Explicación de las bombas desactivadas

David Infante Casas
75165296P
davidinfante@correo.ugr.es
Grupo de prácticas: D1

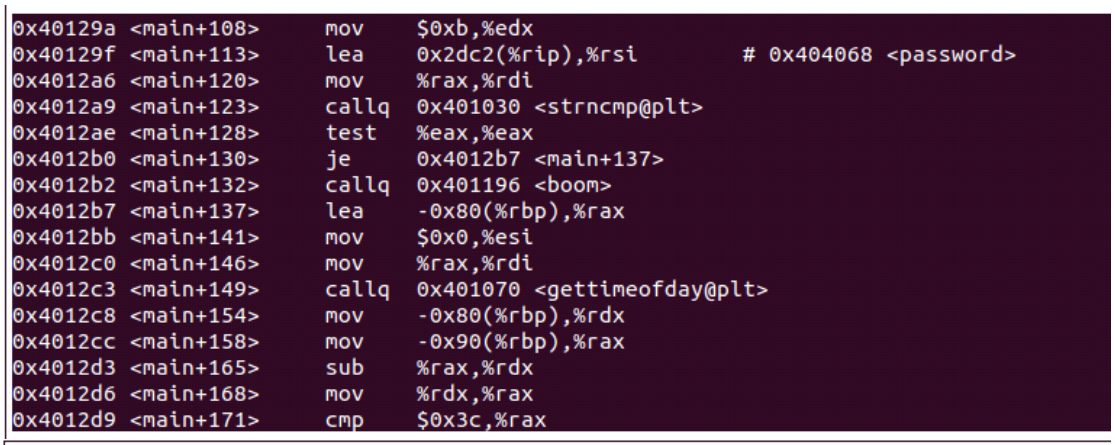
Se ha usado la herramienta gdb.

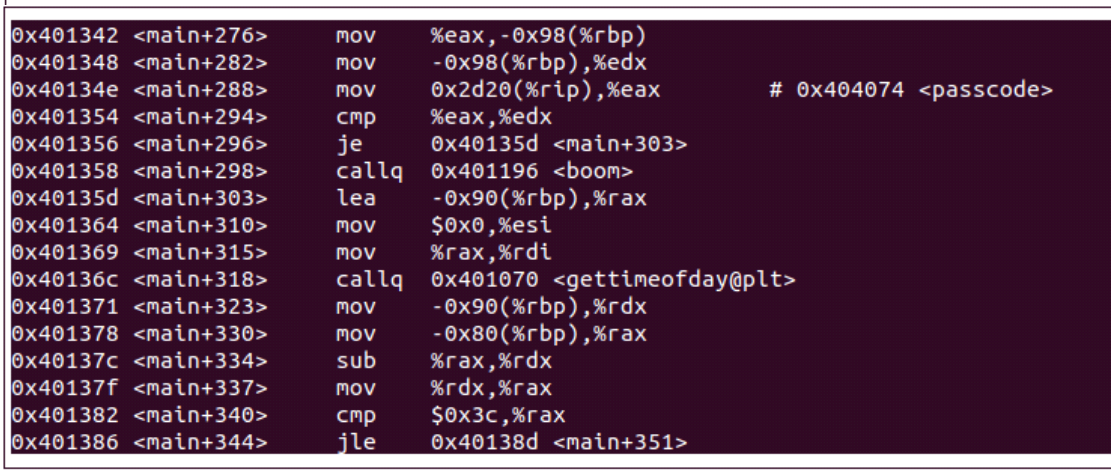
Las bombas desactivadas son de:
- Francisco Javier Bolívar
- Enrique Moreno Carmona

Bomba de Francisco Javier Bolívar

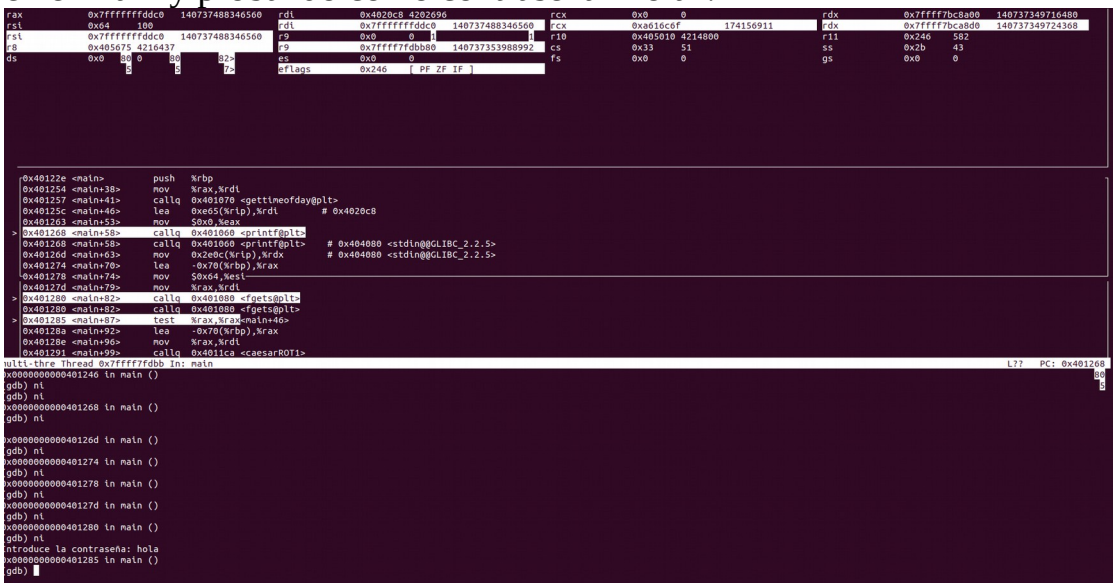
La contraseña y pin originales que se han de escribir son: “aaabbbaaa\n” y 1234
La contraseña y pin modificados que lee el programa son: “bbbcccbbb\n” y 1238

