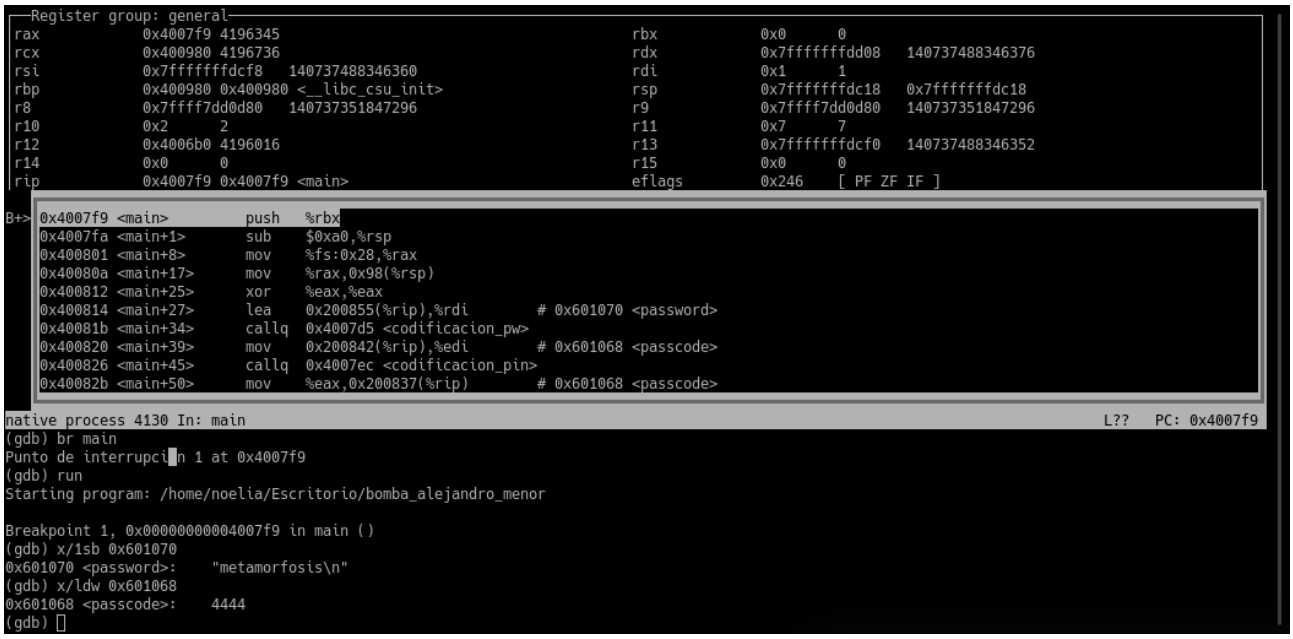
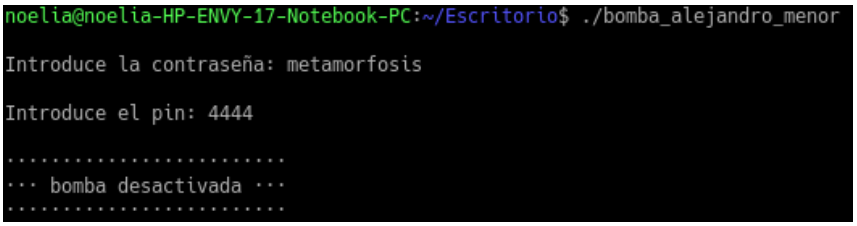
Descodificación bomba Alejandro Menor Molinero
Noelia Escalera Mejías. Grupo A3

Al abrir el programa con gdb, vemos que tiene guardadas dos variables, una llamada password y otra passcode, vamos a ver su interior.

