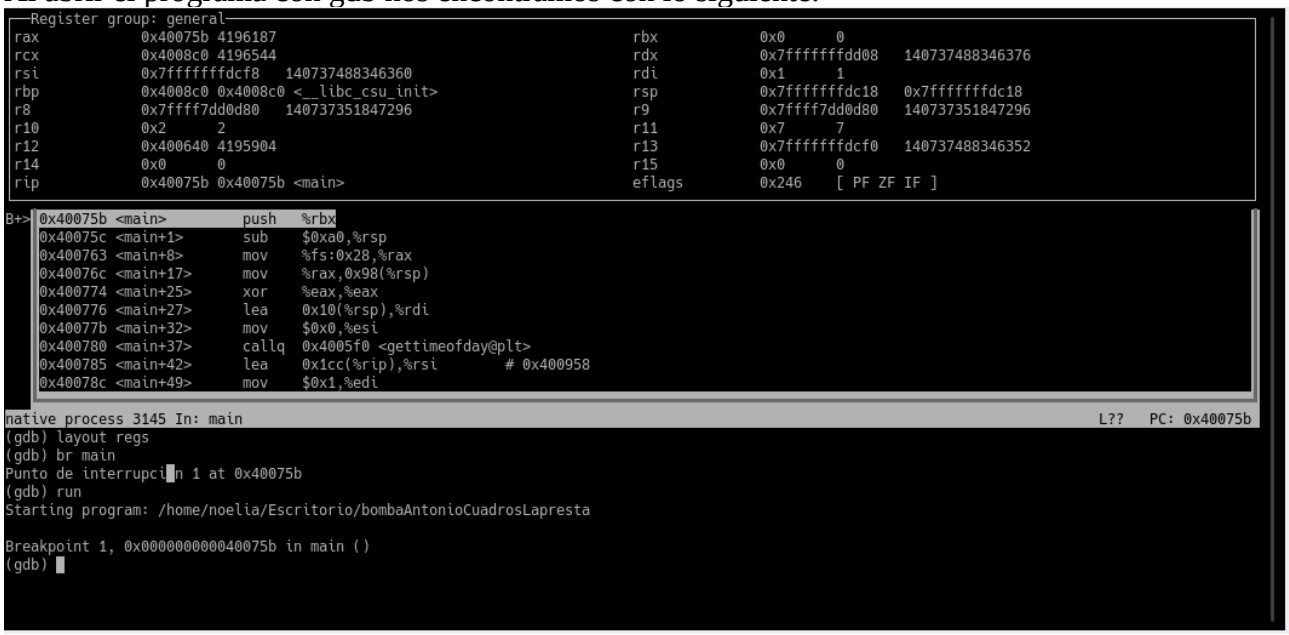
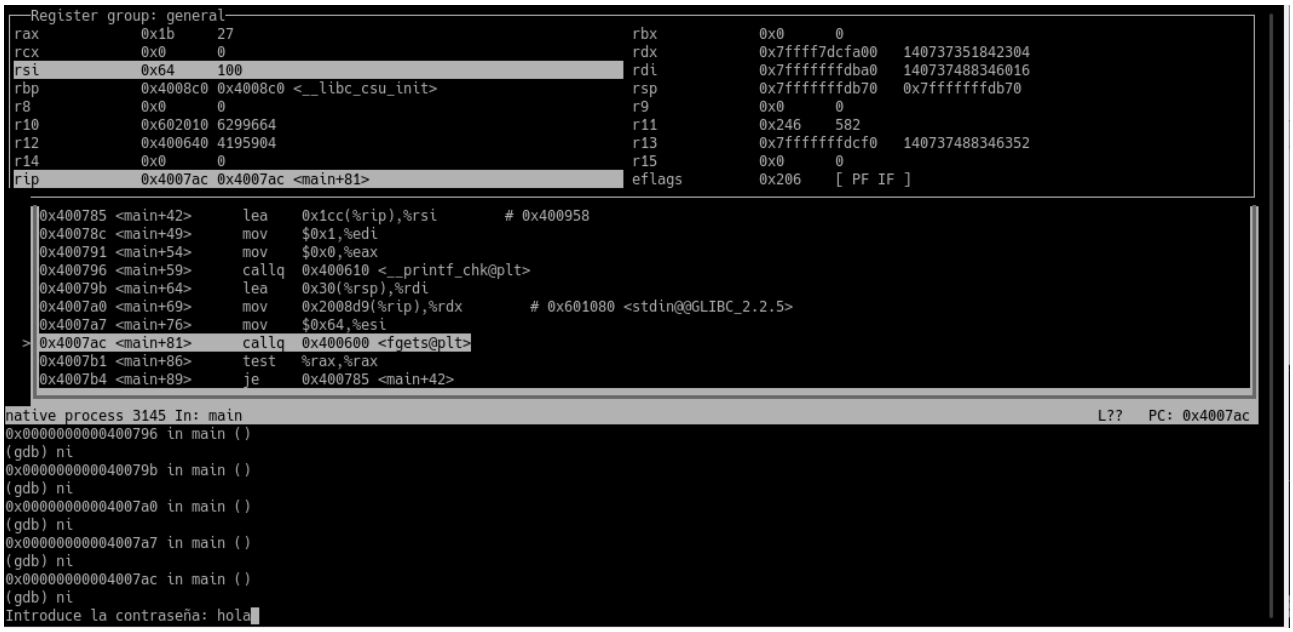
Descodificación bomba Antonio Cuadros Lapresta
Noelia Escalera Mejías. Grupo A3

