Estructura de computadores
Práctica 4
Bomba propia desactivada

Alumno: Antonio David López Machado **Grupo:** C-2

1.Desactivación de bomba digital propia

El primer punto ha sido buscar la primera llamada a la función fgets y viendo que no se ha realizado nada inusual antes de dicha llamada.

Tras esta llamada he detectado un loop entre las líneas main+97 y main+142. Deduzco que en dicho loop se realiza la manipulación(encriptación) de la contraseña introducida en el get. Analizando este bucle podemos ver que la contraseña introducida por teclado esta en la dirección de la pila 0x28. En la dirección de la pila 0x14($esp) tenemos el contador de dicho loop y podemos ver en la línea main+137 que el contador debe llegar a 10 (<=). También sabemos que el contador empieza en 0.

Para averiguar el proceso que realiza he ido realizando volcados de memoria del registro $ecx que mantiene nuestra contraseña.
Introduciendo la contraseña -> contrasena , he podido deducir el funcionamiento del bucle con los valores numéricos de cada elemento.Lo explico a continuación.

C	O	N	T	R	A	S	E	N	A
99	111	110	116	114	97	115	101	110	97

Y la encriptación que se ha realizado la podemos encontrar antes de la llamada a la función strcmp como podemos observar en la figura 01.

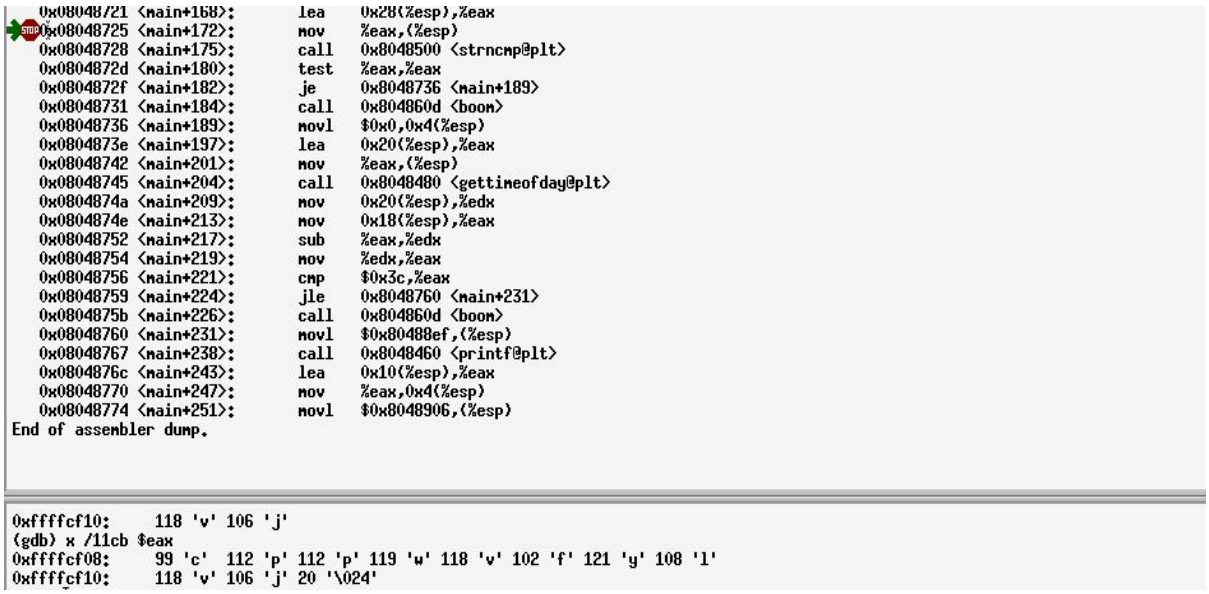

Figura 01. Contraseña introducida cifrada.

Como podemos ver en la figura 01 le suma el contador del bucle(0,1,2,3…) a cada elemento dando otro char y encriptando así la contraseña.

Tras analizar la forma de encriptación buscamos la llamada a la instrucción strcmp para conocer qué contraseña es la que tiene la bomba. Nos fijamos en las instrucciones realizadas justo antes de strcmp y podemos deducir que en la dirección 0x804a040 podemos encontrar la contraseña de nuestra bomba lógica. El valor de esta contraseña podemos observarlo en la figura 02.

.

```
(gdb) x /12cb 0x804a040
0x804a040 <password>:   115 's' 112 'p' 123 '{' 120 'x' 114 'r' 102 'f' 104 'h' 118 'v'
0x804a048 <password+8>: 117 'u' 107 'k' 107 'k' 10 '\n'
(gdb)
```

Figura 02. Contraseña de la bomba cifrada

Si le aplicamos la encriptación de forma inversa podremos deducir la contraseña que deberemos introducir la cual será:

S	O	Y	U	N	A	B	O	M	B	A
115	111	121	117	110	97	98	111	109	98	97

Una vez que hemos descifrado por completo la contraseña pasamos a descifrar el código. Para ello lo primero que tenemos que hacer es buscar la llamada a la función fscan . Al valor introducido se le resta $0x6e(110 en decimal), y este es la forma de encriptación del código.

```
(gdb) x /1dw 0x804a050
0x804a050 <passcode>:   80877
(gdb)
```

Figura 03. Código cifrado

Al realizar la comparación de ambos elementos puedo detectar el código de la bomba digital la cual está en la dirección 0x804a050 y es -> 80877(como podemos observar en la figura 0.3) y si la desencriptados(sumarle 110) nos da como resultado 80987 el cual es el passcode que debo introducir para desactivar la bomba.

Como podemos ver en la figura 04 la desactivación se ha realizado con éxito.

```
antoniolm@antoniolm-Lenovo-Z50-70:~/Grado_Informatica-EC/Practica04$ ./bomba_Ant
onioDavidLopezMachado
Introduce la contraseña: soyunabomba
Introduce el código: 80987
*************************
*** bomba desactivada ***
*************************
antoniolm@antoniolm-Lenovo-Z50-70:~/Grado_Informatica-EC/Practica04$
```

Figura 04. Bomba desactivada