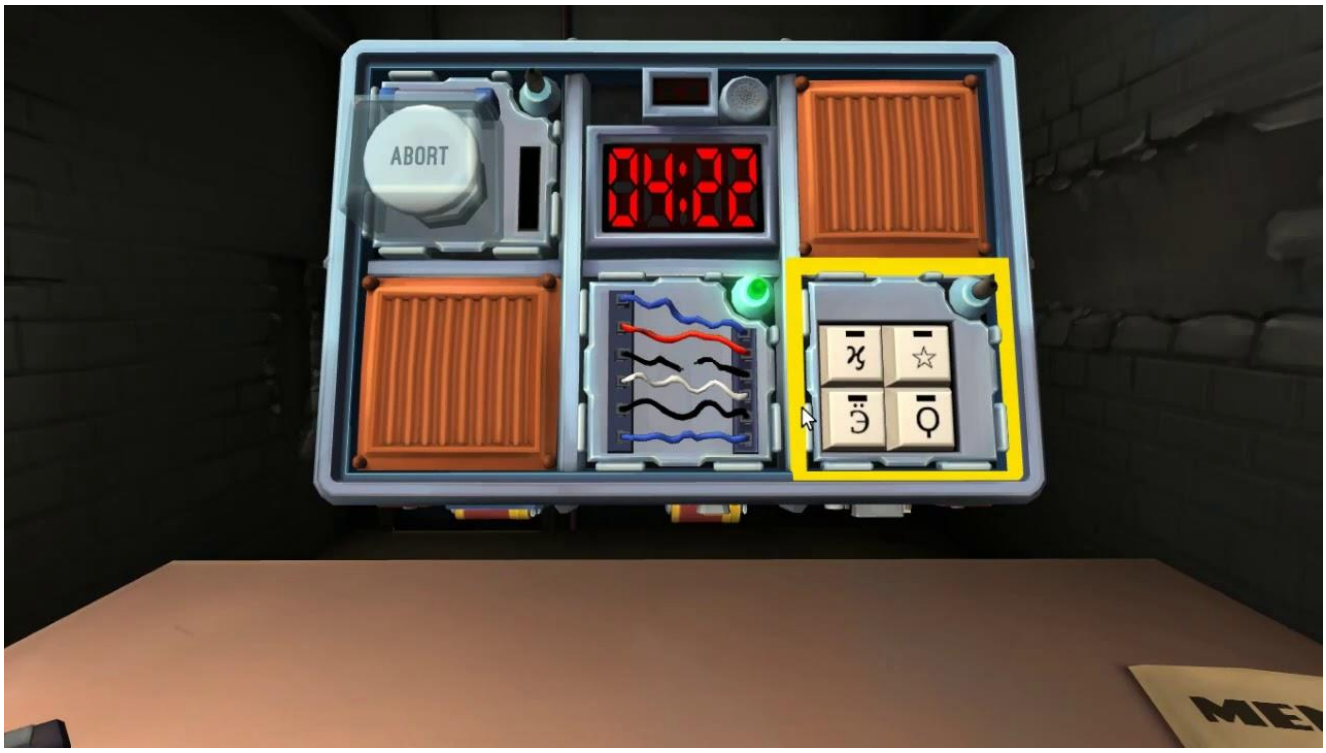
TRABAJO FUNDAMENTOS DE COMPUTADORES Y REDES: FASE II



Hugo Carbajales Quintana

Adrián Gutiérrez García

OBJETIVOS DEL TRABAJO

El objetivo que se ha buscado en este trabajo es desactivar 4 bombas de un archivo .exe descifrando su funcionamiento mediante la observación de la memoria y la pila en lenguaje ensamblador.

Además, se ha modificado el .exe para que las bombas nunca exploten.

A continuación, explicaremos como hemos llevado a cabo esta tarea.