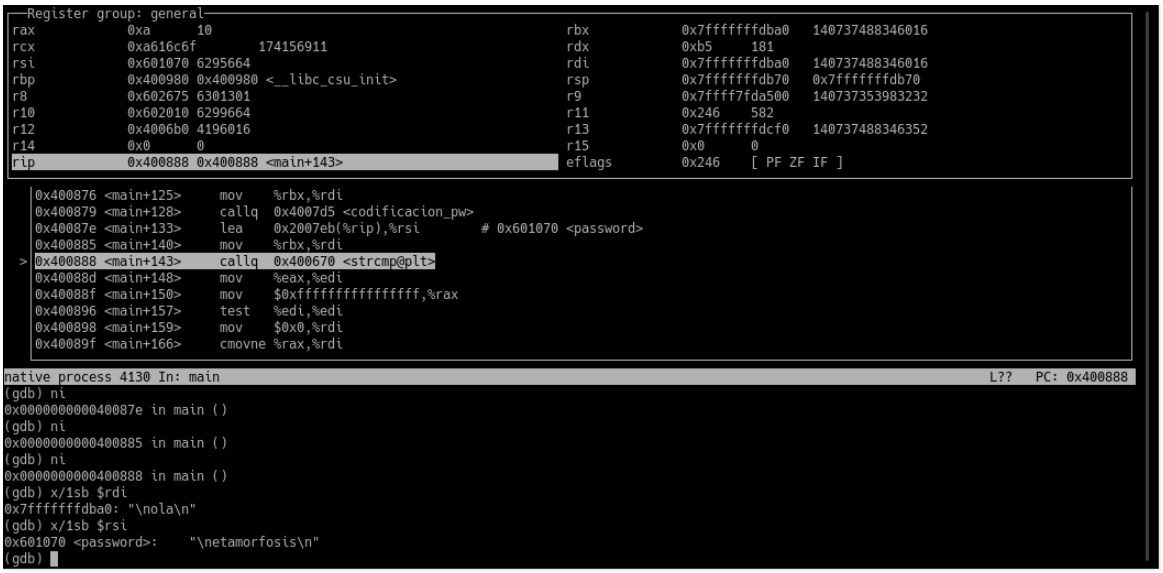


Vemos que la contraseña vale “metamorfosis\n” y el pin 4444. Vamos a ver si estas son las claves verdaderas:

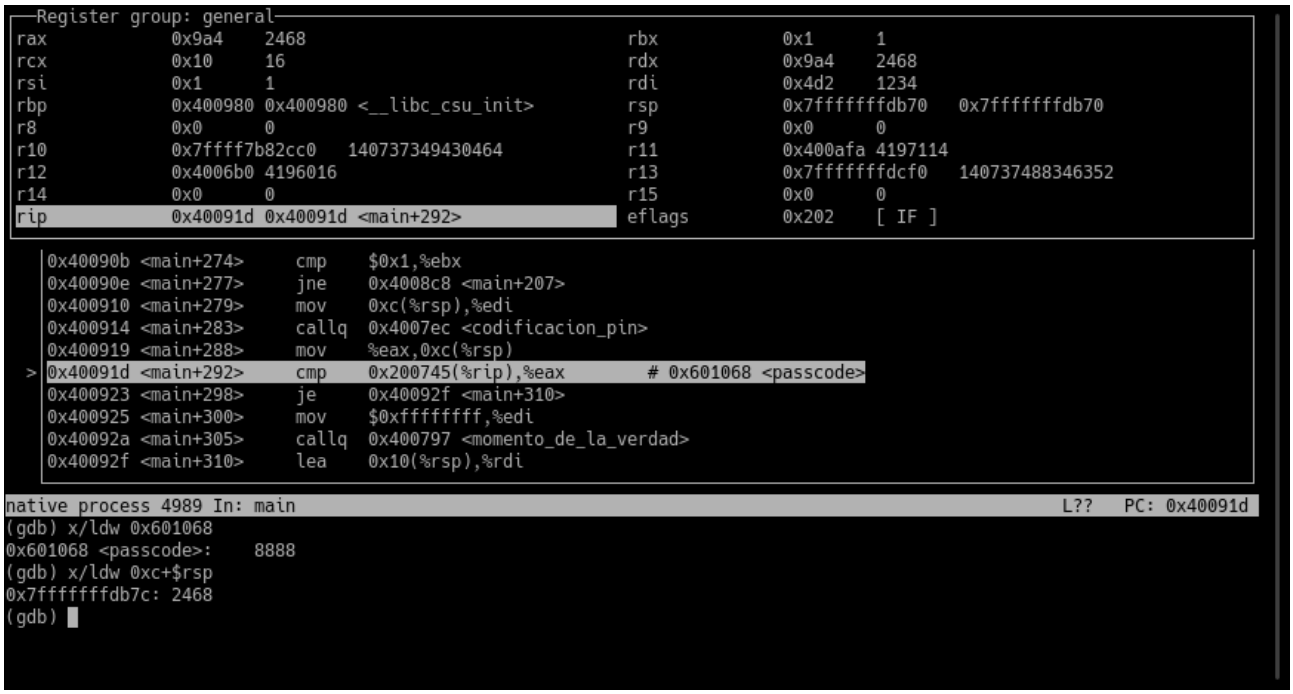


Efectivamente, son estos los credenciales y hemos desactivado la bomba. No obstante, el programa llama posteriormente a una función codificar, es decir, codifica las contraseñas pero las guarda sin codificar y se pueden averiguar sin descifrar la codificación, sin embargo, a mí me gustaría descifrarla.

Hemos introducido como contraseña “hola\n”. Si avanzamos hasta que se comparan las contraseñas y accedemos a los parámetros de strcmp. Como se ve en la captura de la siguiente página, compara “nola\n” con “netamorfosis\n”, es decir, la codificación consiste en cambiar la primera letra de la contraseña por una n.



Como pin hemos introducido 1234. Si accedemos a passcode, ahora el pin vale 8888. En main+283 ha codificado nuestro pin también, ha guardado el resultado en 0xc(%rsp), y ahora nuestro pin vale 2468. De aquí podemos deducir que la codificación consiste en multiplicar el pin por 2, es decir, el pin vale 4444.

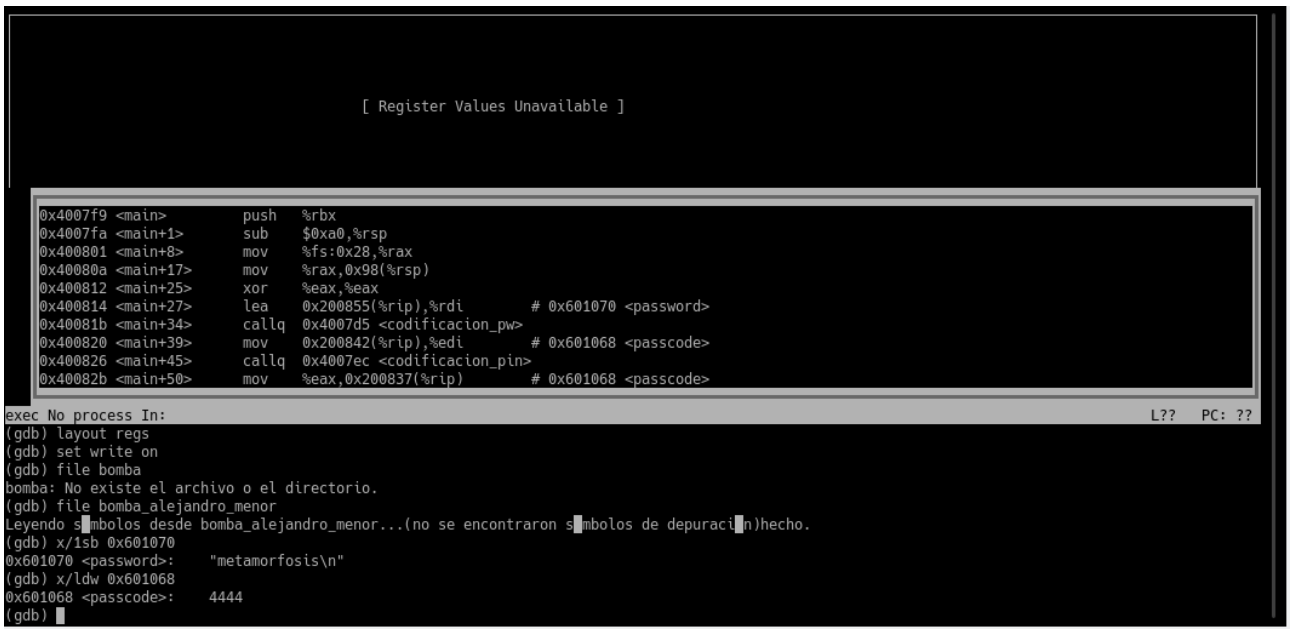


Ahora vamos a cambiarle la contraseña, vamos a permitir la escritura en el ejecutable y vamos a volver a comprobar en qué direcciones están el password y el passcode

