ESTRUCTURA DE COMPUTADORES -
2º GRADO INGENIERÍA INFORMÁTICA
PRÁCTICA 4.- BOMBA DIGITAL – DESENSAMBLADORES

Mario Antonio López Ruiz - 45109755Q

BOMBA DE JULIO ANTONIO FRESNEDA GARCÍA MODIFICADA

RESUMEN
Esta bomba aplicaba una máscara a la contraseña introducida por pantalla, sumandole 5 al valor de cada carácter de forma intermitente. Con el código lo que hacía era sumarle un valor constante (12345) al código introducido por pantalla, a través del cual se tenía que llegar al código original.
Los cambios que voy a hacer van a ser:

-CONTRASEÑA: Voy a cambiar el valor original de la contraseña, y además la operación que se realiza con la contraseña introducida por pantalla lo voy a modificar

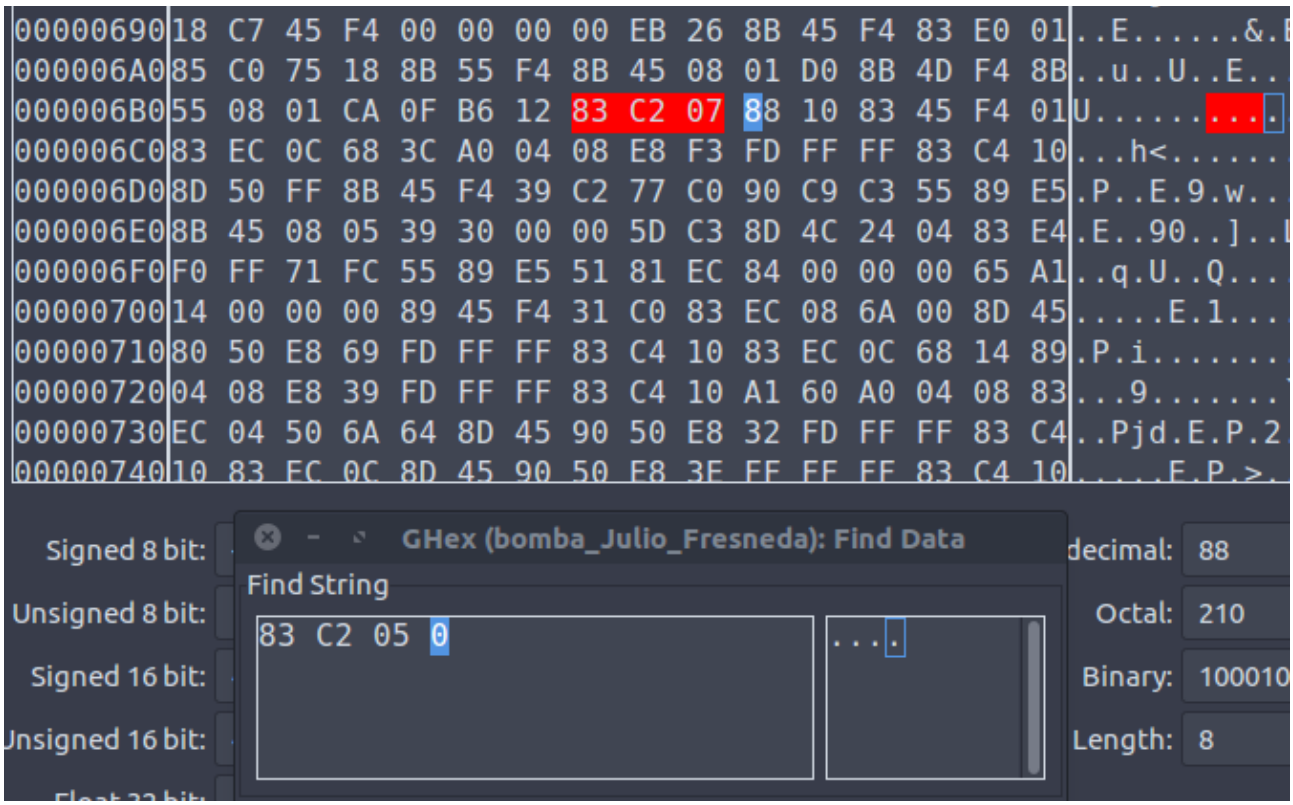
-CÓDIGO: Voy a cambiar el valor original del código y la cantidad que le voy a sumar al introducido por pantalla.

Son modificaciones simples, pero que cambian el resultado por completo.

1.CONTRASEÑA
Voy a buscar la operación donde se sumaba 5 a cada carácter y voy a cambiar ese valor:

```
80486a7:    8b 45 08          mov   0x8(%ebp),%eax
80486aa:    01 d0             add   %edx,%eax
80486ac:    8b 4d f4          mov   -0xc(%ebp),%ecx
80486af:    8b 55 08          mov   0x8(%ebp),%edx
80486b2:    01 ca             add   %ecx,%edx
80486b4:    0f b6 12          movzbl (%edx),%edx
80486b7:    83 c2 05          add   $0x5,%edx
80486ba:    88 10             mov   %dl,(%eax)
80486bc:    83 45 f4 01       addl  $0x1,-0xc(%ebp)
80486c0:    83 ec 0c          sub   $0xc,%esp
80486c3:    68 3c a0 04 08    push  $0x804a03c
80486c8:    e8 f3 fd ff ff    call  80484c0 <strlen@plt>
```

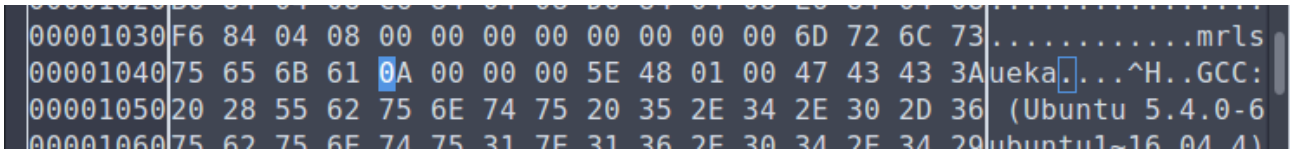
Abro el editor hexadecimal, y cambio 83 c2 05 → 83 c2 07, con lo cual ahora estoy sumando 7 en vez de 5:



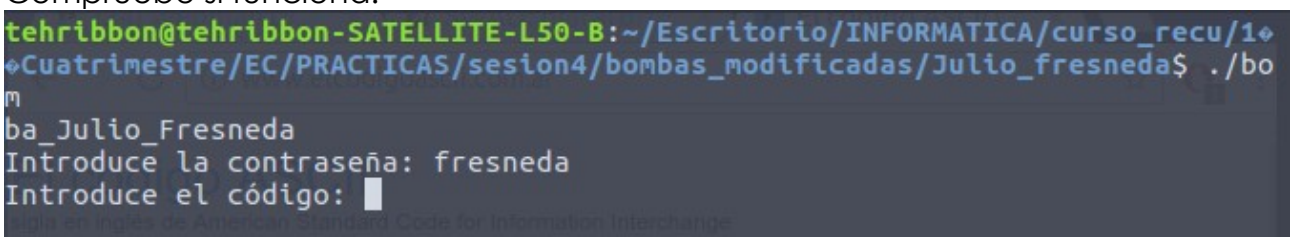
Ahora procedo a cambiar la contraseña original. Quiero que la contraseña que tenga que introducir por pantalla sea "fresneda", por lo tanto en la variable original tengo que introducir:

f → m
r → r
e → l
s → s
n → u
e → e
d → k
a → a

Modifico en el editor hexadecimal la cadena original de la contraseña por: "mrlsueka"



Compruebo si funciona:



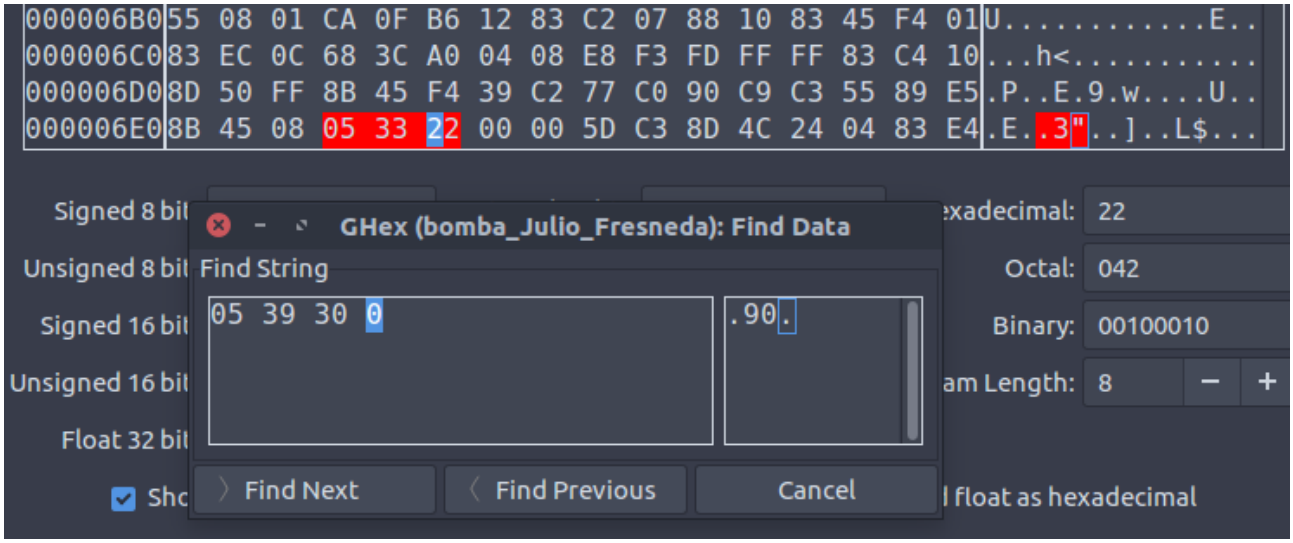
La contraseña está modificada correctamente.

2.CÓDIGO

El proceso va a ser muy similar al de la contraseña. Accedo a la posición en la que se realiza la suma del valor concreto, y cambio ese valor:

```
080486dd <cifrar_passcode>:
 80486dd:       55                      push   %ebp
 80486de:       89 e5                   mov    %esp,%ebp
 80486e0:       8b 45 08                mov    0x8(%ebp),%eax
 80486e3:       05 39 30 00 00          add    $0x3039,%eax
 80486e8:       5d                      pop    %ebp
 80486e9:       c3                      ret
```

Y lo cambio desde el editor:



Por lo tanto ahora el código que tendrá que introducir es 84062-8755 = 75307 para desactivar la bomba. Compruebo:

```
tehribbon@tehribbon-SATELLITE-L50-B:~/Escritorio/INFORMATICA/curso_recu/
◆Cuatrimestre/EC/PRACTICAS/sesion4/bombas_modificadas/Julio_fresneda$ ./
m
ba_Julio_Fresneda
Introduce la contraseña: fresneda
Introduce el código: 75307
************************
*** bomba desactivada ***
************************
tehribbon@tehribbon-SATELLITE-L50-B:~/Escritorio/INFORMATICA/curso_recu/
◆Cuatrimestre/EC/PRACTICAS/sesion4/bombas_modificadas/Julio_fresneda$
```