Adrián de la Torre Rodríguez

RESOLUCIÓN DE LAS BOMBAS

BOMBA: bombaArthurRN

Contraseña: grlions18

Código: 216981

Para averiguar la contraseña abrimos el ddd, si miramos el programa nos damos cuenta de que se hacen comparaciones con 0x3c por encima de ebp en varias partes del programa. Al principio del programa vemos que en esa sección de la pila se guarda una dirección de memoria:

```
0x08048746 <+51>:   movl   $0x8048bb9,0x3c(%esp)
```

Si hacemos un volcado de memoria de esa dirección:

Data > Memory

1 string bytes from: 0x8048bb9

Obtenemos:

```
0x8048bb9:      "grlions18"
```

Esa es la contraseña.

Para averiguar el código hay que irse a la instrucción del programa:

```
0x0804896e <+603>:  cmp    %eax,%edx
```

Y establecemos allí un breakpoint. Una vez estemos en esa dirección pulsamos:

Status > Registers

Y vemos que en eax esta el numero en decimal: `216981`

Ese es nuestro código.

Para cambiar el código y la contraseña abro el ghex y busco “grlions18”, en la parte resaltada en rojo escribo encima la nueva contraseña, que en este caso será: “TePasaste”. Por otro lado busco el código en hexadecimal “34F95” que pasado a little endian es: “95 4F 03”. Una vez encontrado escribo encima el código nuevo: “123456” que en little endian es: “40 E2 01”.

MI BOMBA: bombaAdriandelaTorreRodriguez26.zip

Contraseña: sergiosam

Código: 7899

Como la contraseña esta almacenada en un array cuyos elementos con índice primo son caracteres de la contraseña, accedo a ese array volcando la memoria:

Data > Memory
1 string bytes from: 0x0804a040

Obtengo:

“`atseursgsowiyoghzsqalkkmqwfrh\n`”

Cogiendo los caracteres que están en una posición con índice primo sale la contraseña:

“`sergiosam`”

Para obtener el código hay que poner un breakpoint en la instrucción:

```
0x0804896e <+603>:  cmp    %eax,%edx
```

Aquí se comparan el código válido y el que se ha introducido. Una vez llegamos a este punto miramos los registros y vemos que eax vale: “7899”.