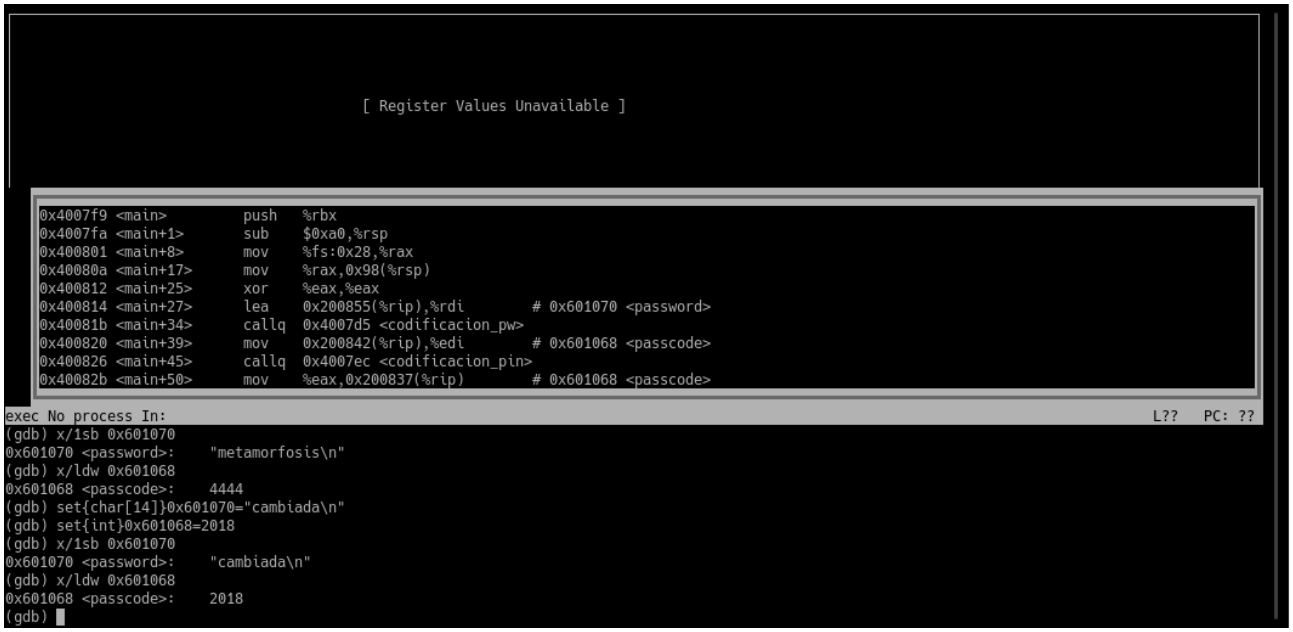
---

Noelia Escalera Mejías

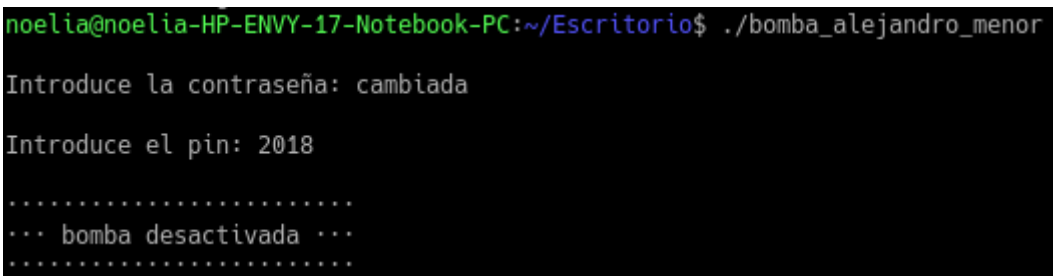
Grupo A3



Ahora cambiamos las contraseñas: el password a “cambiado\n” y el passcode a 2018.



Vamos a ver que los cambios se hayan resuelto correctamente:



Luego se han hallado los resultados esperados.

Noelia Escalera Mejías

Grupo A3