Resolución del ejercicio "Bomba"

Bomba realizada por: Raimundo Perez Rubio. Bomba desactivada por: Javier Galera Garrido.

Primeras Pistas:

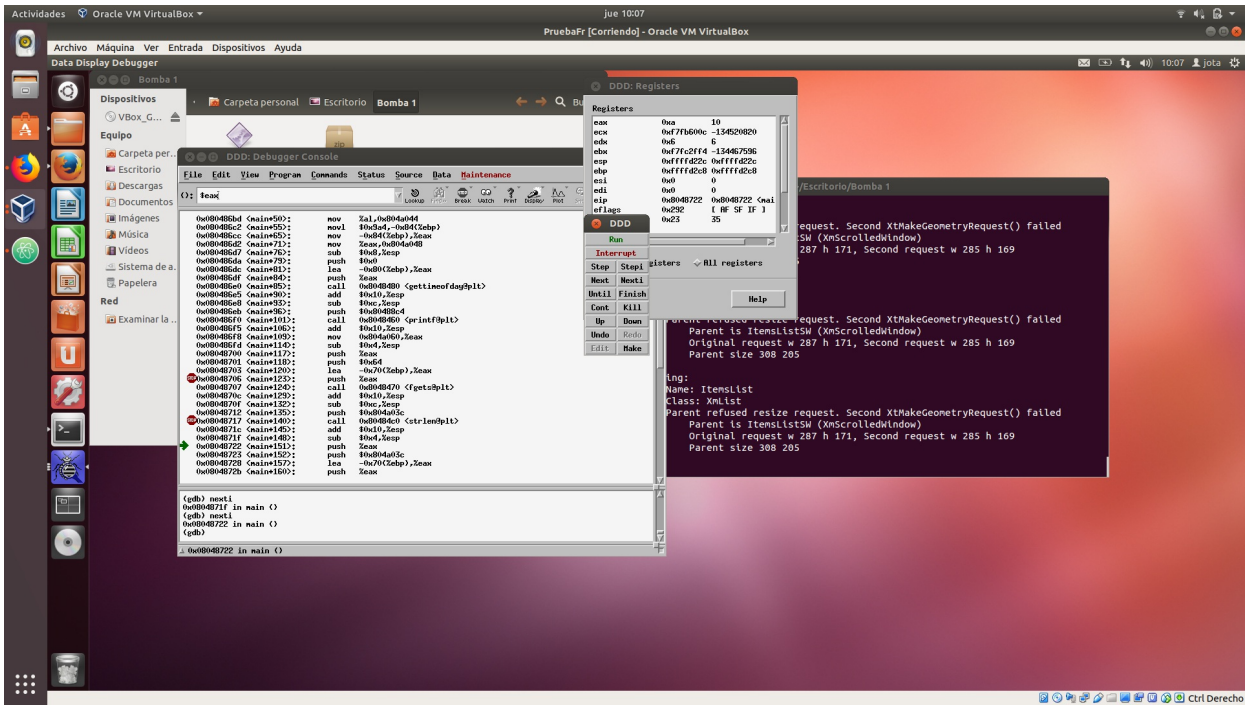
```
1.Sabemos que la contraseña tendrá un máximo de caracteres(10).

2.La contraseña nos la piden por primera vez en la linea <main+124>

3.En el ddd podemos ver que en la linea <main+140> se hace un llamado a strlen,
suponesmos que, justo a partir de ahí uno de los registros contendrá la longitud
de la contraseña.
```

Desglosando Información:

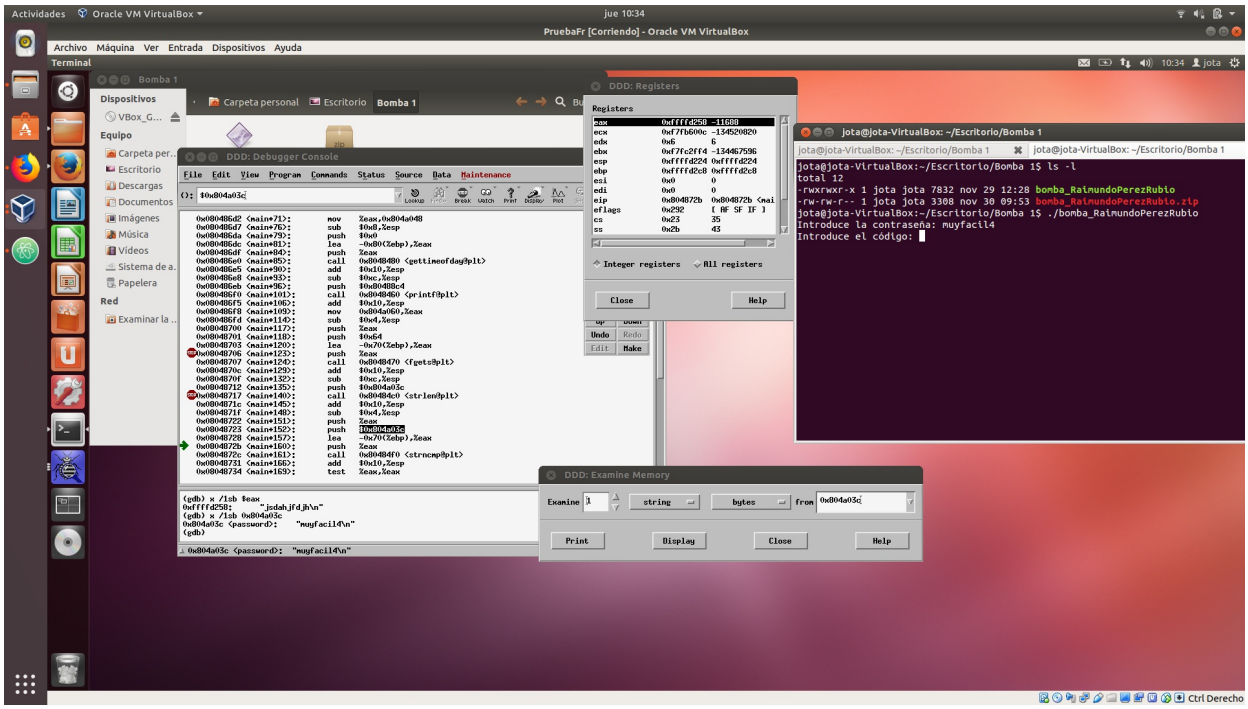
Observamos que una vez pasamos por la linea hemos introducido cualquier cosa y pasamos por la llamada a strlen en y llegamos a la señalada en la imagen en la línea hay un push %eax , el valor de ese registro es:10. Del cual deducimos que la longitud de la cadena es 10.



Strcnmp compara dos string, si el primero es correcto seguirá comparando hasta encontrar uno que no lo sea. Valores de retorno:

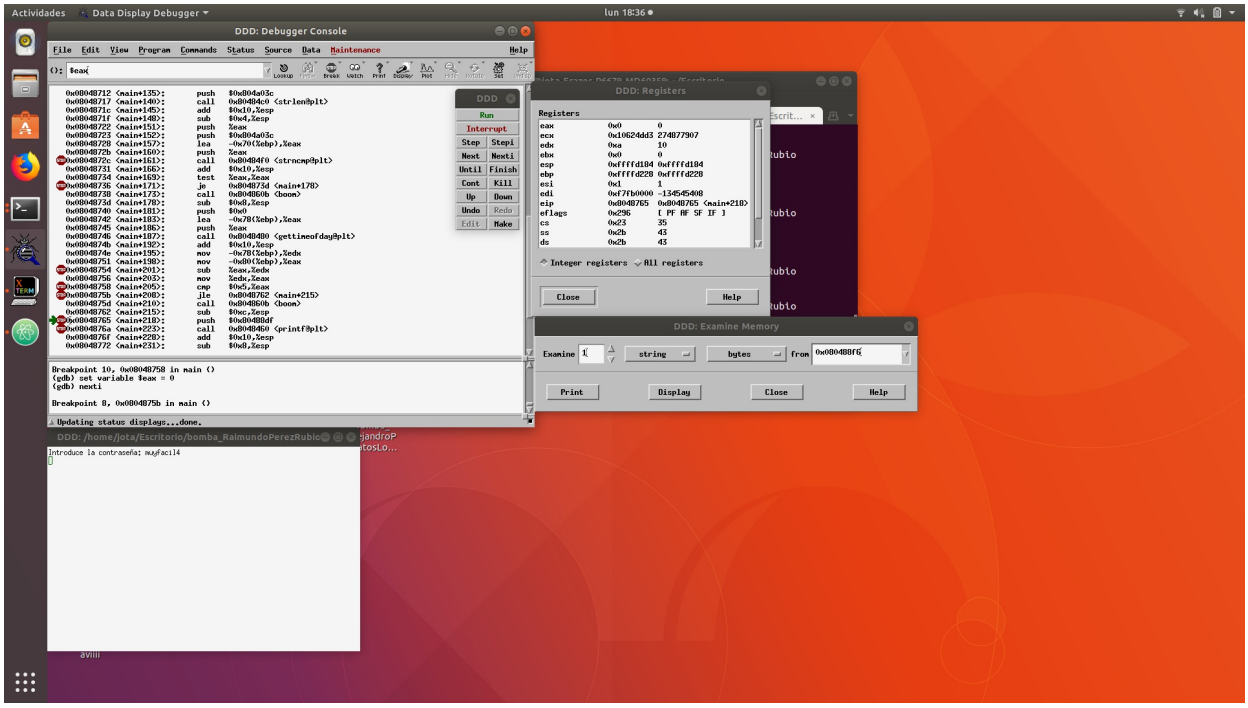
```
<0  el primer carácter que no coincide tiene un valor menor en str1 que en str2.
0   el contenido de los 2 strings es identico.
>0  el primer carácter que no coincide tiene un valor menor en str1 que en str2.
```

Por tanto, deducimos que los push de y podrían ser las contraseñas. Utilizando el examinador de memoria de ddd observamos que en está el string que hemos utilizado para hacer la comprobación. Y que en está la "posible contraseña"(muyfacil4), abrimos una terminal para probar y efectivamente la contraseña no esta cifrada y, por tanto, nos deja acceder a la siguiente fase: acceder al codigo numérico

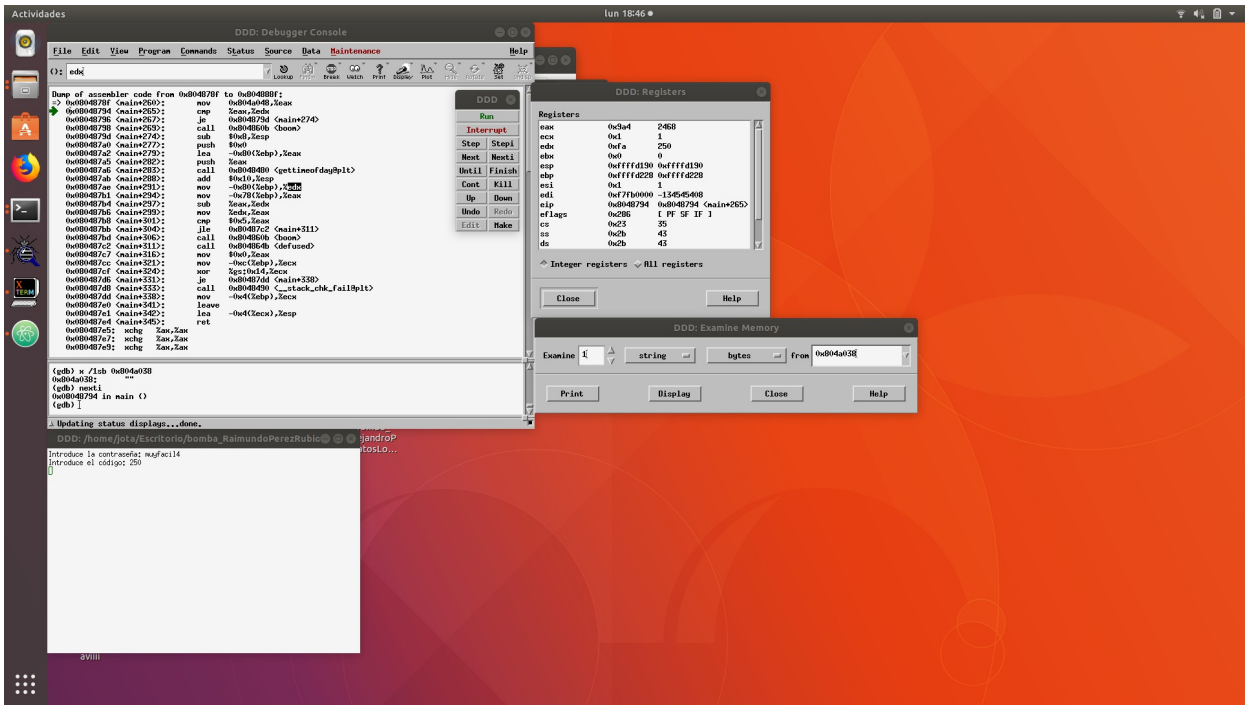


El time de explosión entre la contraseña y el código es bajísimo por tanto tenemos que saltarnos la comprobación de tiempo:

```
<main+205> en el cmp modificamos el valor del registro $eax = 0
De esta manera el programa continuará con normalidad y podremos seguir hasta
incluir el código
```



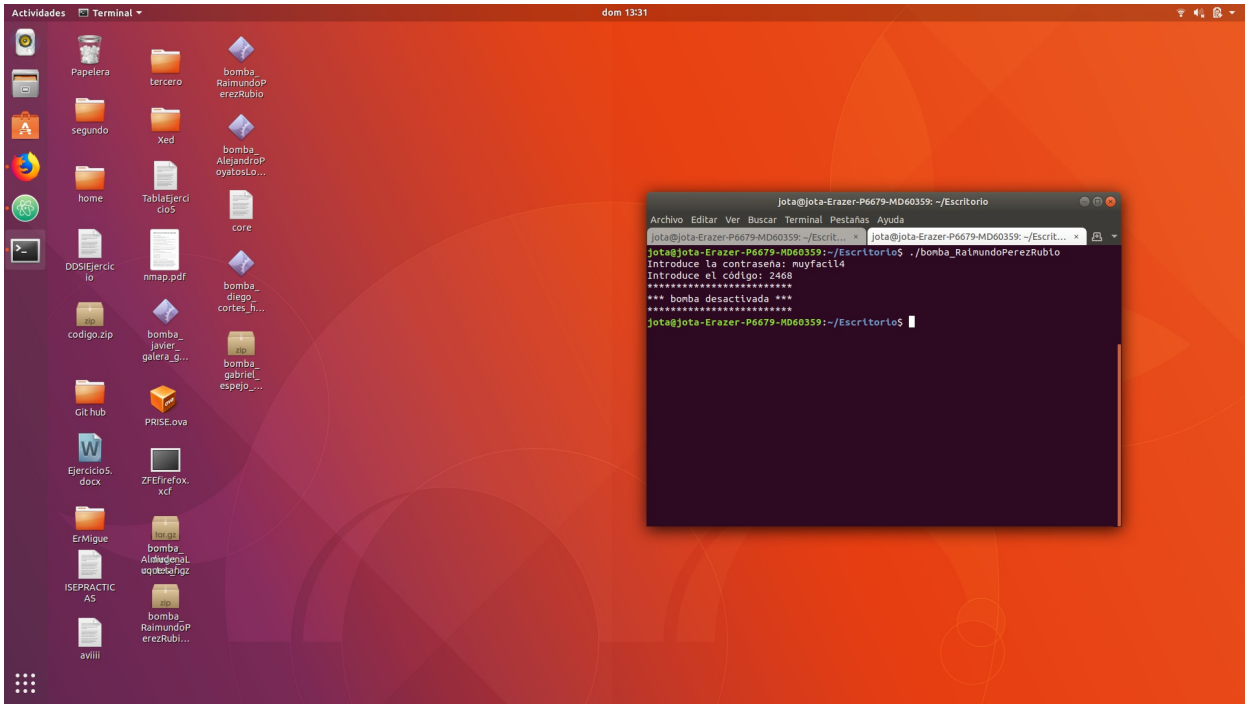
Por último en tenemos una comparación entre los registros $eax y $edx, puesto que en $eax está el código que habiamos insertado de prueba "250", observamos que en $edx está el original "2468"



Solución:

Comprobamos que llegamos al estado desactivado de la bomba:

```
Password:muyfacil4
Codigo:2468
```


Actividades
Terminal
dom 13:31
Papelera
tercero
bomba_RaimundoPerezRubio
segundo
Xed
bomba_AlejandroPoyatosLo...
home
TablaEjercicio5
core
DDSIEjercicio
nmap.pdf
bomba_diego_cortes_h...
codigo.zip
bomba_javier_galera_g...
bomba_gabriel_espejo_...
Git hub
PRISE.ova
Ejercicio5.docx
ZFEfirefox.xcf
ErMigue
ISEPRACTICAS
bomba_RaimundoPerezRubi...
aviiii
jota@jota-Erazer-P6679-MD60359: ~/Escritorio
Archivo Editar Ver Buscar Terminal Pestañas Ayuda
jota@jota-Erazer-P6679-MD60359:~/Escritorio$ ./bomba_RaimundoPerezRubio
Introduce la contraseña: muyfacil4
Introduce el código: 2468
****
*** bomba desactivada ***
****
jota@jota-Erazer-P6679-MD60359:~/Escritorio$