Para descubrir las contraseñas y pines, lo primero que he comprobado ha sido si se encontraban las direcciones de memoria donde se guardan dichas variables en el código asm que ofrece gdb, y así ha sido, siendo 0x404068 para bbbcccbbb y 0x404074 para 1328.

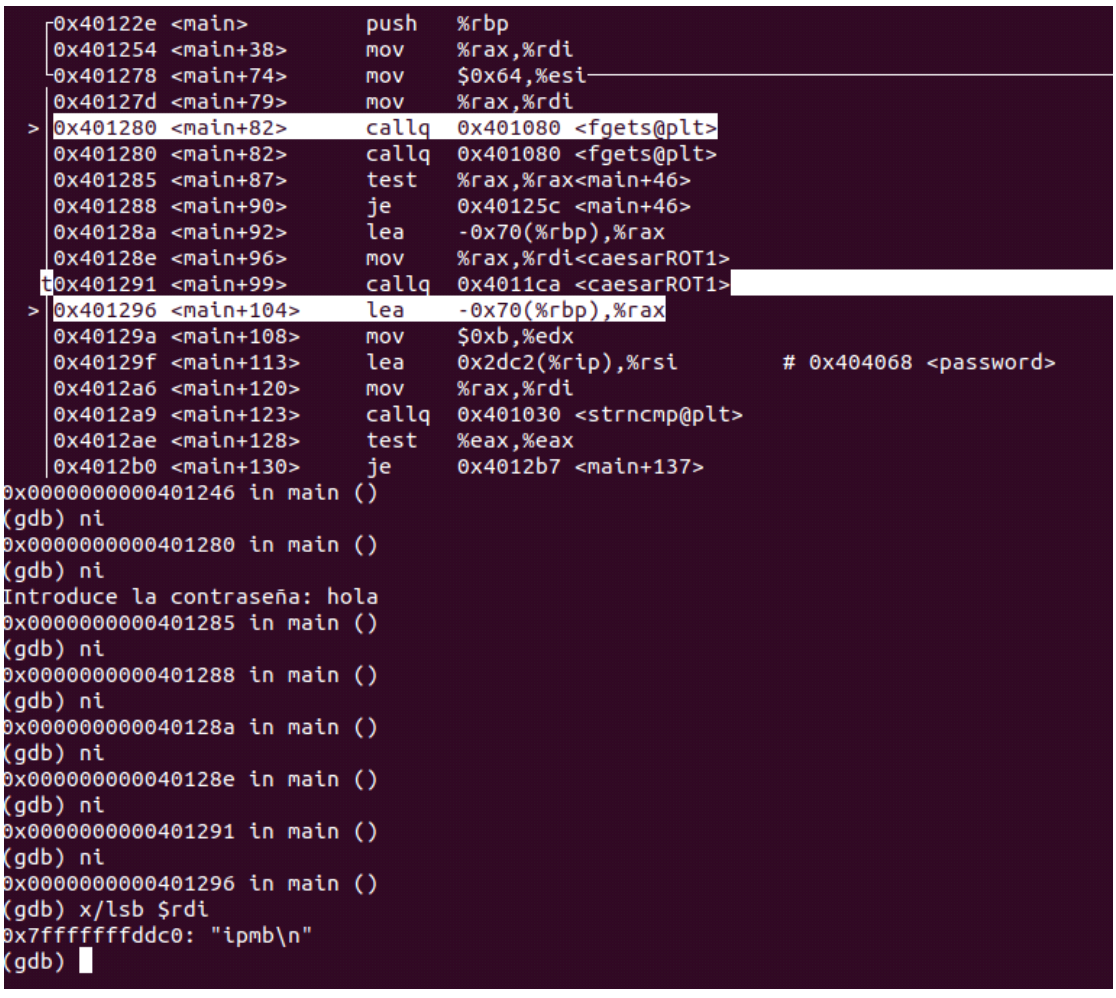




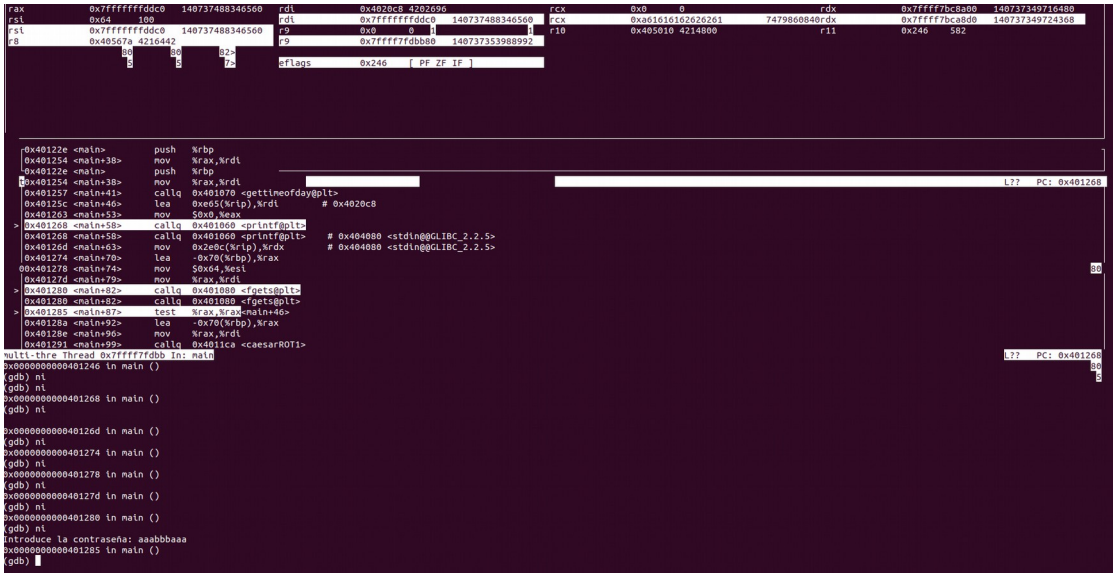
A continuación he iniciado una ejecución del programa estableciendo un breakpoint en el main y probando como contraseña “hola”.



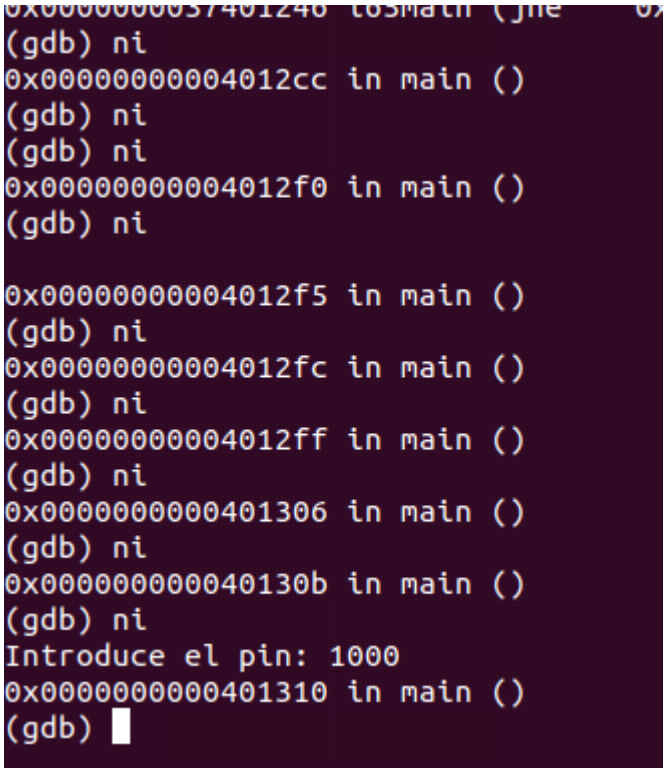
