

# Resolución del ejercicio "Bomba"

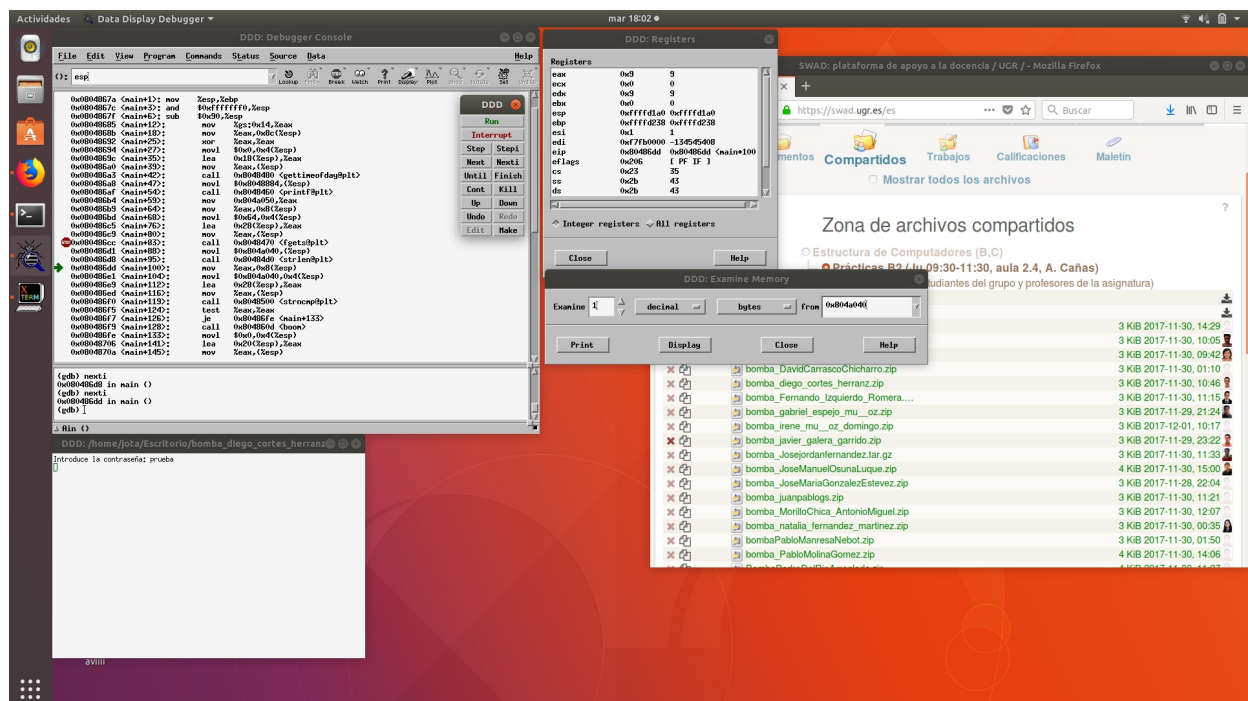
Bomba realizada por: Diego Cortes. Bomba desactivada por: Javier Galera Garrido.

## Primeras Pistas:

1. Sabemos que la contraseña tendrá un máximo de caracteres(10).
2. La contraseña nos la piden por primera vez en la linea <main+83>
3. En <main+100> hay una llamada a strlen por lo que entendemos que justo por ahí, se comprobará la longitud de la cadena de la contraseña.
4. En el ddd podemos ver que en la linea <main+133> se hace un llamado a boom, suponemos que, justo antes, en <main+129> test %eax,%eax tendremos la clave para poder burlar la seguridad

