BOMBA DE SANTIAGO VIDAL MARTINEZ

CONTRASEÑA: adivinaestaclave
CÓDIGO: 2000

En primer lugar, para averiguar esta contraseña, he utilizado (como en anteriores casos) el comando ltrace -i -S ./bomba, mediante el cual he obtenido lo siguiente tras introducir una contraseña aleatoria, que en este caso ha vuelto a ser aaaaaaaaaaaa:

```
[0xf777cba0] SYS_write(26, "Introduce la contrase\303\261a: ", 4150725779Introduce la contraseña: )
[0xf777cba0] SYS_read(1024aaaaaaaaaaaa
, "aaaaaaaaaaaa\n", 4150725651)
[0x8048734] <... fgets resumed> "aaaaaaaaaaaa\n", 100, 0xf774e600)
[0x804876f] strncmp("aaaaaaaaaaaa\n", "adivinaestaclave", 16)
[0x80485b6] puts("***************" <unfinished ...>
[0xf777cba0] SYS_write(16, "***************\ntrase\303\261a: ", 4150725779***************
)                                                                                    = 16
[0x80485b6] <... puts resumed> )
[0x80485c2] puts("*** BOOM!!! ***" <unfinished ...>
[0xf777cba0] SYS_write(16, "*** BOOM!!! ***\ntrase\303\261a: ", 4150725779*** BOOM!!! ***
)                                                                                    = 16
[0x80485c2] <... puts resumed> )
[0x80485ce] puts("***************" <unfinished ...>
[0xf777cba0] SYS_write(16, "***************\ntrase\303\261a: ", 4150725779***************
)                                                                                    = 16
[0x80485ce] <... puts resumed> )
[0x80485da] exit(-1 <unfinished ...>
[0xf777cba0] SYS_exit_group(-143328560 <no return ...>
[0xffffffffffffffff] +++ exited (status 255) +++
ixjosemi@ixjosemi-GE70-2PE:~/Downloads$
```

Donde podemos ver que aparece la función strncmp("aaaaaaaaaaaa\n", "adivinaestaclave", 16) donde vemos claramente que compara la contraseña que nosotros hemos introducido, con el tamaño de su cadena que es 16 y con la contraseña, sin codificar, “adivinaestaclave”.

Por otro lado, para encontrar el código que desactiva esta bomba, he vuelto a recurrir al gdb(un gran compañero) para estudiar el código en ensamblador, de donde he extraído el siguiente fragmento que es de donde he obtenido la clave:

```
0x080487c1 <+236>:   call   0x80484d0 <__isoc99_scanf@plt>
0x080487c6 <+241>:   mov    0x34(%esp),%edx
0x080487ca <+245>:   mov    0x804a084,%eax
0x080487cf <+250>:   cmp    %eax,%edx
0x080487d1 <+252>:   je     0x80487d8 <main+259>
0x080487d3 <+254>:   call   0x80485a4 <boom>
```

En primer lugar vemos como llama a la función scanf para leer el código, y tras ello mueve el código que introducimos al registro $edx.
Posteriormente mueve lo que hay en la dirección de memoria 0x804a084 al registro $eax para finalmente comparar $eax con $edx, por lo que podemos intuir que en $eax se encuentra el código y efectivamente, tras hacer print $eax obtenemos:

```
(gdb) print $eax
$1 = 2000
```

Por tanto el código que estábamos buscando era 2000.

Y efectivamente, tras introducir la contraseña y el código que hemos obtenido, se desactiva la bomba: