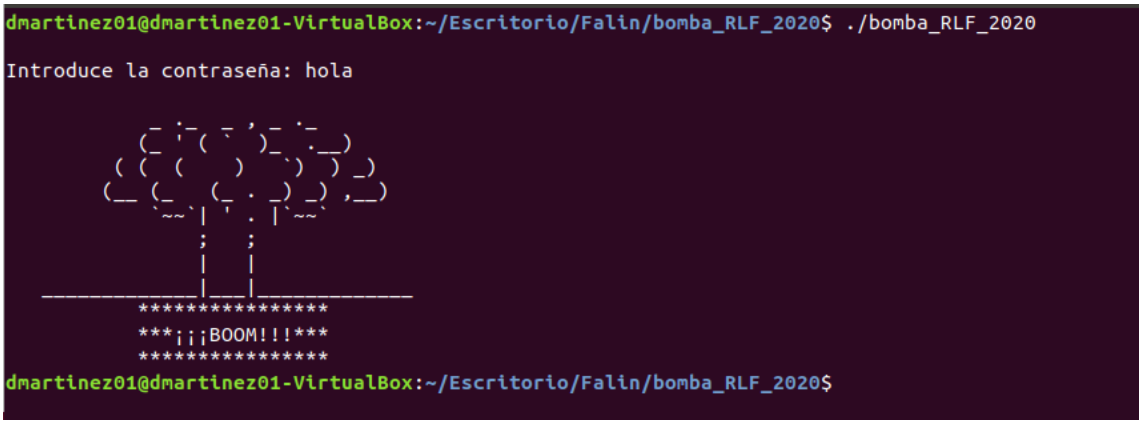
Desactivar Bomba Digital

David Martínez Díaz

Bomba_RLF_2020:

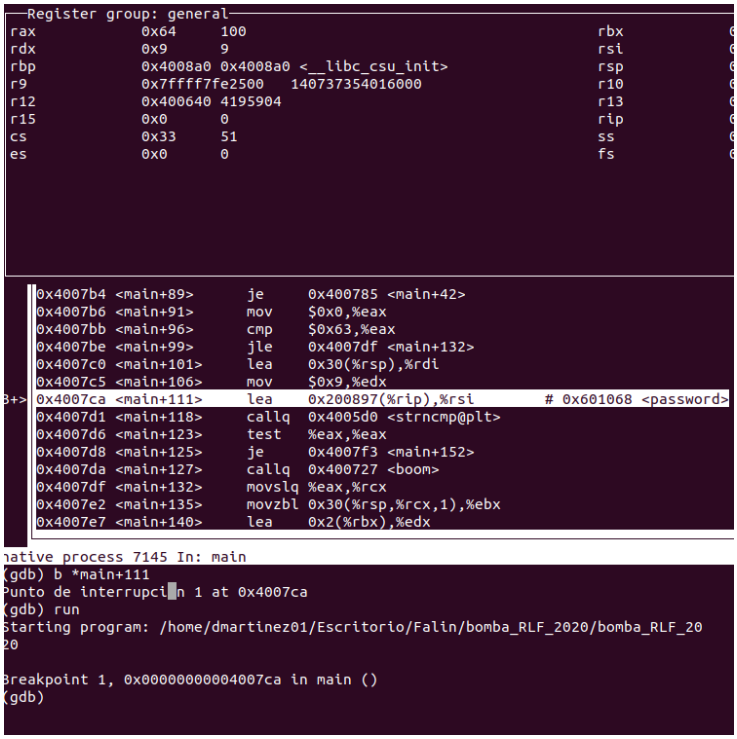
1.- En primer lugar es ejecutarlo, donde vemos que tenemos que averiguar su contraseña y pin correspondiente.