Avanzamos en la ejecución hasta que modifica la contraseña y comprobamos en el registro %rdi que nos devuelve “ipmb\n”. Pensando un poco, me doy cuenta que tiene el mismo número de caracteres que “hola” y además, cada carácter es “uno más” de su posición lógica en el abecedario, por tanto, si la clave es “bbbcccbbb”, la que debemos introducir es “**aaabbbaaa**”.



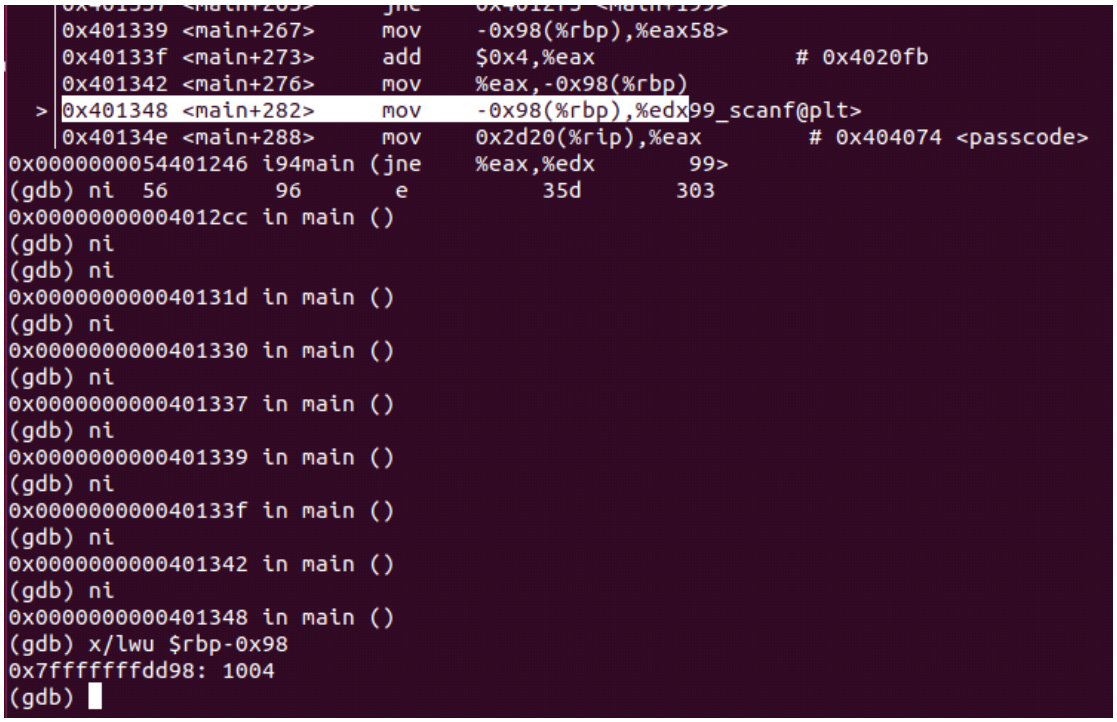
Reiniciamos la ejecución para introducir la contraseña correcta e intentar averiguar el pin.



