Práctica 4: Explicación para desactivar la bomba de Jose Manuel Enríquez Fernández.

En el achivo bomba.c se encuentra la bomba que yo he desarrollado. En la cual he encriptado el passcode. Para encriptar el passcode lo que he hecho ha sido calcular el numero que sale de la resta entre la letra seleccionada y la “a” en ASCII. Con este valor, lo sumamos a la variable passcode y obtenemos el resultado.

Desactivar la bomba:

Los pasos que he seguido para desactivar son los que voy a describir a continuación. En primer lugar hemos compilado con la orden que se encuentra en la primera línea del documento bomba.c. Tras esto, hemos abierto el gdb en modo interfaz de usuario y establecido el layout a asm como se indica en el guión. He puesto un breakpoint en la función main y he empezado a bajar viendo donde explotaba la bomba. Esto lo he hecho para ir apuntando breakpoints en cada punto crítico y poder estudiarlos más detenidamente a posteriori. En el primer filtro de los 3 que hay, el de la contraseña, lo que he hecho ha sido observar que justo hay una instrucción “test eax,eax” y después un salto a la función boom. Para evitar este salto solo he tenido que variar el contenido de eax a 0. En el segundo filtro, nos encontramos con la instrucción “cmp”, en mi caso está comprobando un registro y el valor que le he introducido cuando me ha pedido el pin (calculado con la calculadora para asegurarme de que es así). Al ser la instrucción cmp seguida de un salto je tan solo debo hacer que coincidan tanto el registro que está comparando como el valor que le he dado antes. Para esto cambio el valor del registro que se está comparando, en mi caso rax, para que tenga el mismo valor que el valor inmediato introducido antes. Con esto pasaríamos el segundo filtro. Por último, el tercer filtro se encarga de comprobar que el tiempo en el que estás desactivando la bomba es menor del que se pide. En mi caso, he variado el tiempo a 60 segundos. En este tercer filtro nos encontramos con otra instrucción “cmp” que está comparando el registro donde se encuentra el tiempo que ha capturado el programa que llevamos nosotros y un valor inmediato que es el que hemos indicados nosotros como maximo. Tenemos que coger una calculadora y pasar a decimal el valor inmediato para ver cuanto tiempo tenemos de maximo y mirar el registro donde está el tiempo que hemos gastado. Como tenemos cmp seguido de una instrunccion de salto jle tenemos que hacer que el registro (rax en mi caso) tenga un valor menor que el inmediato. Si hacemos esto, habremos conseguido desconectar la bomba.