EXPLICACIÓN BOMBA 18

ESTRUCTURA DE LOS COMPUTADORES
Prácticas 2ºB B1

David Gómez Hernández

La bomba que me fue asignada fue la bomba número 18.
Su contraseña original es: hsGYbmQa.
Su pin es: 2823.

Tras modificarla sus nuevos códigos son:

- asGYbmQa para la contraseña
- 0000 para el pin

Los pasos para sacar la contraseña fue usar el GDB e ir paso a paso hasta que llegaras a la octava instrucción donde el programa movía la palabra <password> a %rsi y %rdi con lo cual de ahí obtenidas ambas partes.

La contraseña podría parecer algo más complicado pero simplemente tras averiguar la contraseña unas instrucciones más abajo viene la palabra <passcode> donde según en el GDB estaba localizada en %eax y si tienes aplicados los comandos “layout asm” y “layout regs” podías observar que en efecto en %eax estaba la serie de números 2823.

A la hora de modificar ambos apartados, aunque es posible hacerlos con el GDB, utilizando la herramienta GHEX es muchísimo más sencillo.

Antes de nada realizamos una copia de la bomba original para no alterar sus valores.

Para modificar la contraseña era tan fácil como utilizar la herramienta buscador que proporciona el GHEX y buscar la serie de caracteres “hsGYbmQa”. Tras esto decidí solamente cambiar un carácter, la primera h pasó a ser una a.

Para modificar la contraseña tiene truco ya que si intentabas buscar la serie de números 2823 veías que no aparecía en el buscador. La solución a esto es pasar susodicha serie de decimal a hexadecimal y posteriormente buscarlo en el buscador del GHEX.

La clave está en que aunque tu lo busques sigue sin aparecer, debido a que el GHEX trabaja en little-endian, así que tienes que poner la sucesión de números en hexadecimal al revés. De esta forma ya encontramos la contraseña y podemos modificarla. En mi caso cambié todos los valores y los puse a 0.

De esta forma ya hemos modificado correctamente la bomba con nuevos valores.