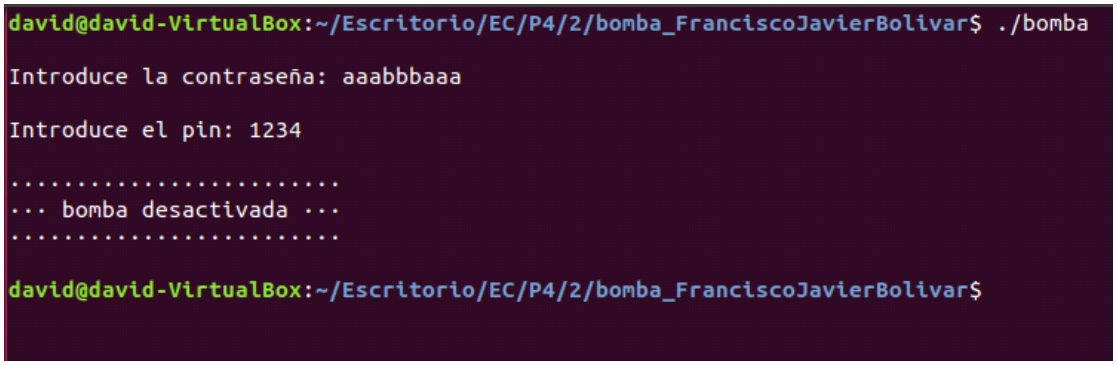
Nos pide el pin, e introducimos 1000 como prueba.



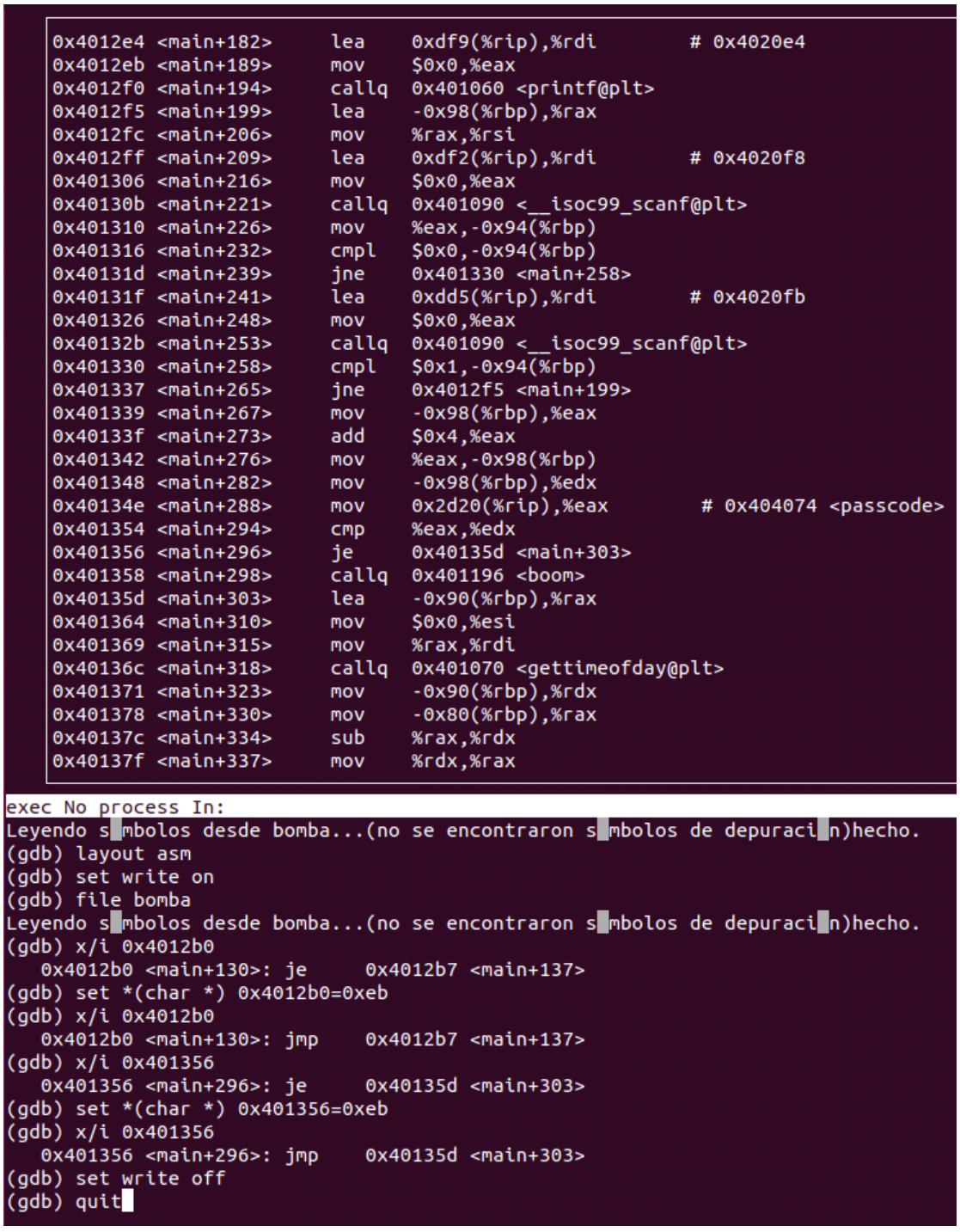
Comprobamos el pin modificado en el registro %rbp-0x98 y nos devuelve 1004, podemos suponer rápidamente que el programa suma 4 a nuestro pin por tanto, si el pin con el que se compara es 1238, el pin debe ser 4 menos, es decir, **1234**.



