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	movCOI	0x8(%ebp),%eax
80486aa:	01 d0	voy add umo	%edx,%eax
80486ac:	8b 4d f4	Son MOV diffic	-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	ese movor:	%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></strlen@plt>

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

```
000006A0<mark>85    C0    75    18    8B    55    F4    8B    45    08    01    D0    8B    4D    F4    8B    ..u..U..E..</mark>
000006B0<mark>55 08 01 CA 0F B6 12 <mark>83 C2 07 8</mark>8 10 83 45 F4 01<mark>U.....</mark></mark>
000006C0<mark>8</mark>3 EC 0C 68 3C A0 04 08 E8 F3 FD FF FF 83 C4 10...h<...
000006D0<mark>8</mark>D 50 FF 8B 45 F4 39 C2 77 C0 90 C9 C3 55 89 E5<mark>.P..E.9.w..</mark>
000006E0<mark>8B 45 08 05 39 30 00 00 5D C3 8D 4C 24 04 83 E4</mark>.E..90..]..
000006F0F0 FF 71 FC 55 89 E5 51 81 EC 84 00 00 00 65 A1..q.U..Q...
00000700<mark>14 00 00 00 89 45 F4 31 C0 83 EC 08 6A 00 8D 45</mark>
00000720<mark>0</mark>4 08 E8 39 FD FF FF 83 C4 10 A1 60 A0 04 08 83<mark>...9...</mark>
|00000730|EC 04 50 6A 64 8D 45 90 50 E8 32 FD FF FF 83 C4|..Pid.E.P.2
|00000740|10 83 EC 0C 8D 45 90 50 E8 3E FF FF FF 83 C4 10|
              🔞 - 💌 GHex (bomba_Julio_Fresneda): Find Data
  Signed 8 bit:
                                                               decimal: 88
              Find String
Unsigned 8 bit:
                                                                 Octal: 210
              83 C2 05 0
 Signed 16 bit:
                                                                Binary: 100010
Jnsigned 16 bit:
                                                               Length: 8
```

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:

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

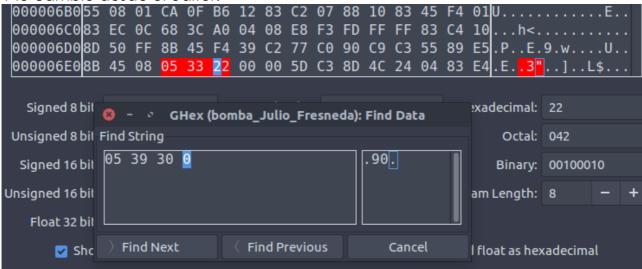
La contraseña está modificada correctamente.

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>:
                55
 80486dd:
                                         push
                                                %ebp
 80486de:
                89 e5
                                                %esp,%ebp
                                         mov
                8b 45 08
                                                0x8(%ebp),%eax
 80486e0:
                                         mov
                05 39 30 00 00
 80486e3:
                                         add
                                                $0x3039,%eax
 80486e8:
                5d
                                                %ebp
                                         DOD
80486e9:
                с3
                                         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/
oCuatrimestre/EC/PRACTICAS/sesion4/bombas_modificadas/Julio_fresneda$ ./
m
ba_Julio_Fresneda
Introduce la contraseña: fresneda
Introduce el código: 75307
********************
*** bomba desactivada ***
**** bomba desactivada ***
tehribbon@tehribbon-SATELLITE-L50-B:~/Escritorio/INFORMATICA/curso_recu/
oCuatrimestre/EC/PRACTICAS/sesion4/bombas_modificadas/Julio_fresneda$
```