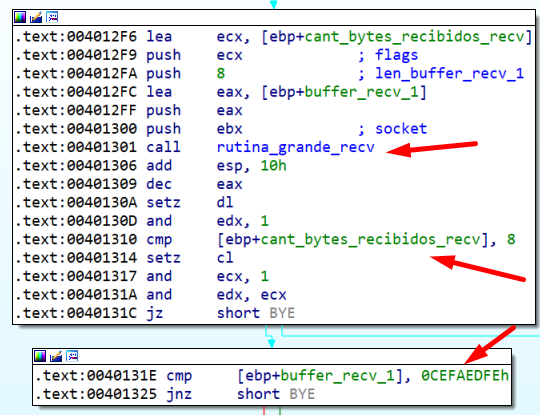
En el bloque amarillo vemos que **len\_buffer\_recv** va a tener un valor diferente dependiendo desde donde se llegue.

****

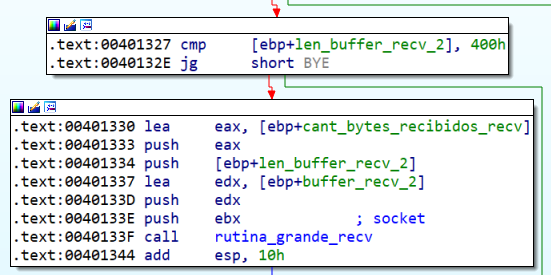
Si llega desde el bloque de la izquierda entonces **len\_buffer\_recv** valdrá **0x100**, mientras que si llega desde el bloque derecho, el **len\_buffer\_recv** será el valor que se le pasa por argumento a toda esta rutina.



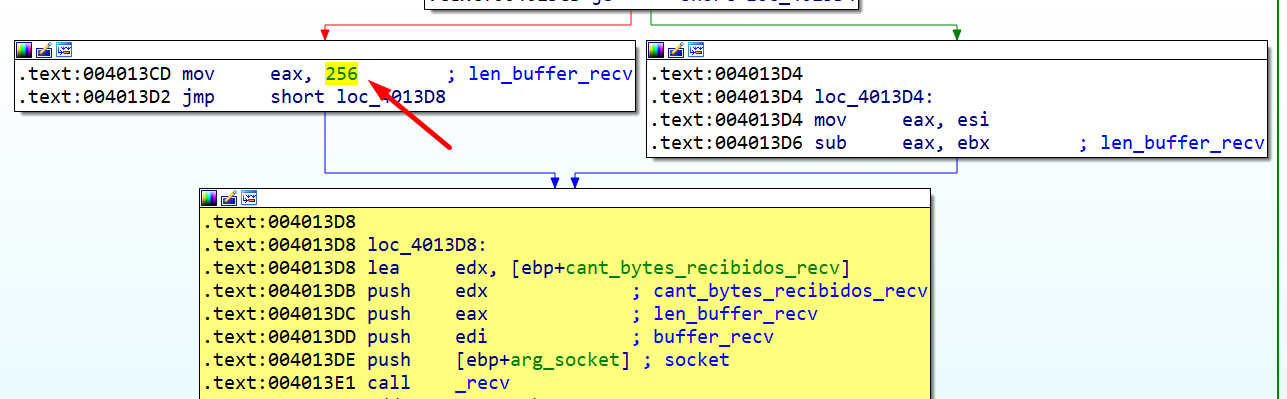
Ese valor es fijo, es de **8 bytes**. también vemos aquí que los primeros **4 bytes** deben ser **0xCEFAEDFE**



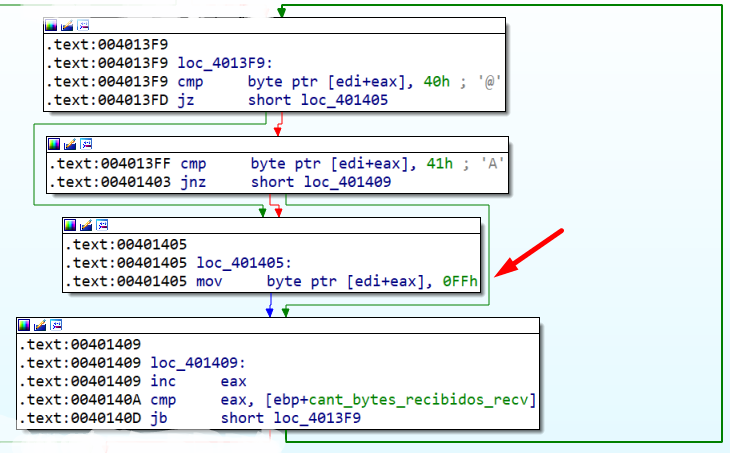
Después de pasar todo esto, vuelve a ejecutar la función **recv**

****

En esta ocasión va a leer **256 bytes**



Algo a tener en cuenta es que si entre los **256** bytes hay dígitos **0x40 o 0x41,** los modifica por un **0xFF,** esto pasa en el **segundo** **recv**

****

Inmediatamente debajo de este bloque tenemos un **memcpy**

**SIN TERMINAR**

**Referencias:**

* [JB](http://unixwiz.net/techtips/x86-jumps.html)
* [memcpy](https://www.tutorialspoint.com/c_standard_library/c_function_memcpy.htm)