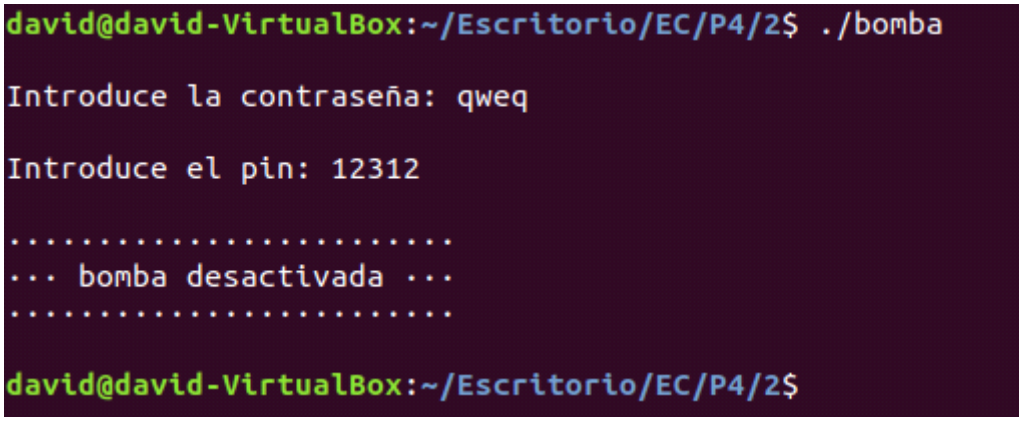
Como ya tenemos ambos, contraseña y pin, los probamos en una ejecución de la bomba.
La bomba es desactivada con éxito.



Para modificar la bomba y que la contraseña y pin introducidos den igual, vamos a modificar ambos saltos en el código ensamblador usando gdb y la función set write on. Modificamos el código como se muestra en la imagen.



Probamos la bomba nueva.
Funciona.



Bomba de Enrique Moreno Carmona

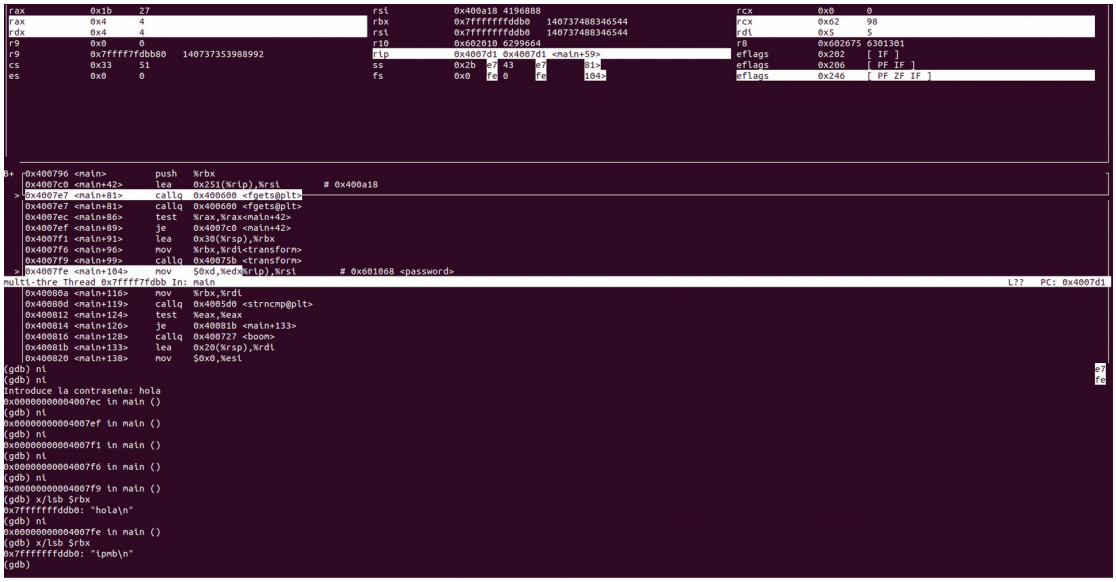
La contraseña y pin originales que se han de escribir son: “rdmcmnnckdr\n” y 1800
La contraseña y pin modificados que lee el programa son: “sendnoodles\n” y 1800

Al igual que antes, compruebo si están la password y el passcode siendo la dirección 0x601080 para la contraseña sendnoodles y 0x601060 para el pin 1800.

