

# Desactivación Bomba de Javier Bueno

Estructura de Computadores - Grupo C3

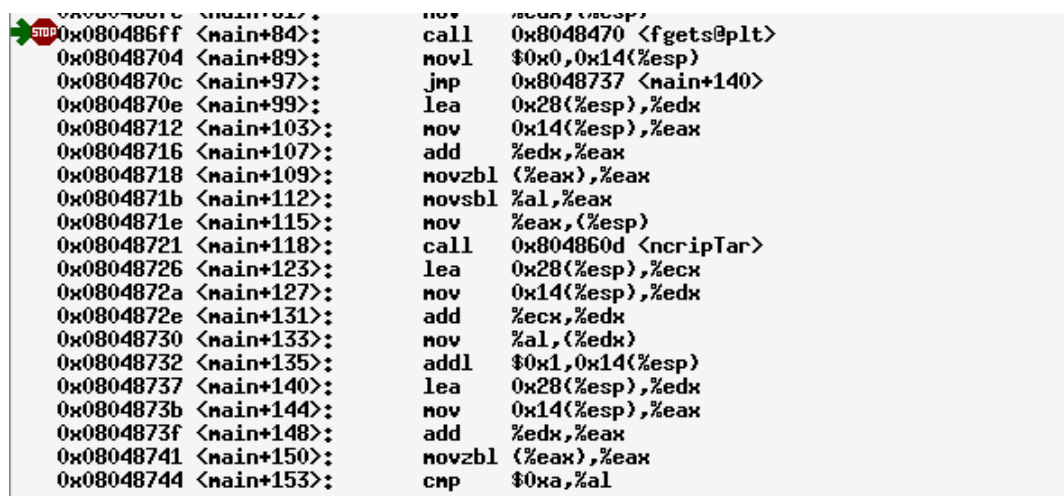
Mario Rodríguez Ruiz

## 1. Contraseña

Para averiguar la contraseña se ha utilizado el depurador **DDD** realizando los siguientes pasos:

En primer lugar se ha puesto un punto de ruptura en la llamada a **fgets**, que es cuando se le pide al usuario por pantalla que ingrese una contraseña.

Una vez funcionando el programa y detenido ahí (como se ve en la Figura 1.1) se ha metido una contraseña al azar (**hola**) para avanzar.



```
0x080486ff <main+84>: call 0x8048470 <fgets@plt>
0x08048704 <main+89>: movl $0x0,0x14(%esp)
0x0804870c <main+97>: jmp 0x8048737 <main+140>
0x0804870e <main+99>: lea 0x28(%esp),%edx
0x08048712 <main+103>: mov 0x14(%esp),%eax
0x08048716 <main+107>: add %edx,%eax
0x08048718 <main+109>: movzbl (%eax),%eax
0x0804871b <main+112>: movsbl %al,%eax
0x0804871e <main+115>: mov %eax,(%esp)
0x08048721 <main+118>: call 0x804860d <ncripTar>
0x08048726 <main+123>: lea 0x28(%esp),%ecx
0x0804872a <main+127>: mov 0x14(%esp),%edx
0x0804872e <main+131>: add %ecx,%edx
0x08048730 <main+133>: mov %al,(%edx)
0x08048732 <main+135>: addl $0x1,0x14(%esp)
0x08048737 <main+140>: lea 0x28(%esp),%edx
0x0804873b <main+144>: mov 0x14(%esp),%eax
0x0804873f <main+148>: add %edx,%eax
0x08048741 <main+150>: movzbl (%eax),%eax
0x08048744 <main+153>: cmp $0xa,%al
```

Figura 1.1: Comienzo de la depuración desde DDD

Una vez introducida la contraseña por consola, el programa entra en una función llamada **ncripTar** para modificar todos los componentes de la cadena.

Se puede demostrar que se han cambiado todos éstos viendo el contenido del registro que contiene ahora la contraseña modificada justo después de salir de **ncripTar**.

Para ello se ha utilizado la herramienta **Data→Memory**, volcando el contenido de **%edx** en pantalla.

En la Figura 1.2 puede verse que el valor de la cadena después del " encriptado " es **]daV** . Esto supone que se ha realizado una **resta con valor 11** sobre cada uno de los componentes de la cadena.