STAGE 1

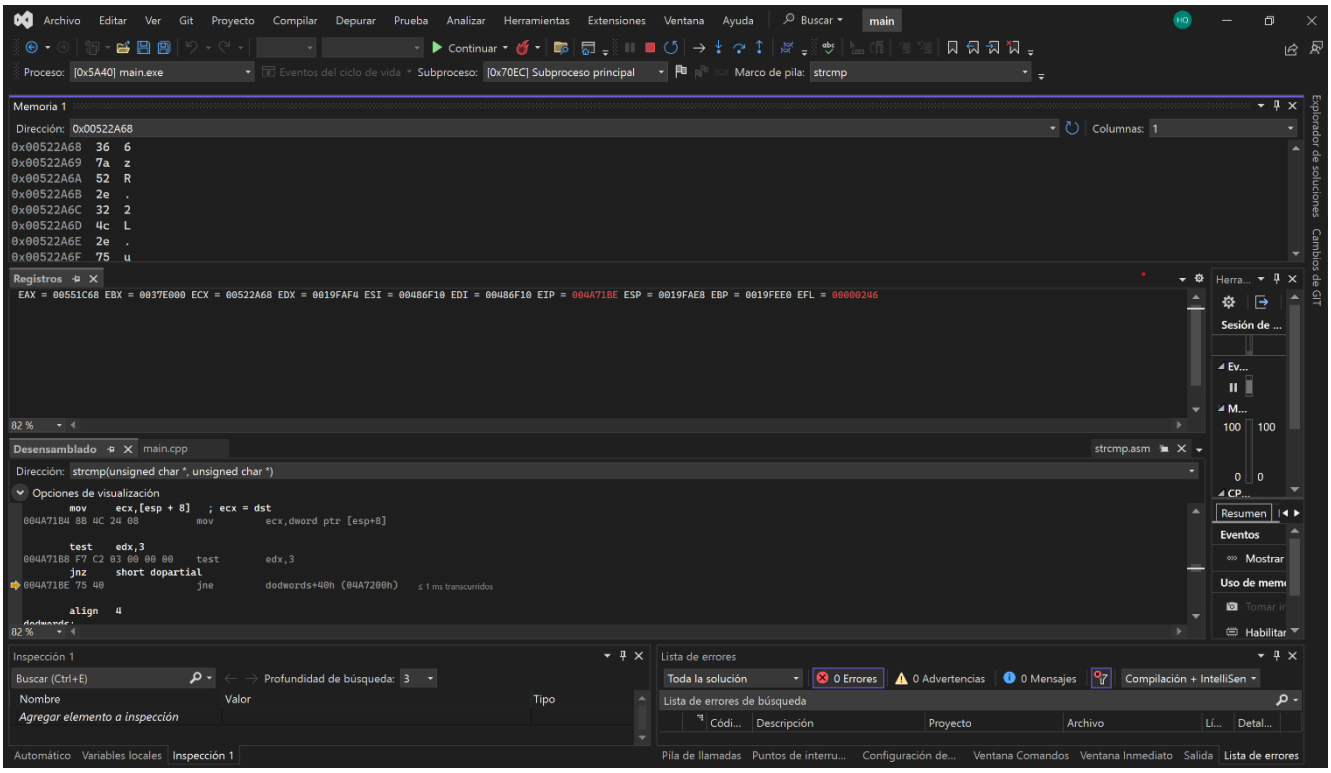
El programa se ejecuta y comienza pidiéndote la contraseña para desactivar la primera bomba.

Para averiguar la contraseña, nos hemos metido en el desensamblado de la función.

Lo primero interesante que vemos es que hace un call a una función que es la encargada de pedirnos la contraseña mediante la terminal.

Siguiendo por el desensamblado, vimos que hacia un push ecx donde entrando en la memoria vimos que se almacenaba nuestra contraseña (la introducida en la terminal) y que después se llamaba a una función llamada strcmp, que supusimos que comparaba 2 strings.

Tras entrar en ella, vimos que al registro ecx se movía algo y se comparaba con nuestra contraseña, donde logramos localizar cual era la contraseña que comparaba y por tanto, la correcta.



Después si la contraseña es correcta, se llama a la función defuse, si es falsa, a la función explode.

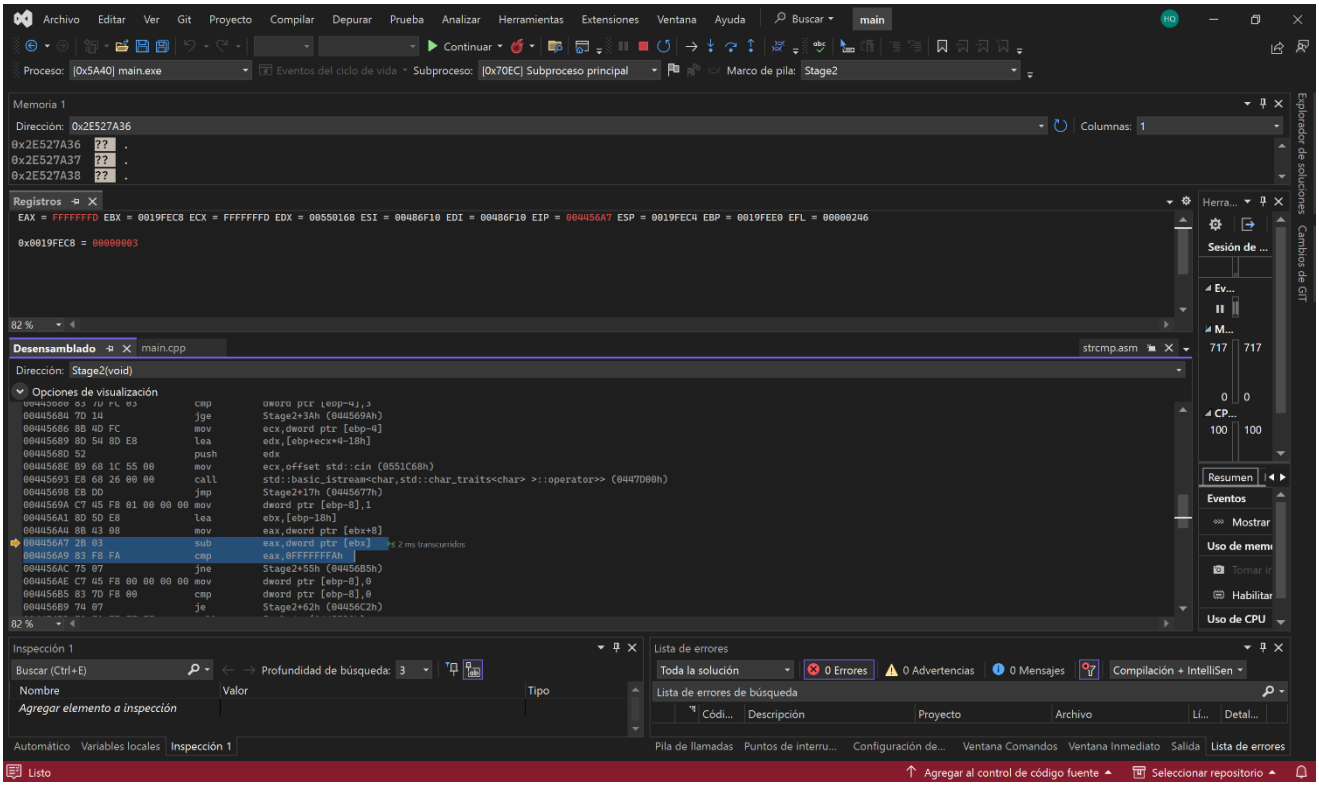
La contraseña que hace que pase a la función defuse es: **6zR.2L.u**

STAGE 2

Comenzamos metiéndonos dentro de la función en el desensamblado.

En esta función, nos piden 3 entradas para introducir en el símbolo del sistema, y vemos como esos valores se van guardando en el registro ecx.

Seguimos navegando y vemos, dos operaciones clave, que son las que en la fotografía están subrayadas en azul.