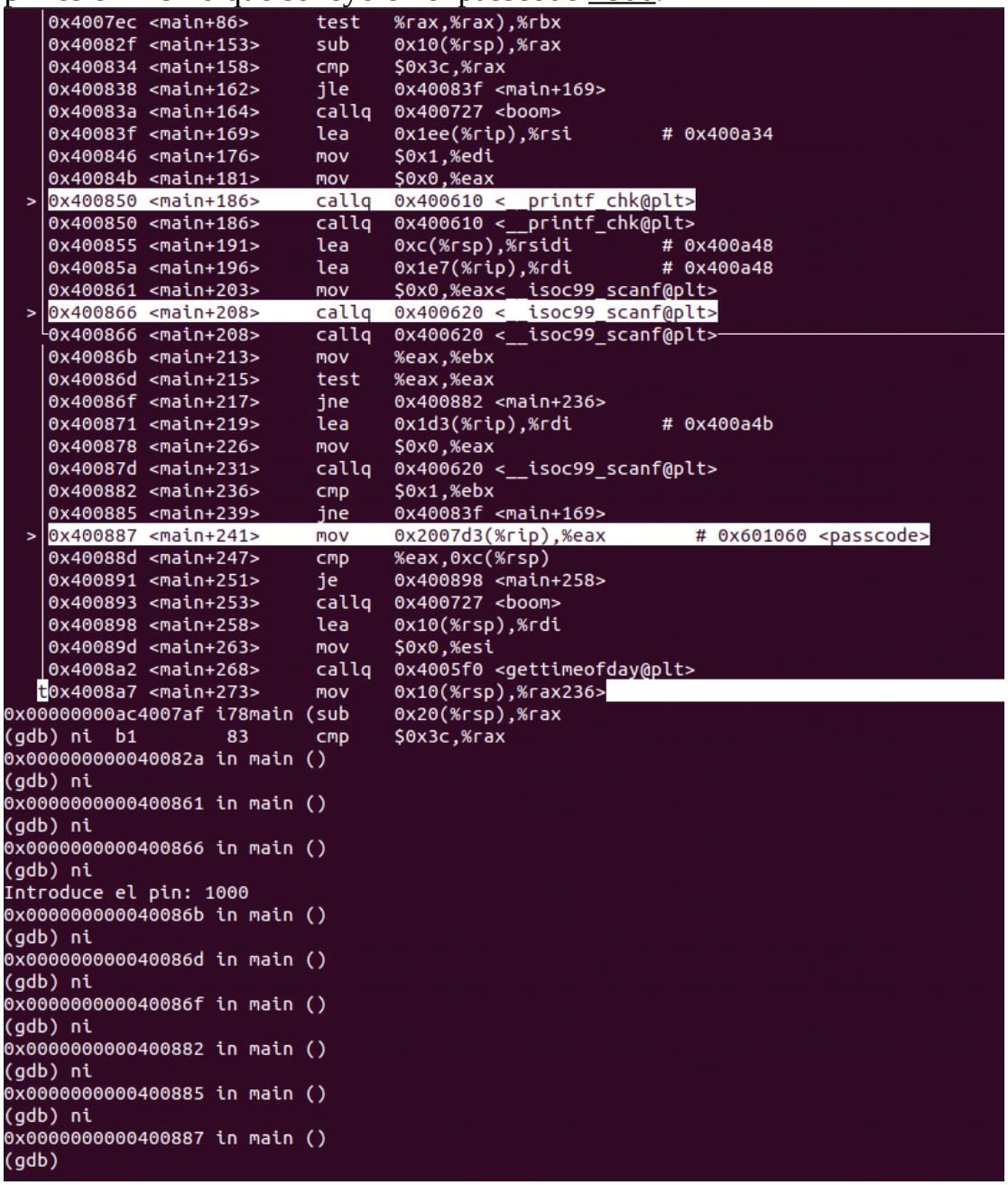
```
0x4007f1 <main+91>      lea    0x30(%rsp),%rbx
0x4007f6 <main+96>      mov    %rbx,%rdi
0x4007f9 <main+99>      callq  0x40075b <transform>
0x4007fe <main+104>     mov    $0xd,%edx
0x400803 <main+109>     lea    0x20085e(%rip),%rsi        # 0x601068 <password>
0x40080a <main+116>     mov    %rbx,%rdi
0x40080d <main+119>     callq  0x4005d0 <strncmp@plt>
0x400812 <main+124>     test   %eax,%eax
0x400814 <main+126>     je     0x40081b <main+133>
0x400816 <main+128>     callq  0x400727 <boom>
0x40081b <main+133>     lea    0x20(%rsp),%rdi
0x400820 <main+138>     mov    $0x0,%esi
0x400825 <main+143>     callq  0x4005f0 <gettimeofday@plt>
0x40082a <main+148>     mov    0x20(%rsp),%rax
0x40082f <main+153>     sub    0x10(%rsp),%rax
0x400834 <main+158>     cmp    $0x3c,%rax
```

```
0x400878 <main+226>     mov    $0x0,%eax
0x40087d <main+231>     callq  0x400620 <__isoc99_scanf@plt>
0x400882 <main+236>     cmp    $0x1,%ebx
0x400885 <main+239>     jne    0x40083f <main+169>
0x400887 <main+241>     mov    0x2007d3(%rip),%eax        # 0x601060 <passcode>
0x40088d <main+247>     cmp    %eax,0xc(%rsp)
0x400891 <main+251>     je     0x400898 <main+258>
0x400893 <main+253>     callq  0x400727 <boom>
0x400898 <main+258>     lea    0x10(%rsp),%rdi
0x40089d <main+263>     mov    $0x0,%esi
0x4008a2 <main+268>     callq  0x4005f0 <gettimeofday@plt>
0x4008a7 <main+273>     mov    0x10(%rsp),%rax
0x4008ac <main+278>     sub    0x20(%rsp),%rax
0x4008b1 <main+283>     cmp    $0x3c,%rax
0x4008b5 <main+287>     jle    0x4008bc <main+294>
0x4008b7 <main+289>     callq  0x400727 <boom>
```