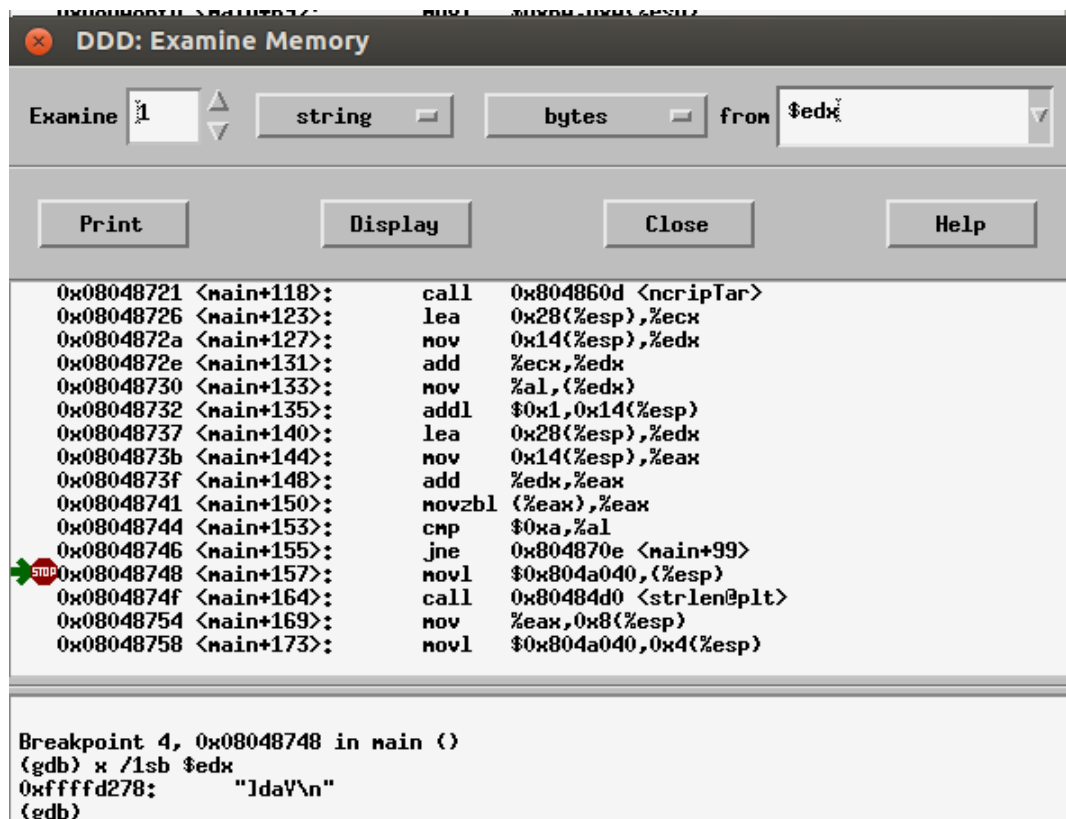


Figura 1.2: Contraseña introducida modificada

Ahora tan solo falta encontrar una supuesta contraseña con la que se compare la que se ha introducido. Lo que se hace es volcar el contenido del registro que se encuentra justo antes de la comparación de ambas, ya que es ahí donde se encuentra liberado. Este volcado se consigue mediante la misma herramienta que en el caso anterior (**Data→Memory**), pero cambiando el valor del registro, que será: **0x804a040**.