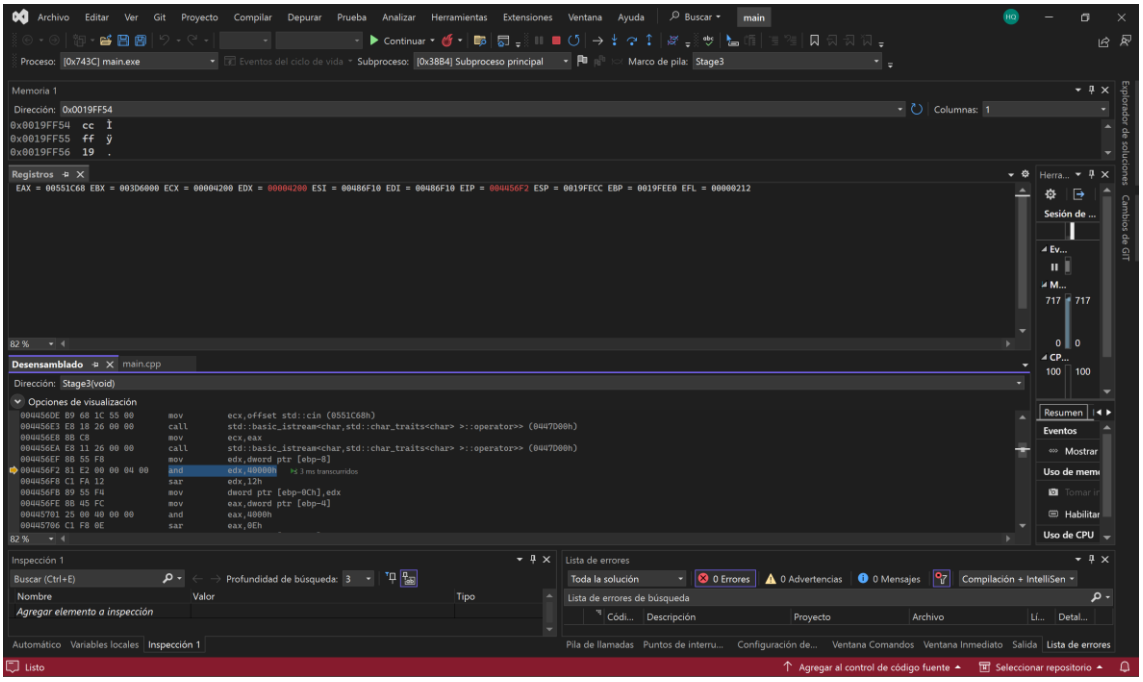
En estas instrucciones, en concreto en la sub, vemos que se resta el 3 parametro introducido, que esta guardado en EAX menos el primer parámetro introducido que esta en EBX.

La contraseña se encuentra claramente en el cmp donde el numero a la derecha del eax es el numero -6 en hexadecimal en complemento a 2 (FFFFFFFAh)

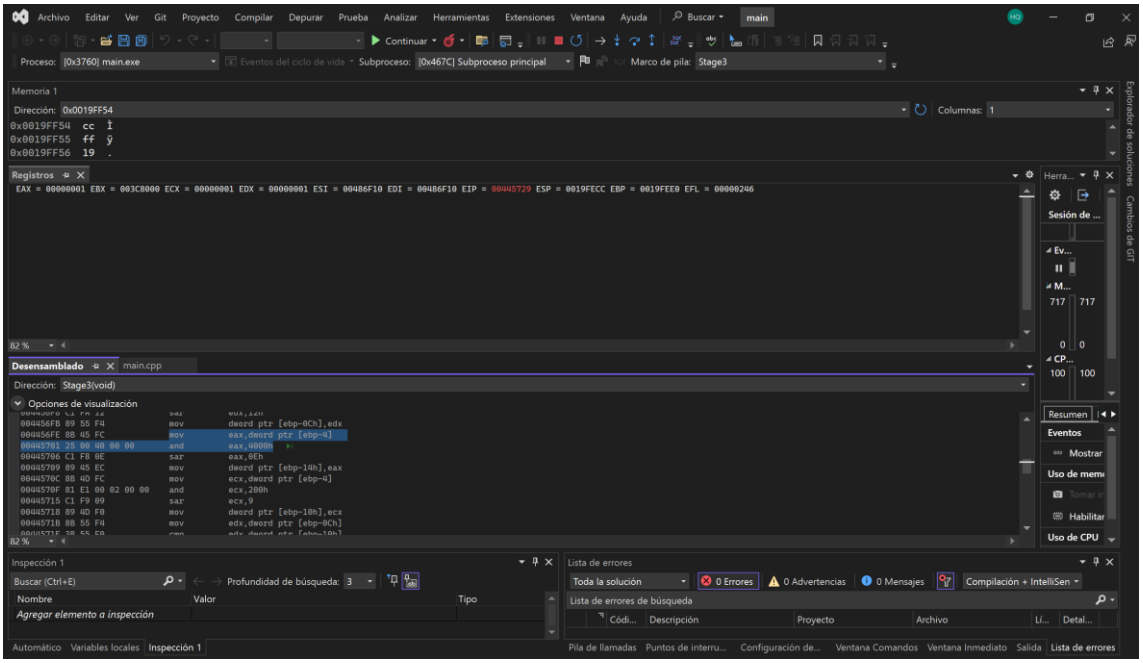
Podemos afirmar que el modo de desactivar la bomba es que la resta entre el tercer parámetro y el primero sea .6.