Al abrir el programa con gdb nos encontramos con lo siguiente:



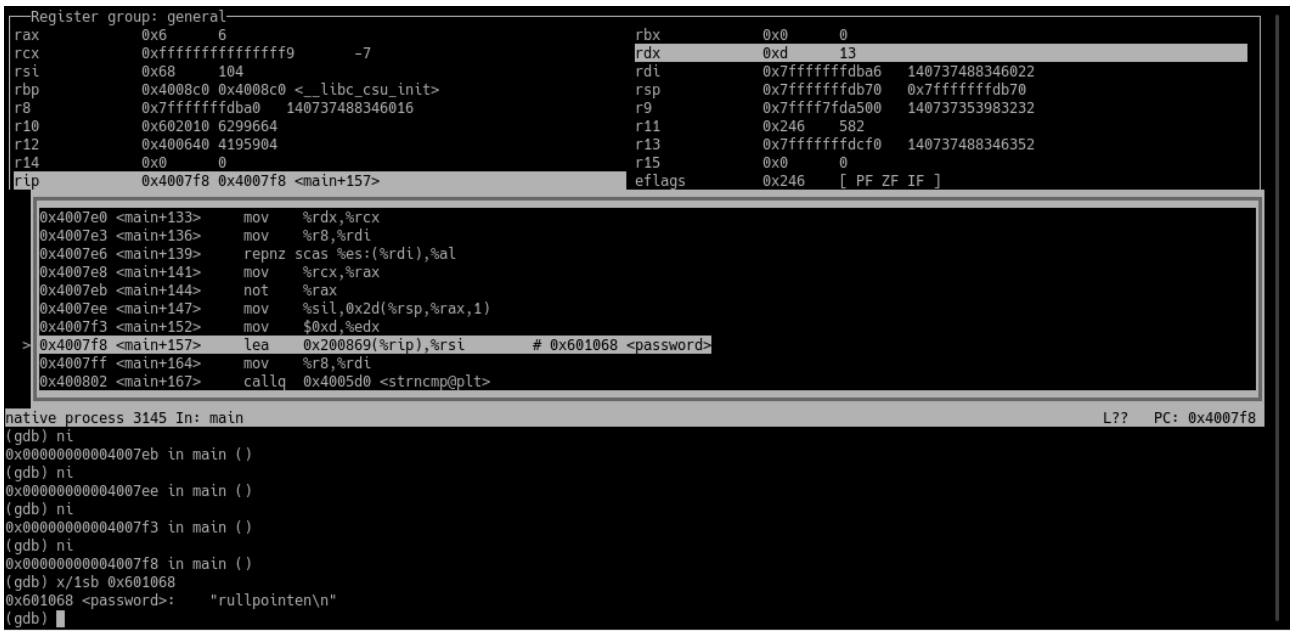
Avanzamos con ni hasta que nos pida la contraseña, nosotros hemos introducido “hola\n” como contraseña:



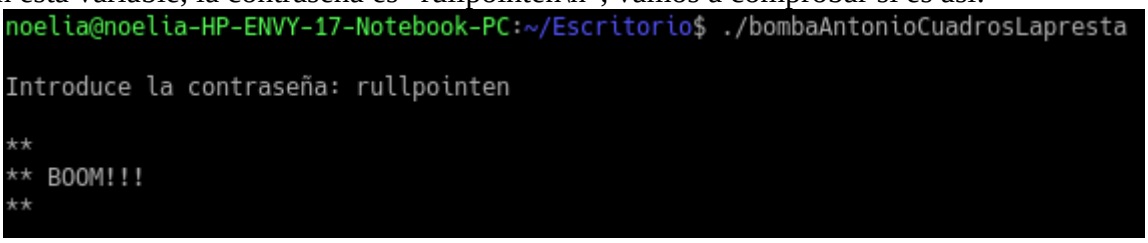
Seguimos avanzando y nos encontramos una variable llamada password, vemos su contenido:

Noelia Escalera Mejías

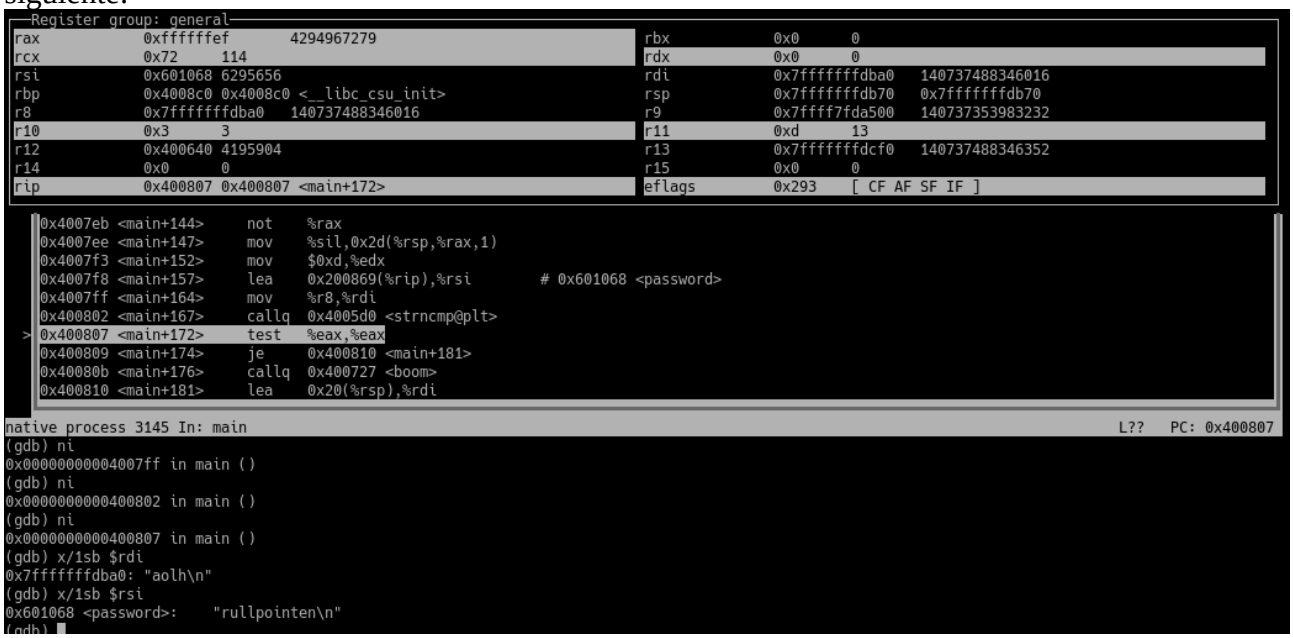
Grupo A3



Según esta variable, la contraseña es “rullpointen\n”, vamos a comprobar si es así:



Luego no es la contraseña, está codificada, vamos a intentar descifrar la codificación. Avanzamos en el programa hasta que llegamos a una función strncmp, si comprobamos los argumentos vemos lo siguiente:

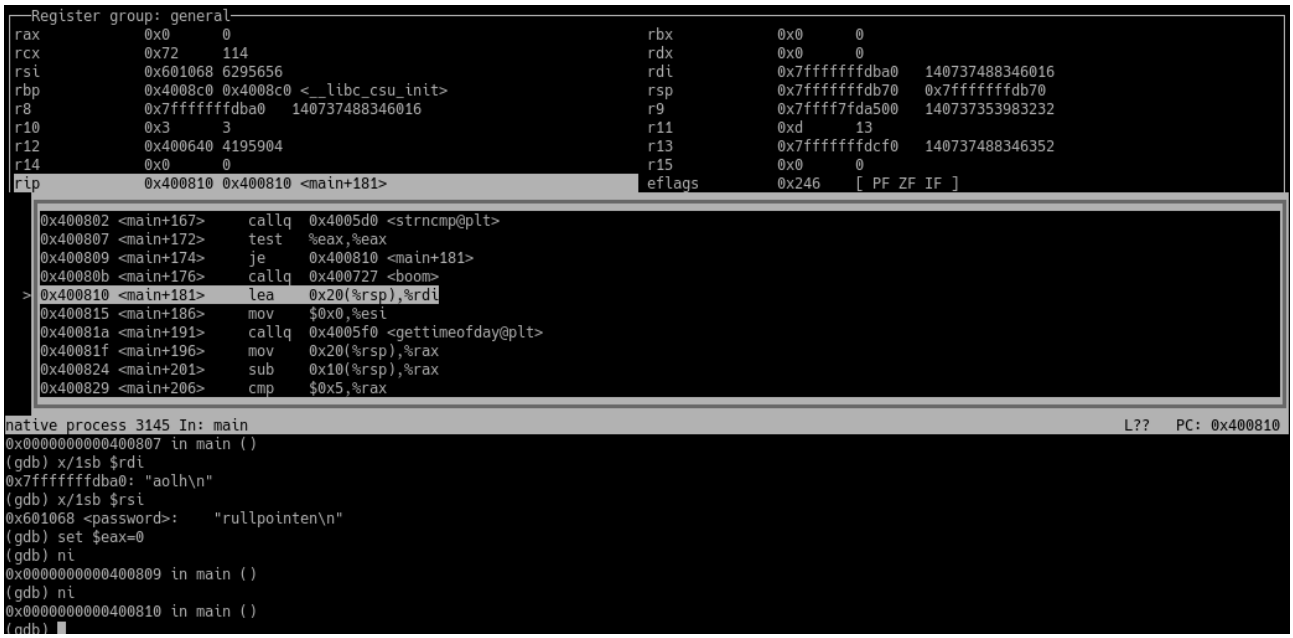


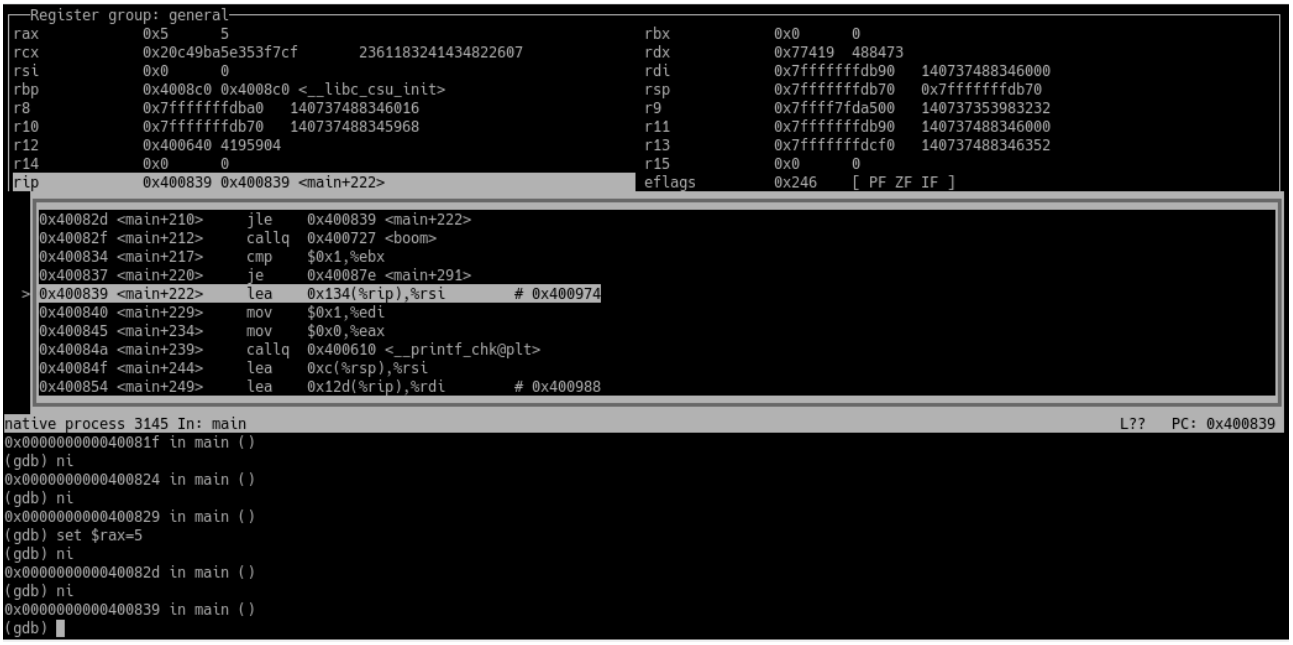
Noelia Escalera Mejías

Grupo A3

Uno de los argumentos es la contraseña codificada anteriormente hallada y el otro es “aolh\n”: nuestra contraseña (“hola\n”) con el primer y el último carácter (sin contar ‘\n’) intercambiados, es decir, nuestra contraseña codificada. Si aplicamos esta codificación a la contraseña del programa, nos queda “nullpointer\n”.

Ahora vamos a intentar hallar el pin. Vamos a seguir avanzando, para ello nos debemos saltar los distintos test para que no se active el boom:

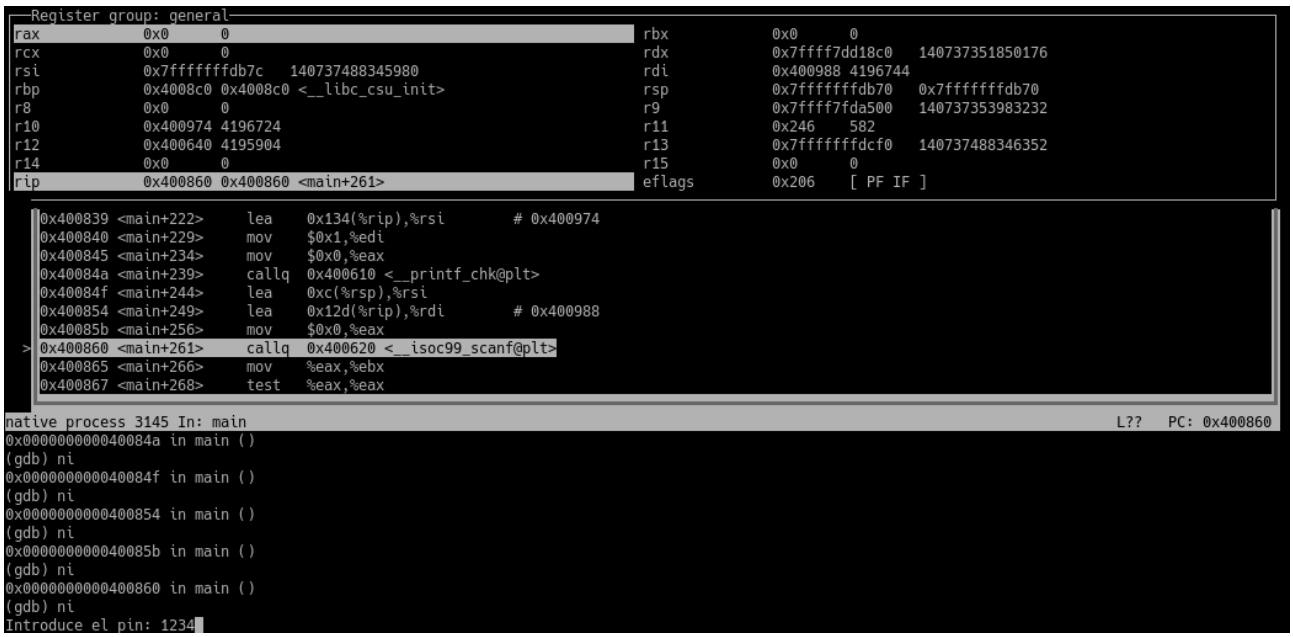




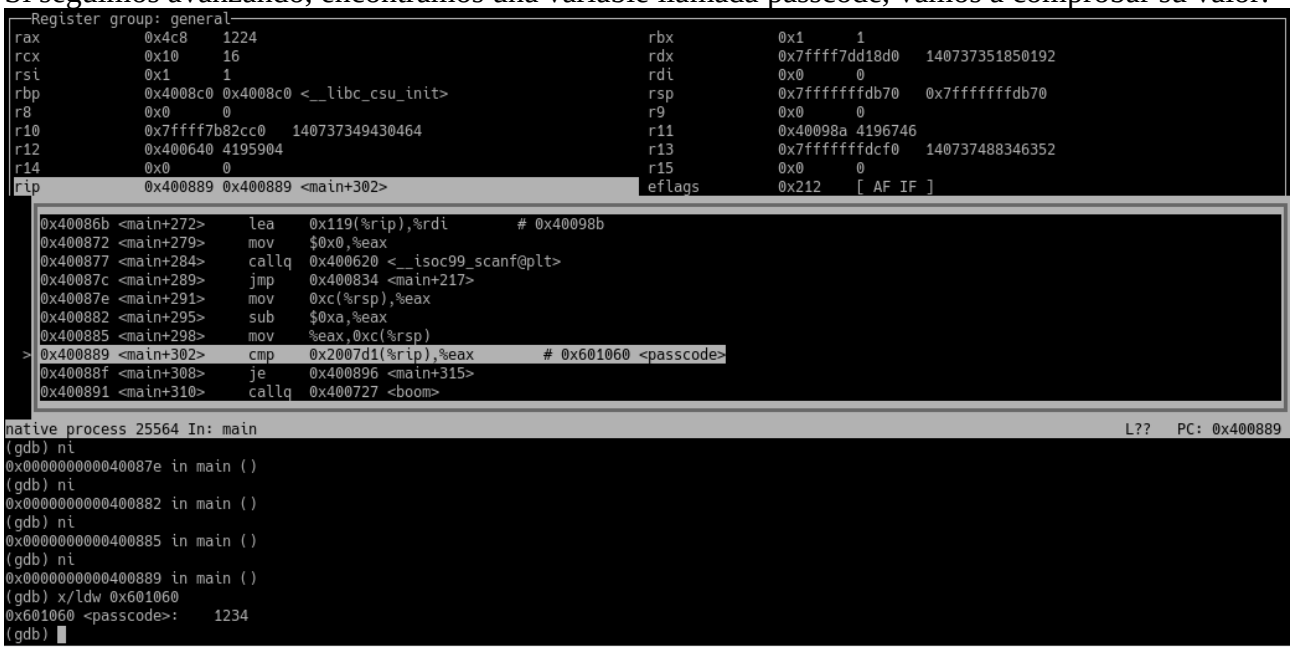
Cuando nos pide el pin, introducimos 1234:

Noelia Escalera Mejías

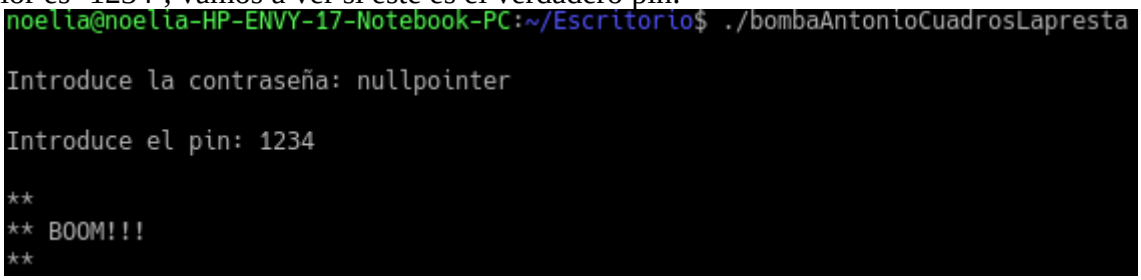
Grupo A3



Si seguimos avanzando, encontramos una variable llamada passcode, vamos a comprobar su valor:



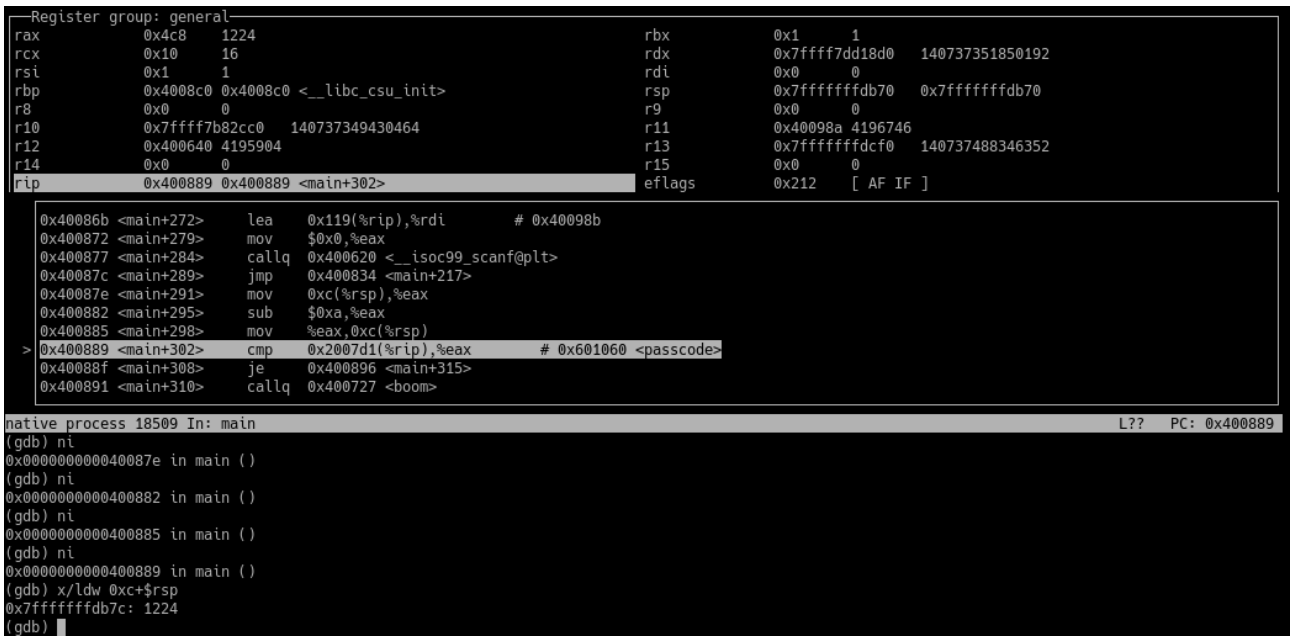
Su valor es ‘1234’, vamos a ver si este es el verdadero pin:



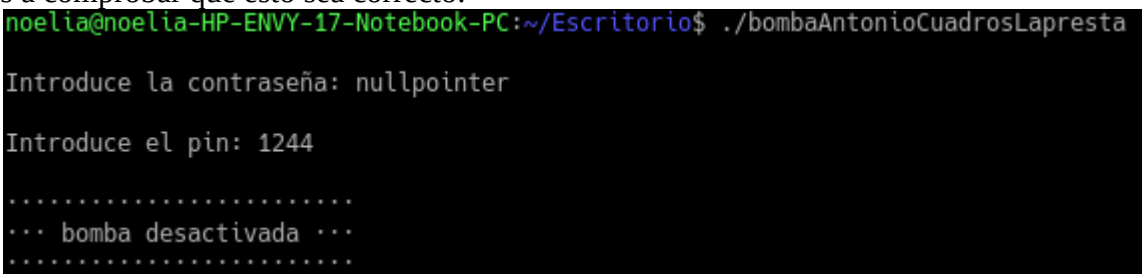
Luego este no es el pin correcto y está codificado, vamos a intentar averiguar la codificación. Veamos qué se le pasa a cmp:

Noelia Escalera Mejías

Grupo A3

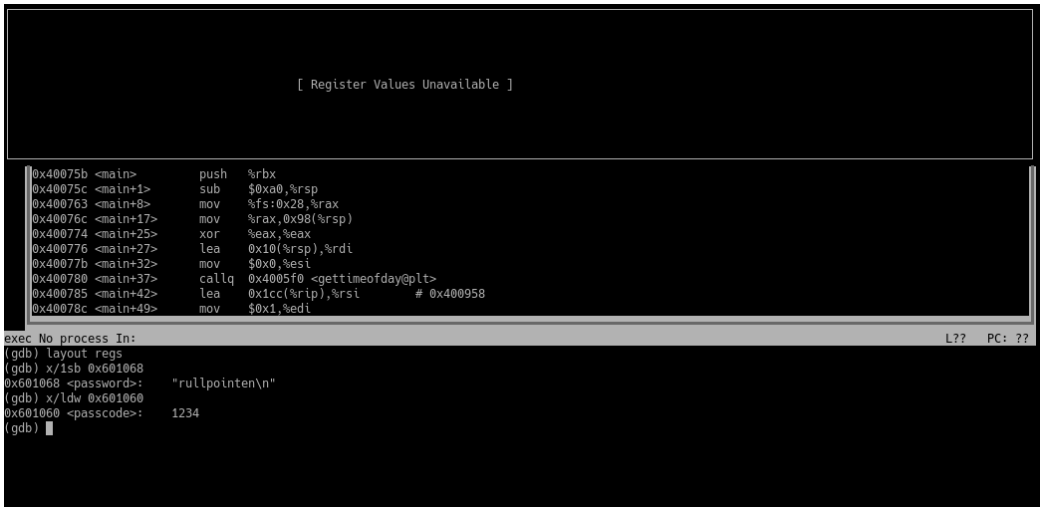


Como vemos se comparará con passcode un número ‘1224’, que es nuestro pin codificado. La codificación consiste en restarle 10 al número, luego podemos deducir que su pin original es ‘1244’, vamos a comprobar que esto sea correcto:



Luego efectivamente hemos hallado los credenciales correctos.

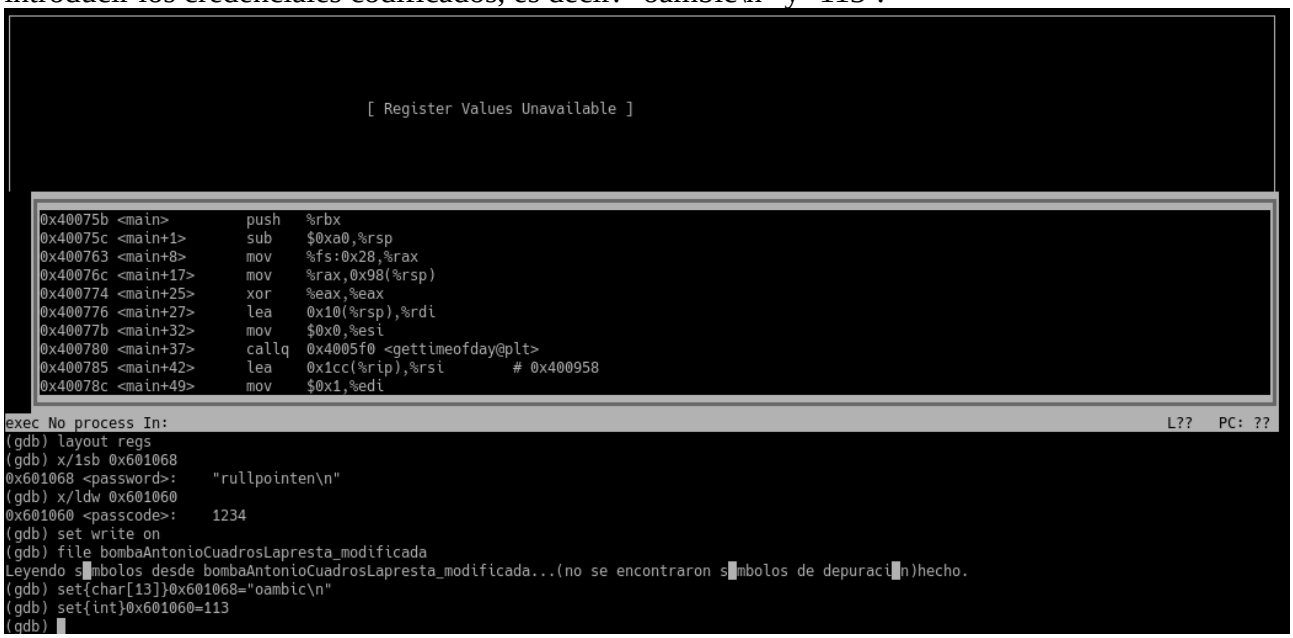
Ahora vamos a cambiar el password y el passcode, como en la otra bomba que he desactivado, voy a hacerlo en un archivo a parte. Tenemos que cambiar las direcciones 0x601068 (password) y 0x601060 (passcode), he cogido estas direcciones de las anteriores capturas.



Noelia Escalera Mejías

Grupo A3

Vamos a cambiar la contraseña por “cambio\n” y el passcode por ‘123’, para ello habrá que introducir los credenciales codificados, es decir: “oambic\n” y ‘113’.



Comprobamos que lo hemos cambiado correctamente:

Luego está correctamente cambiado.

Noelia Escalera Mejías

Grupo A3