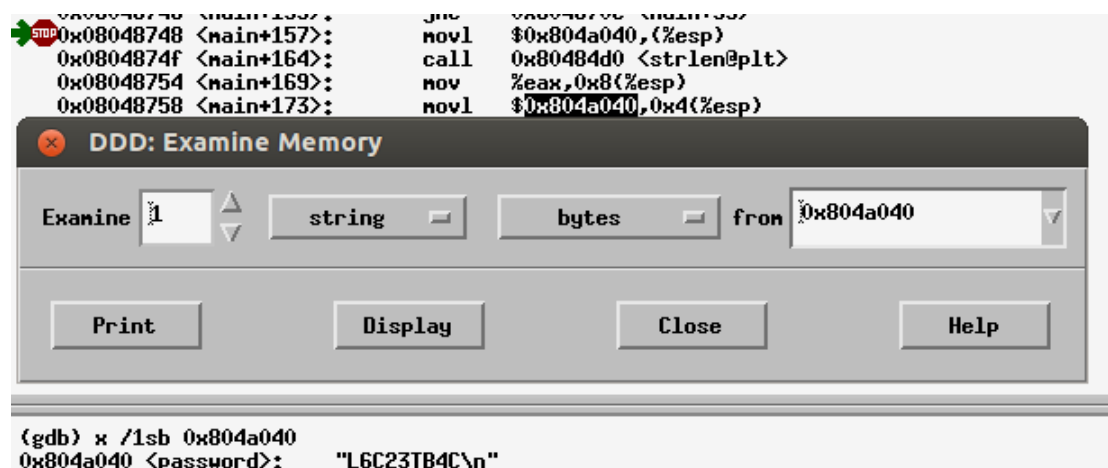


Figura 1.3: Valor de la contraseña a buscar encriptada

El valor que aparece en la Figura 1.3 (**L6C23TB4C**) se trata de la contraseña que se está buscando pero con el único inconveniente de estar cifrada (mediante la función que se vio anteriormente: **ncripTar**).

Su valor original se obtiene al hacer la función inversa, es decir, sumándole 11 a cada componente de la cadena.

Contraseña: **WAN=>\_M?N**

## 2. Código

Para averiguar la contraseña se ha utilizado el depurador **DDD** realizando los siguientes pasos:

Llegando a la sección del programa que se encarga de procesar y validar el código, se ha puesto un punto de ruptura en esta parte para futuros intentos.

En este punto el programa vuelve a solicitar datos, en este caso los correspondientes al código. El código introducido como prueba es **1111**, tal y como se ve en la Figura 2.1 en el estado de registros (**Status→Registers**)

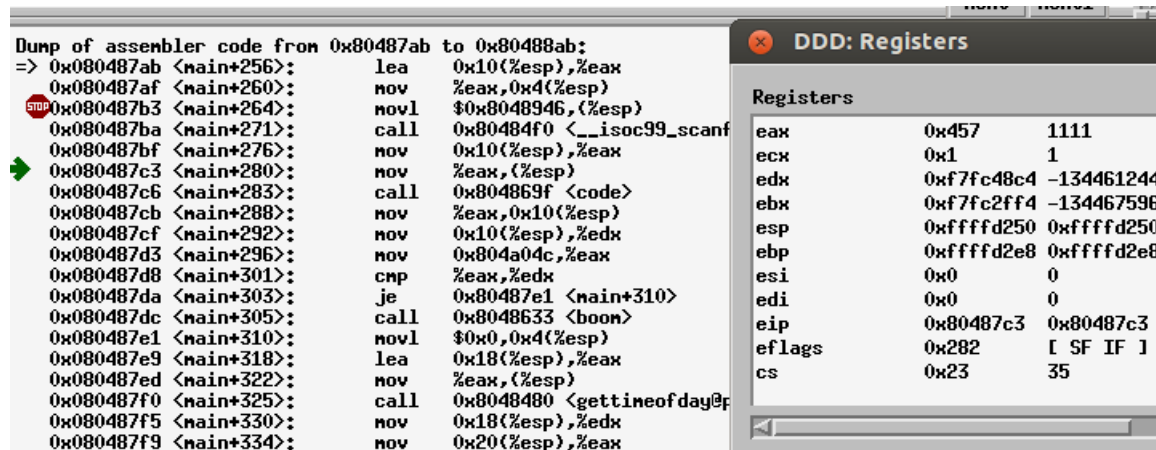


Figura 2.1: Status Registers desde DDD para el código

Siguiendo el trascurso del programa mediante **Nexti** y manteniendo la ventana del estado de registros abierta, se puede comprobar cómo el valor del código introducido ha sido modificado. Ahora su valor es de **1090** como presenta la Figura 2.2.

