Práctica 4 EC – Segunda Parte.

Vicente Martínez Rodríguez

Juan José Montero Parodi

Bombas Desactivadas.

bomba_LuisGilGuijarro:

La contraseña es: resaca

El código es: 7237

La contraseña aparece en 0x08048681 <main+57>: movzbl /%eax),%eax

Con Data Memory se hace un print de $eax para que muestre el dato en formato string.

A continuación hace un bucle modificando las letras , pero compruebo de nuevo $eax y la contraseña aparece “resaca/n”

Después de este bucle hay otro del mismo estilo que cambia las letras pero no cambia nada en la contraseña que se debe introducir.

Se escribe en la consola del gdb set $eax=0 para saltar la comprobación de si el código introducido es correcto, igualmente para saltar la comprobación de que no ha pasado el tiempo.

En la línea de <main+479> se pide introducir la clave, se introduce la clave 0000 para así poder ver como se modifica el código introducido.

A continuación aparece un bucle que parece que suma a nuestro numero el 202 en 101 iteraciones, se pone un break detrás de la comprobación <main+545> y se ejecuta cont para que llegue hasta después del bucle, en la línea <main+557> se hace la comprobación de %eax y %edx por lo que realizo un print de estos dos registros, mostrándose en %edx → 0xCA=202 y en %eax → 0x1d0f= 7439, por lo que el código ha introducir es 7439-202 = 7237.

bomba_JuanEstebanMorenoLopez:

La contraseña es: abracadabra

La clave es: 7777

En la línea <main+27> se realiza una llamada a la función recontrola, pero esta función se hace para despistar ya que aún no se ha introducido el código y en todo caso modifica la clave propia.

En la línea <main+93> se introduce $0x804a040 a (%esp), al imprimir este valor con Data Memory se obtiene la contraseña verdadera que será comprobada, “abracadabra\n”.

Se saltan las comprobaciones de la clave y el tiempo ejecutando en set la instrucción set $eax=0.

Desde las líneas <main+207> hasta <main+221> se puede observar como se llama a scanf para introducir el código, se mueve el código a %edx, se mueve el valor de 0x804a068 a %eax y se comparan %edx y %eax, por lo tanto el código se puede mostrar imprimiendo en formato decimal, words, la dirección 0x804a068 que contiene el código 7777.