MI BOMBA.
BOMBA JOSE MIGUEL HERNÁNDEZ GARCÍA

CONTRASEÑA: LANZAROTE
CÓDIGO: 954

Para desactivar mi bomba, lo que he hecho ha sido, en primer lugar, utilizar el comando ltrace -i -S ./bomba_JoseMiguelHernandezGarcia_1 que tras introducir la contraseña que he utilizado en las otras dos bombas que he desactivado, aaaaaaaaaaaa, he obtenido lo siguiente:

```
[0xf775dba0] SYS_write(26, "Introduce la contrase\303\261a: ", 4150598803Introduce la contraseña: )
[0xf775dba0] SYS_read(1024aaaaaaaaaaaa
, "aaaaaaaaaaaa\n", 4150598675)
[0x8048531] <... fgets resumed> "aaaaaaaaaaaa\n", 100, 0xf772f600)
[0x80487f0] strncmp("ccccccccc\220]\367x\236\224\377x\236\224\377\210\236\224\377\b\237\224\3779\205\004\b"..., "NCP\\CTQVG", 9)
[0x80486ca] putchar(10, 0xf7781938, 0xff949e58, 0x80487f0 <unfinished ...>
[0xf775dba0] SYS_write(1, "\nntroduce la contrase\303\261a: ", 4150598803
)                                                                                 = 1
[0x80486ca] <... putchar resumed> )
[0x80486d6] puts("***************" <unfinished ...>
[0xf775dba0] SYS_write(16, "***************\ntrase\303\261a: ", 4150598803***************
)                                                                                 = 16
[0x80486d6] <... puts resumed> )
[0x80486e2] puts("*** BOOM!!! ***" <unfinished ...>
[0xf775dba0] SYS_write(16, "*** BOOM!!! ***\ntrase\303\261a: ", 4150598803*** BOOM!!! ***
)                                                                                 = 16
[0x80486e2] <... puts resumed> )
[0x80486ee] puts("***************" <unfinished ...>
[0xf775dba0] SYS_write(16, "***************\ntrase\303\261a: ", 4150598803***************
)                                                                                 = 16
[0x80486ee] <... puts resumed> )
[0x80486fa] putchar(10, 0xf7781938, 0xff949e58, 0x80487f0 <unfinished ...>
[0xf775dba0] SYS_write(1, "\n***************\ntrase\303\261a: ", 4150598803
)                                                                                 = 1
[0x80486fa] <... putchar resumed> )
[0x8048706] exit(-1 <unfinished ...>
[0xf775dba0] SYS_exit_group(-143455536 <no return ...>
[0xffffffffffffffff] +++ exited (status 255) +++
ixjosemi@ixjosemi-GE70-2PE:~/MEGAsync/2nd_Computing/1st_Quart/EC/Practices/P_4$
```

Donde podemos ver que aparece la función strncmp("ccccccccc\220]\367x\236\224\377x\236\224\377\210\236\224\377\b\237\224\3779\205\004\b"..., "NCP\\CTQVG", 9), que nos muestra en primer lugar, nuestra contraseña (no toda, solo los nueve primeros caracteres dado que se puede ver que la longitud de la cadena que buscamos es 9 y la de nuestra contraseña es 11), codificada, posteriormente vemos una serie de números y tras ello podemos ver la cadena "NCP\\CTQVG" lo que nos da indicios de que esta puede ser la contraseña que buscamos codificada.

Así pues, si vemos como se ha codificado nuestra contraseña, ha pasado de ser aaaaaaaaaaaa a ser ccccccccc por lo que podemos intuir que lo que ha ocurrido es que a cada carácter se le ha sumado un 2 en su codificación ASCII, por tanto si aplicamos de forma inversa esta codificación a la cadena "NCP\\CTQVG", podemos ver que aparece la cadena LANZAROTE (tras ir restando 2 a cada caracteres y gracias a la tabla ASCII), que resulta ser la contraseña que buscábamos.

```
ixjosemi@ixjosemi-GE70-2PE:~/MEGAsync/2nd_Computing/1st_Quart/EC/Practices/P_4$ ./bomba_JoseMiguelHernandezGarcia_1
Introduce la contraseña: LANZAROTE
Introduce el código:
```

Tras ello podemos pasar a buscar el código que necesitamos para terminar de desactivar nuestra bomba, y para ello he recurrido a la mejor herramienta que puede existir, el gdb.

En primer lugar, tras varios minutos investigando mi propio código, he dado con el siguiente fragmento de código en ensamblador:

```
0x08048579 <+153>:   call   0x80484c0 <__isoc99_scanf@plt>
0x0804857e <+158>:   mov    0x804a03c,%eax
0x08048583 <+163>:   add    $0x10,%esp
0x08048586 <+166>:   add    $0x5,%eax
0x08048589 <+169>:   lea    (%eax,%eax,8),%eax
0x0804858c <+172>:   cmp    %eax,-0x94(%ebp)
0x08048592 <+178>:   mov    %eax,0x804a03c
0x08048597 <+183>:   je     0x804859e <main+190>
0x08048599 <+185>:   call   0x80486c0 <fail>
```

Donde vemos que en primer lugar se llama a la función scanf que se utiliza para leer el código(Y aquí he colocado un punto de ruptura para poder trabajar con este fragmento de código de forma más cómoda y he utilizado como código “1111” para poder saltarme esta función) y posteriormente, se mueve lo que hay en la dirección de memoria 0x804a03c al registro $eax, que si imprimimos en pantalla lo que hay en ese registro obtenemos:

```
(gdb) print $eax
$1 = 101
```

Pero vemos que posteriormente, aparece la instrucción

```
add    $0x5,%eax
```

que le está sumando 5 a ese 101 que hemos encontrado y a esto le sigue la instrucción

```
lea    (%eax,%eax,8),%eax
```

que lo que hace es multiplicar el resultado anterior por 9, por tanto obtenemos (101 + 5) * 9 que finalmente vuelve a guardarse en $eax y en la siguiente instrucción se compara $eax con -094x(%ebp) que es donde se ha guardado la instrucción que nosotros hemos introducido. Por tanto si hacemos print $eax obtenemos:

```
(gdb) print $eax
$2 = 954
```

Que es el resultado de (101 + 5) * 9. Por lo que este es el código que nosotros buscábamos, por tanto ya hemos encontrado la contraseña y el código.

```
ixjosemi@ixjosemi-GE70-2PE:~/MEGAsync/2nd_Computing/1st_Quart/EC/Practices/P_4$ ./bomba_JoseMiguelHernandezGarcia_1
Introduce la contraseña: LANZAROTE
Introduce el código: 954

************************
*** bomba desactivada ***
************************

ixjosemi@ixjosemi-GE70-2PE:~/MEGAsync/2nd_Computing/1st_Quart/EC/Practices/P_4$
```