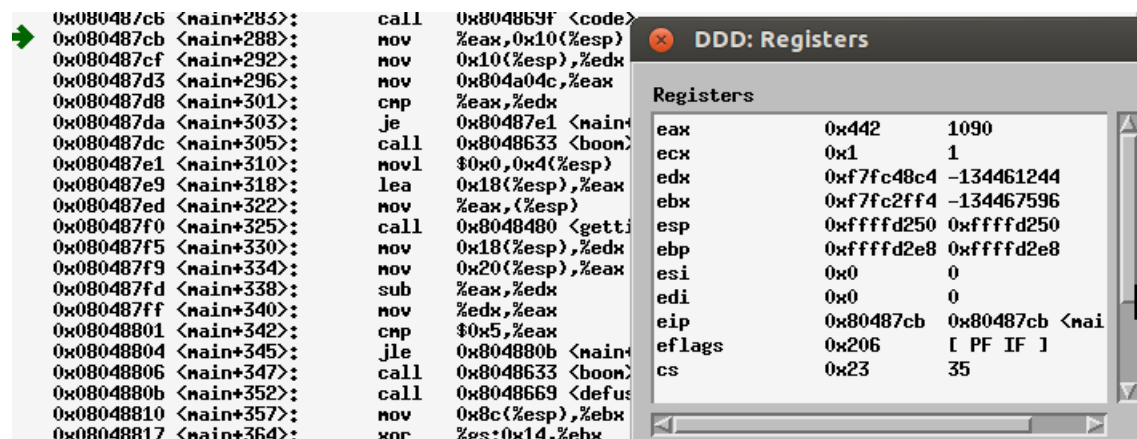


Figura 2.2: Status Registers desde DDD para el código

Al parecer no se realiza ninguna modificación más sobre el código introducido por consola, porque ya se ha llegado a la comparación final de valores antes de retornar a main. Se puede deducir que lo único que se hace para cambiar el valor es la **resta de 21** sobre éste.

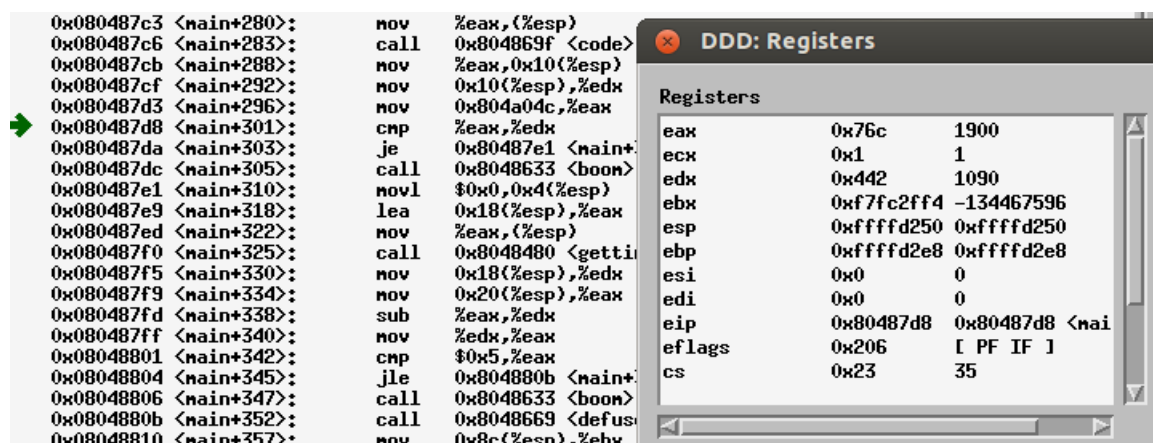


Figura 2.3: Status Registers desde DDD para el código

Dicha comparación puede visualizarse en la Figura 2.3, donde se encuentran ambos valores en la ventana del estado de registros:

El código introducido por consola y modificado posteriormente se encuentra en el registro **%edx** con el valor anteriormente mencionado (**1090**) y el valor original del código con cifrado está en **%eax** con **1900** como contenido.

Por tanto, para terminar con el proceso lo único que hay que hacer es realizar la modificación inversa sobre **1900 (suma de 21)**.

Código: **1921**

### 3. Prueba final

En la Figura 3.1 se presenta la prueba de desactivación de la bomba del compañero Javier Bueno López con contraseña **WAN=>\_M?N** y código **1921**.

```

mario@mariobuntu: ~/Descargas/compartidos
mario@mariobuntu:~/Descargas/compartidos$ ./bomba_bueno_lopez_javier
Introduce la contraseña: WAN=>_M?N
Introduce el código: 1921
*****
*** bomba desactivada ***
*****
mario@mariobuntu:~/Descargas/compartidos$

```

Figura 3.1: Prueba de desactivación