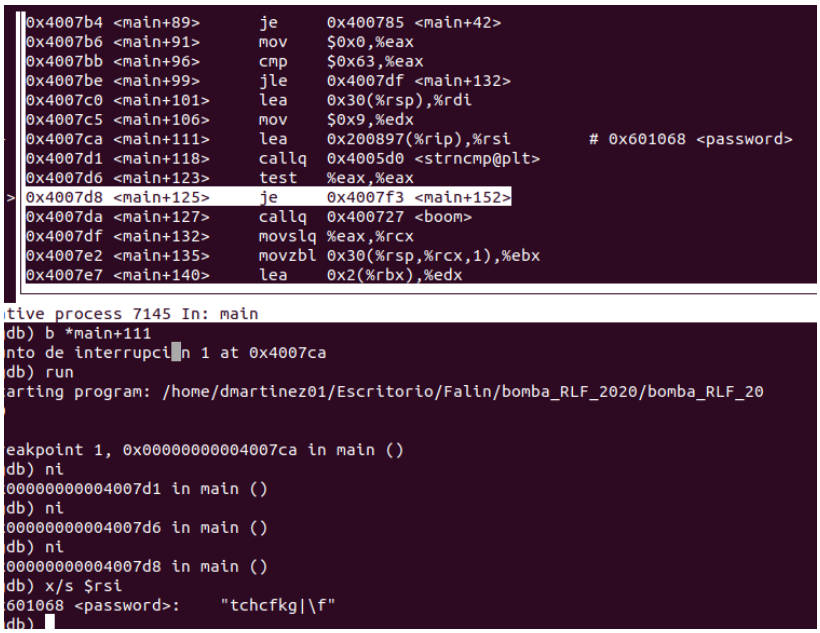
2.- Para ello debemos introducirnos en dicho ejecutable a través del debug e ir mirando los registros para comprobar y obtener las contraseñas.

→ gdb bomba
→ layout regs

Una vez estamos debugeando, hay que buscar el lugar exacto donde se comparan las contraseñas para poder continuar con el ejercicio, donde si nos damos cuenta, esta se realiza en el string compare, en la línea (*main+111).

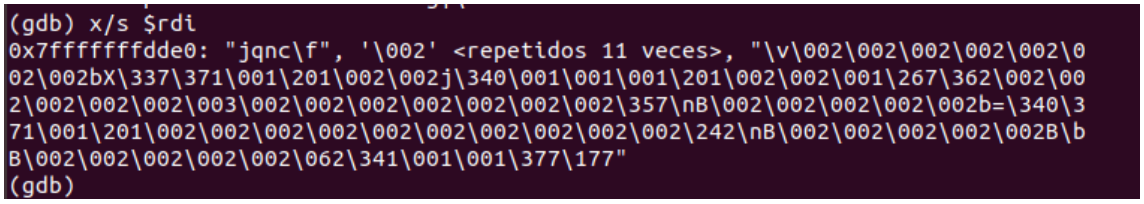


Por tanto, para sacar su contraseña debo ver los valores que hay en el registro %rsi, viendo así su contraseña correspondiente:



Esto quiere decir que la contraseña esta encriptada, y no vamos a poder poner directamente el resultado de %rsi, para ello podemos comprobar con nuestra contraseña anterior y mirar en el registro %rdi para ver dicha comparación y calcular esa razón correspondiente para saber cuánto hay que sumarlo o restarle a esta.

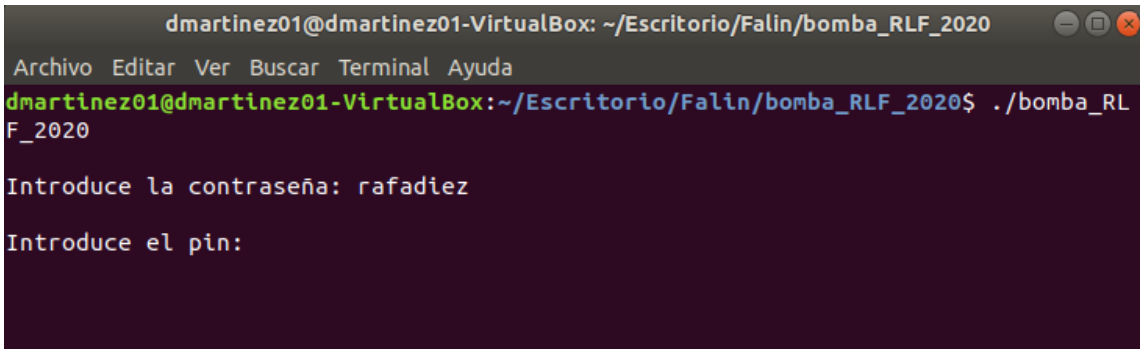
Por ello si introducimos la contraseña “hola” y nos introducimos en el registro %rdi obtenemos lo siguiente:



Donde nuestra nueva contraseña encriptada seria “jqnc”, para saber la razón de encriptación simplemente basta saber qué valor llega desde la primera letra de nuestra contraseña hasta la primera letra de la contraseña encriptada:
“hola” ---> “jqnc”;
“h” ---> “j”
Para sacarlo nos vamos a la tabla ASCII y vemos sus correspondientes valores:
“h” = 104 // “j” = 106
Con esto llegamos a la conclusión de que la razón es 2, y simplemente para saber su contraseña hay que restarle 2 a cada letra.