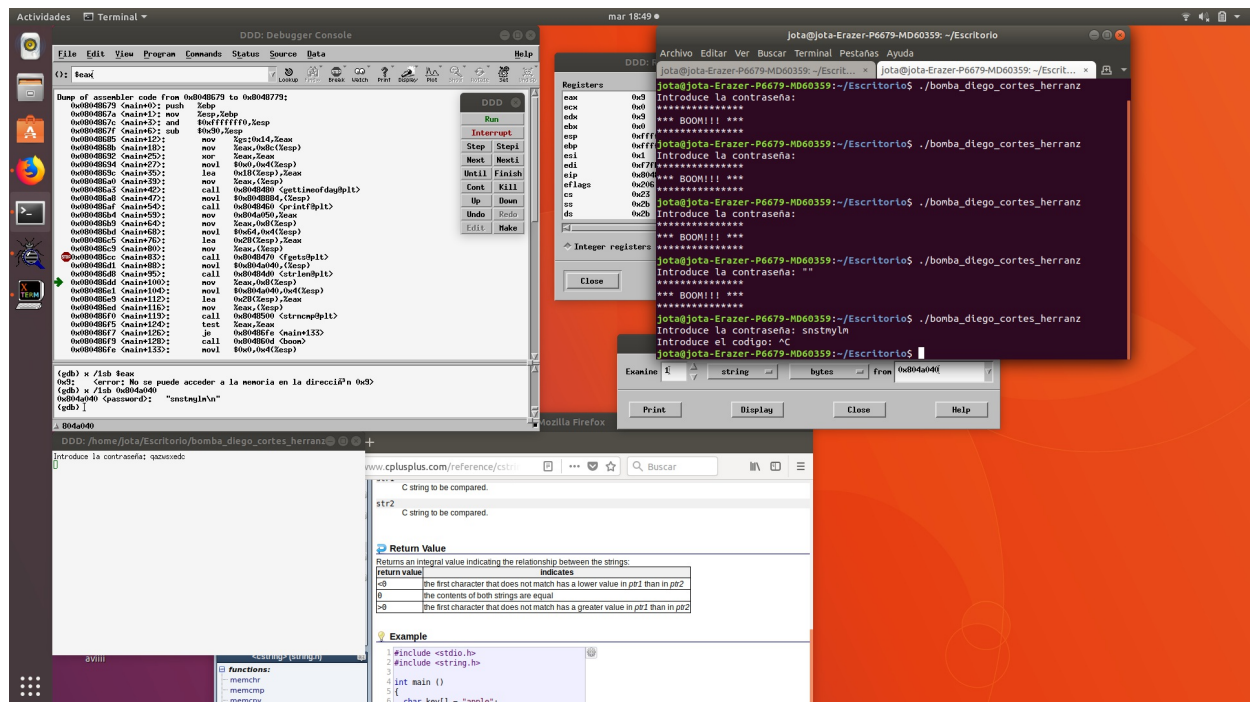
## Desglosando Información:

Vamos a obtener la longitud real de la cadena, hemos probado introduciendo de prueba la palabra: "prueba".

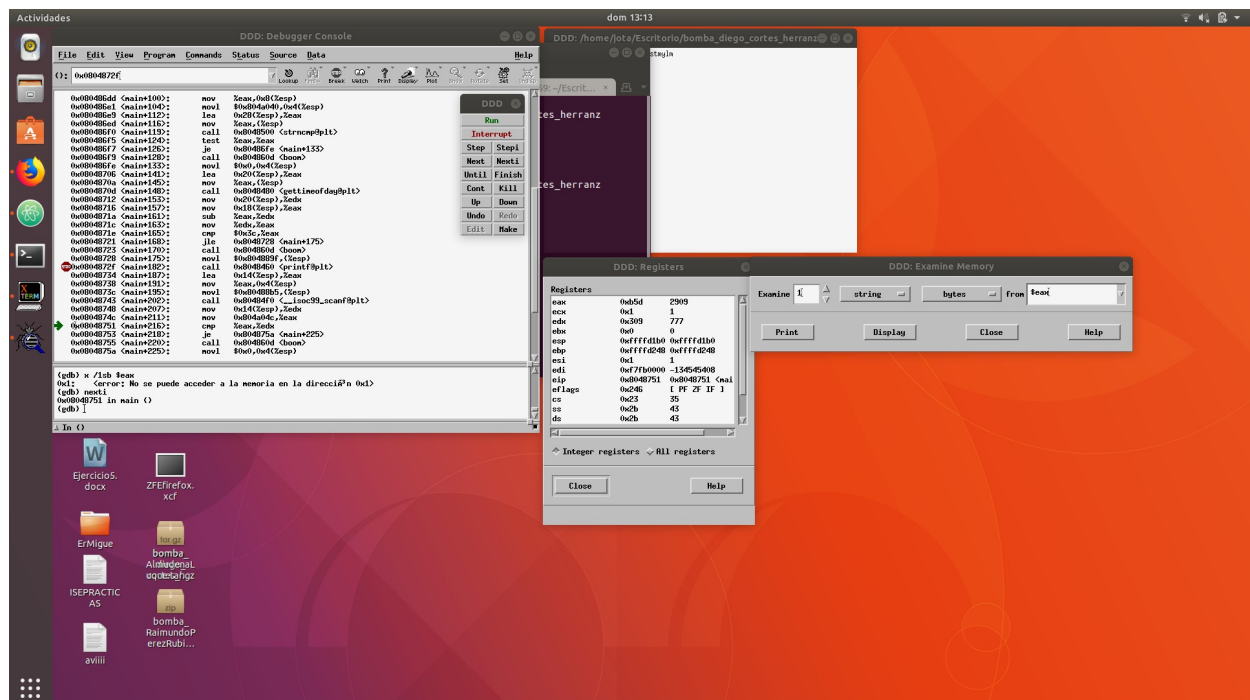


Comprobamos que en \$eax se almacena la contraseña que nosotros hemos introducido y que

en en 0x804a040 encontramos viendo la memoria que la contraseña es "snstmylm". Probamos en el ejecutable y efectivamente es esa.



Si avanzamos en la bomba, podemos comprobar en el registro `$eax` (2909) el código verdadero, el cual se comparará con el que nosotros hemos introducido en el registro `$edx = 7777`



## Solución:

Comprobando llegamos al estado defused de la bomba

Password:snstmylm

Código:2909