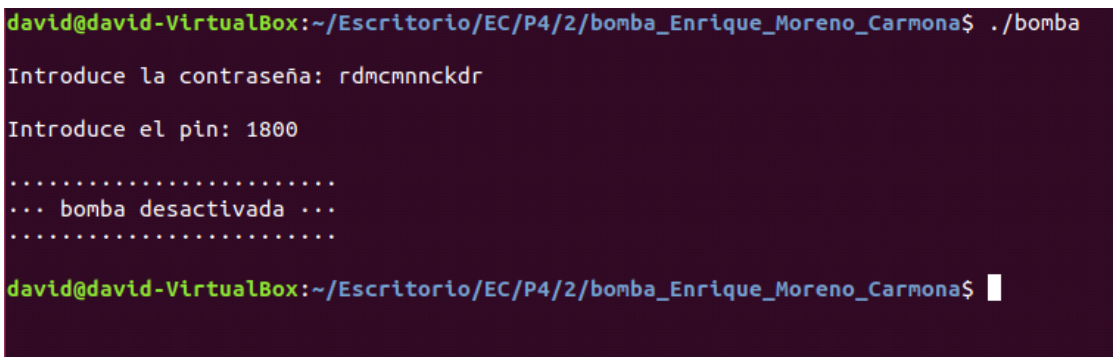
Una vez hecho esto, comenzamos la ejecución igual que antes y en la contraseña probamos de nuevo “hola”. Comprobando el registro %rbx nos devuelve la cadena modificada como “ipmb\n”. Casualmente es exactamente lo mismo que nos devolvió la bomba anterior así que podemos asumir que lo que hace la bomba es lo mismo, dar el valor siguiente a cada carácter en el abecedario, por tanto, si la contraseña es sendnoodles, y pensamos un poco, obtenemos la cadena a introducir: “**rdmcmnnckdr**”.



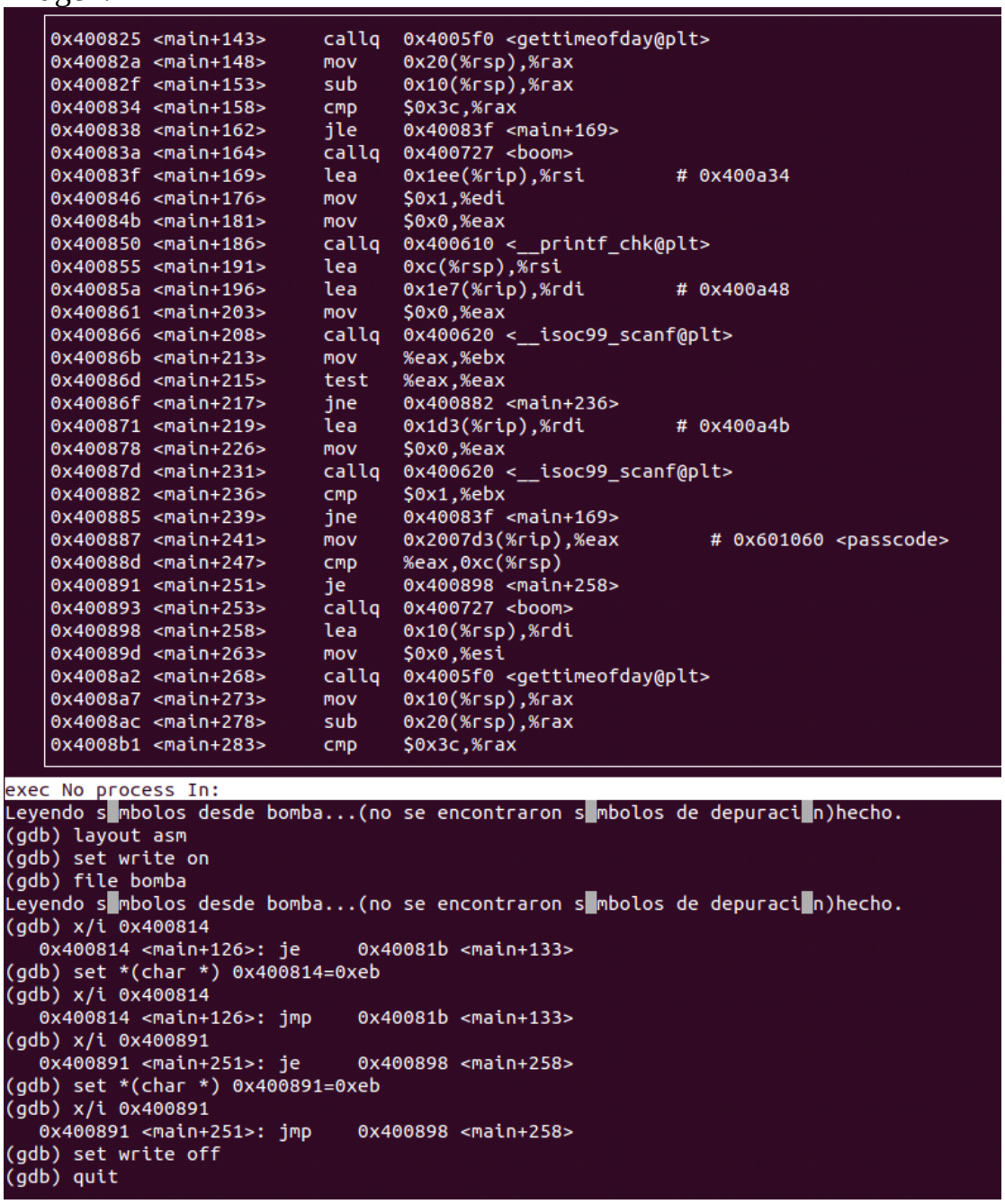
Ahora vemos el pin, probando como antes con 1000. Sin embargo, leyendo el código, vemos que no se pasa ninguna función que modifique al pin, esto quiere decir, que el pin es el mismo que se leyó en el passcode **1800**.