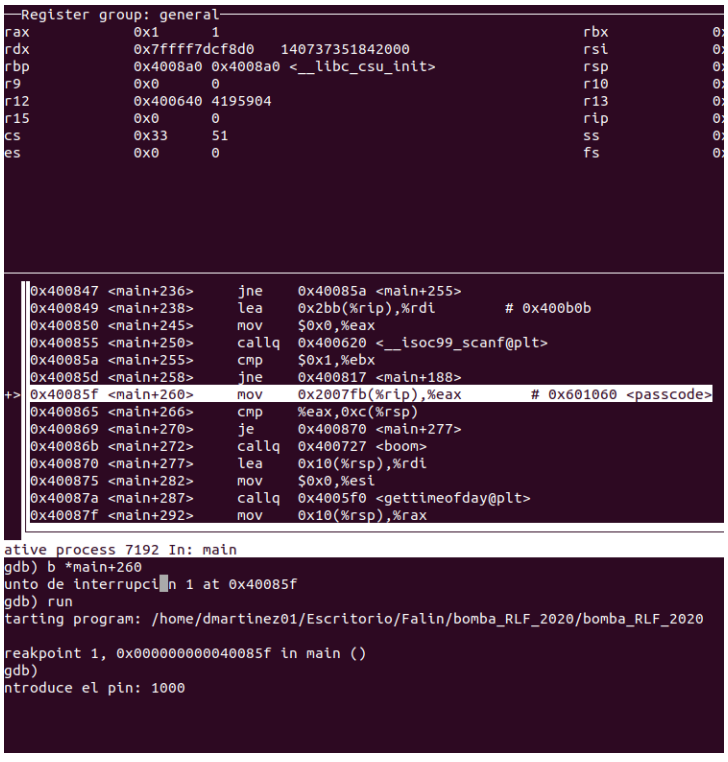
Consiguiendo así la contraseña encriptada:
“tchcfkg|” ---> “rafadiez”;

Vamos a comprobarlo:



Vemos que la contraseña era correcta pero se nos presenta otra problema, ahora nos pide un pin, veamos entonces de nuevo en el gdb, donde se encuentra este.

Como podemos ver se realiza otro string compare el cual vamos a analizar para saber si ahí se realiza la comparación entre pines. Analizando las sentencias llegamos hasta el main+260, donde se realiza una comparación entre los registros con la orden “jne”:



Donde si miramos bien las sentencias y hacemos un par de next instructions vemos como sacan un dato de la pila en la dirección de (%rip+0x2d10), y lo mete en el registro %eax, si lo mostramos vemos que:

```
Breakpoint 1, 0x000000000040085f in main ()
(gdb) ni
0x0000000000400865 in main ()
(gdb) ni
0x0000000000400869 in main ()
(gdb) print $eax
$1 = 1202
(gdb)
```

Vamos a comprobar si este pin es el correcto:

```
dmartinez01@dmartinez01-VirtualBox:~/Escritorio/Falin/bomba_RLF_2020$ ./bomba_RL
F_2020

Introduce la contraseña: rafadiez

Introduce el pin: 1202

       (◕‿◕)
.......................
··· bomba desactivada ···
.......................

dmartinez01@dmartinez01-VirtualBox:~/Escritorio/Falin/bomba_RLF_2020$
```

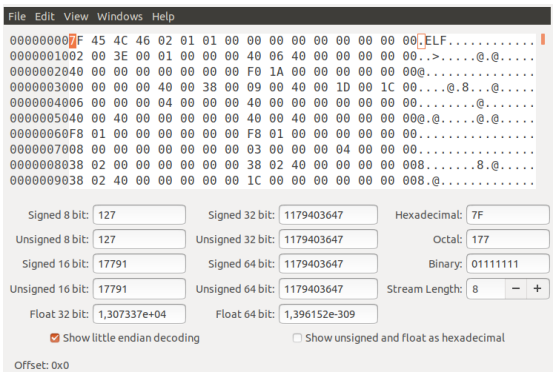
Como hemos podido comprobar el pin que habíamos obtenido era correcto y no se encontraba encriptado por lo que hemos podido desactivar la bomba. Por lo que esta sería la manera de desactivar la bomba.

