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

Mario Antonio López Ruiz - 45109755Q

BOMBA DE JUAN EMILIO GARCÍA MARTÍNEZ MODIFICADA

RESUMEN
Esta bomba tenía como contraseña una cadena, la cual invierte durante el programa y después compara con la contraseña introducida por pantalla.
El código simplemente se podía ver accediendo a la variable "passcode".

```
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$
```

Voy a cambiar el valor de esas variables, por las que yo quiera.

1.CONTRASEÑA
Accedo a la posición en la cual se encuentra la contraseña y la cambio:

```
00001030 F6 84 04 08 00 00 00 00 00 00 00 00 61 1E 00 00 ............a...
00001040 0A 4C 49 56 4F 4D 00 00 00 00 47 43 43 3A 20 28 .LIVOM....GCC: (
00001050 55 62 75 6E 74 75 20 35 2E 34 2E 30 2D 36 75 62 Ubuntu 5.4.0-6ub
00001060 75 6E 74 75 31 7E 31 36 2E 30 34 2E 34 29 20 35 untu1~16.04.4) 5
00001070 2E 34 2E 30 20 32 30 31 36 30 36 30 39 00 00 00 .4.0 20160609...
00001080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00001090 00 00 00 00 54 81 04 08 00 00 00 00 03 00 01 00 ....T...........
```

Y lo modifico por: LIVOM → AIPES

```
00001030 F6 84 04 08 00 00 00 00 00 00 00 00 61 1E 00 00 ............a...
00001040 0A 41 49 50 45 53 00 00 00 00 47 43 43 3A 20 28 .AIPES....GCC: (
00001050 55 62 75 6E 74 75 20 35 2E 34 2E 30 2D 36 75 62 Ubuntu 5.4.0-6ub
00001060 75 6E 74 75 31 7E 31 36 2E 30 34 2E 34 29 20 35 untu1~16.04.4) 5
00001070 2E 34 2E 30 20 32 30 31 36 30 36 30 39 00 00 00 .4.0 20160609...
00001080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00001090 00 00 00 00 54 81 04 08 00 00 00 00 03 00 01 00 ....T...........
```

Por lo tanto, ahora la contraseña que se tiene que introducir es SEPIA.
Compruebo:

```
a

Introduce la contraseña: SEPIA
Introduce el código:
```

2.CÓDIGO

Voy a cambiarle el valor a la variable passcode (vale 7777):

```
80487c0:      83 c4 10                add    $0x10,%esp
80487c3:      8b 95 7c ff ff ff       mov    -0x84(%ebp),%edx
80487c9:      a1 3c a0 04 08          mov    0x804a03c,%eax
80487ce:      39 c2                   cmp    %eax,%edx
80487d0:      74 05                   je     80487d7 <main+0xd2>
```

Dentro de 0x804a03c se encuentra el valor 7777:

```
(gdb) print *0x804a03c
$3 = 7777
(gdb)
```

Voy a cambiar esa instrucción para pasar a %eax directamente un valor, mediante el editor en hexadecimal.
Cambio el tipo de salto JE → JNE, por lo que se desactivará la bomba siempre y cuando no se introduzca un valor igual a 7777

```
007C0 83 C4 10 8B 95 7C FF FF FF A1 3C A0 04 08
007D0 75 05 E8 34 FE FF FF 83 EC 08 6A 00 8D 45
```

Compruebo:

```
Introduce la contraseña: sepia
Introduce el código: nos
************************
*** bomba desactivada ***
************************
tehribbon@tehribbon-SATELLITE-L50-B:~/Escritorio/INFORMATICA/curso_recu/1
◆Cuatrimestre/EC/PRACTICAS/sesion4/bombas_modificadas/Juane_garcia$ ./bom
a
Introduce la contraseña: sepia
Introduce el código: 7777
***************
*** BOOM!!! ***
***************
tehribbon@tehribbon-SATELLITE-L50-B:~/Escritorio/INFORMATICA/curso_recu/1
◆Cuatrimestre/EC/PRACTICAS/sesion4/bombas_modificadas/Juane_garcia$
```