Probamos a ejecutar la bomba con esta contraseña y pin.
Y se desactiva correctamente.



Modificamos esta bomba de la misma forma que la anterior, tal y como se ve en la imagen.



```
0x400825 <main+143>     callq  0x4005f0 <gettimeofday@plt>
0x40082a <main+148>     mov    0x20(%rsp),%rax
0x40082f <main+153>     sub    0x10(%rsp),%rax
0x400834 <main+158>     cmp    $0x3c,%rax
0x400838 <main+162>     jle    0x40083f <main+169>
0x40083a <main+164>     callq  0x400727 <boom>
0x40083f <main+169>     lea    0x1ee(%rip),%rsi        # 0x400a34
0x400846 <main+176>     mov    $0x1,%edi
0x40084b <main+181>     mov    $0x0,%eax
0x400850 <main+186>     callq  0x400610 <__printf_chk@plt>
0x400855 <main+191>     lea    0xc(%rsp),%rsi
0x40085a <main+196>     lea    0x1e7(%rip),%rdi        # 0x400a48
0x400861 <main+203>     mov    $0x0,%eax
0x400866 <main+208>     callq  0x400620 <__isoc99_scanf@plt>
0x40086b <main+213>     mov    %eax,%ebx
0x40086d <main+215>     test   %eax,%eax
0x40086f <main+217>     jne    0x400882 <main+236>
0x400871 <main+219>     lea    0x1d3(%rip),%rdi        # 0x400a4b
0x400878 <main+226>     mov    $0x0,%eax
0x40087d <main+231>     callq  0x400620 <__isoc99_scanf@plt>
0x400882 <main+236>     cmp    $0x1,%ebx
0x400885 <main+239>     jne    0x40083f <main+169>
0x400887 <main+241>     mov    0x2007d3(%rip),%eax        # 0x601060 <passcode>
0x40088d <main+247>     cmp    %eax,0xc(%rsp)
0x400891 <main+251>     je     0x400898 <main+258>
0x400893 <main+253>     callq  0x400727 <boom>
0x400898 <main+258>     lea    0x10(%rsp),%rdi
0x40089d <main+263>     mov    $0x0,%esi
0x4008a2 <main+268>     callq  0x4005f0 <gettimeofday@plt>
0x4008a7 <main+273>     mov    0x10(%rsp),%rax
0x4008ac <main+278>     sub    0x20(%rsp),%rax
0x4008b1 <main+283>     cmp    $0x3c,%rax
exec No process In:
Leyendo s mbolos desde bomba...(no se encontraron s mbolos de depuraci n)hecho.
(gdb) layout asm
(gdb) set write on
(gdb) file bomba
Leyendo s mbolos desde bomba...(no se encontraron s mbolos de depuraci n)hecho.
(gdb) x/i 0x400814
   0x400814 <main+126>: je     0x40081b <main+133>
(gdb) set *(char *) 0x400814=0xeb
(gdb) x/i 0x400814
   0x400814 <main+126>: jmp    0x40081b <main+133>
(gdb) x/i 0x400891
   0x400891 <main+251>: je     0x400898 <main+258>
(gdb) set *(char *) 0x400891=0xeb
(gdb) x/i 0x400891
   0x400891 <main+251>: jmp    0x400898 <main+258>
(gdb) set write off
(gdb) quit
```

La probamos y funciona.

```
david@david-VirtualBox:~/Escritorio/EC/P4/2$ ./bomba

Introduce la contraseña: a

Introduce el pin: 1

.........................
... bomba desactivada ...
.........................

david@david-VirtualBox:~/Escritorio/EC/P4/2$
```