- Modificar la contraseña y pin de la bomba:

Para modificar la contraseña vamos a utilizar el comando ghex que permite ver el código de manera hexadecimal:

"ghex bomba_MRG_2020"

Donde nos aparecerá lo siguiente:



Una vez estamos dentro, tenemos que buscar dicha contraseña, que en mi caso se encuentra encriptada:

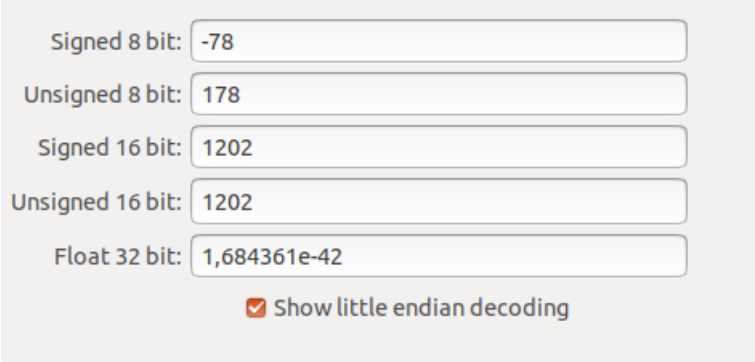
```
..........  .  ......................@.....
..@.......@.......@.......@.....&.@.....6.@
.............................tchcfkg|.GCC:
(Ubuntu 7.5.0-3ubuntu1~18.04) 7.5.0........
.................................8.@.........
```

Una vez que la hemos sacado vemos su Offset, simplemente si la modificamos debería cambiar (teniendo en cuenta la razón de encriptación).
Por ejemplo, si yo cambio la contraseña de esta manera:

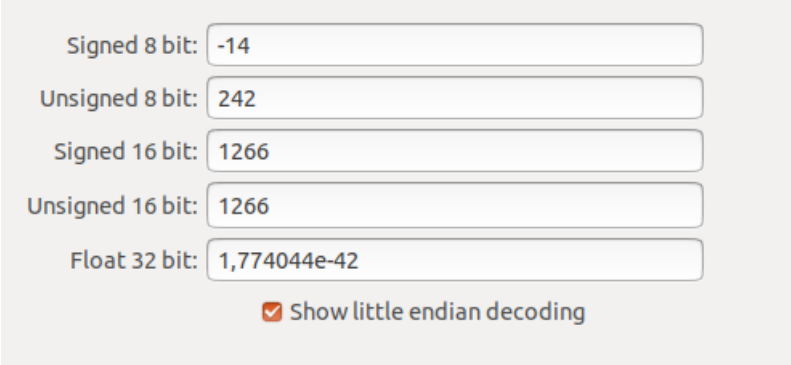
“Vacaroja” →”xcectqlc”

```
dmartinez01@dmartinez01-VirtualBox:~/Escritorio/Falin/bomba_RLF_2020$ ./bomba_RL
F_2020

Introduce la contraseña: vacaroja

Introduce el pin:
```

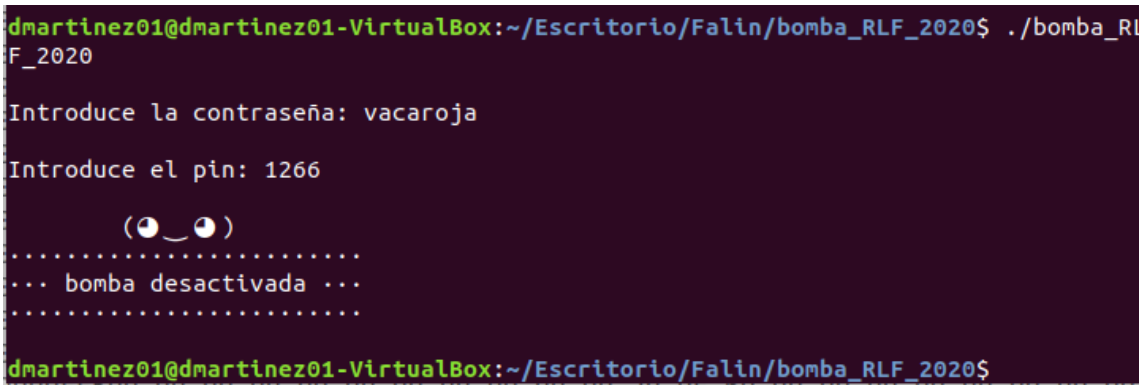
Vemos que si me acepta la contraseña y la hemos podido modificar con éxito.
Para modificar el pin, vamos a emplear otra vez el comando ghex:



Una vez encontramos nuestro pin, probamos a cambiarlo poniendo F4 por ejemplo, quedando:



Por ultimo vamos a comprobar si funciona:



Y confirmamos que se ha modificado con éxito.