STAGE 3

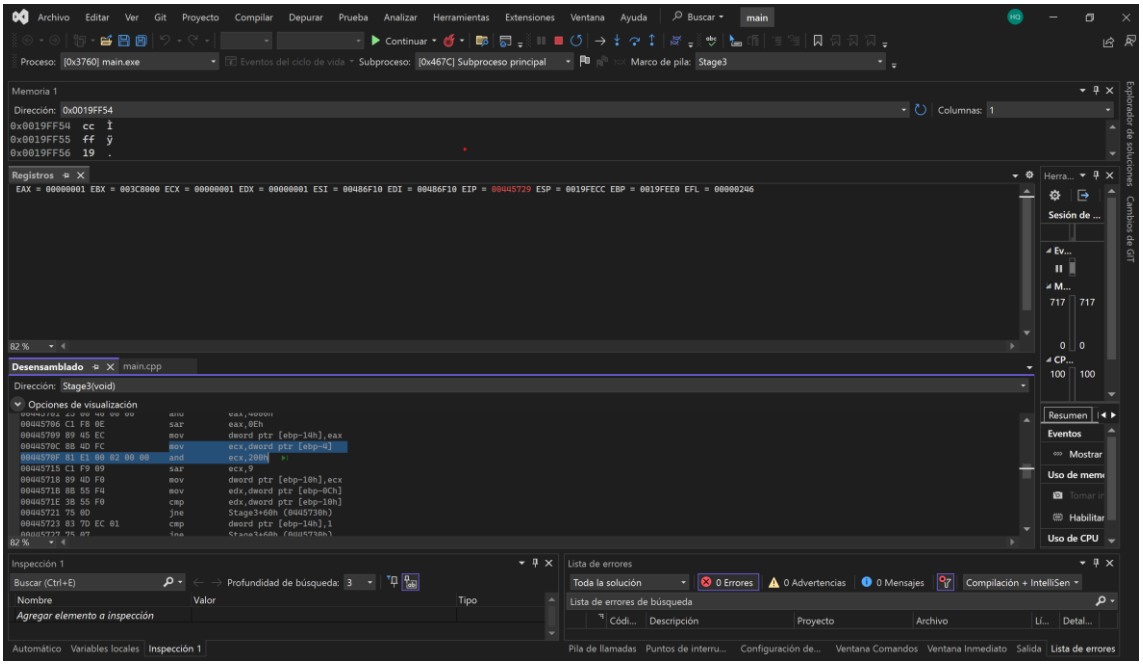
En esta función nos volvemos a meter en la memoria y lo que vemos es que hacer operaciones (and) con máscaras de bits con los dos parámetros que se han pedido por consola.



Aquí se ve como se hace una máscara con el segundo número introducido, hace un and entre el numero introducido y el 40000h, que pone a 1 el registro EAX si numero tiene un 1 en el bit 18 si no lo pone a 0 y lo guarda en el registro ebp-0Ch.



Después hace una máscara con el primer número introducido, una operación and entre ese numero y el 4000h, pone el registro ecx a 1 si el numero tiene un 1 en el bit 14, si no a 0 y lo guarda en la posición ebp-14h.



Ahora hace otra mascara, una operación and con el 200h y el primer número introducido que pone el registro ecx a uno 1 el numero tiene un 1 en el bit 9 y si no a 0.

Ahora hace una comprobación (cmp), compara el resultado de la primera operación and con el resultado de la segunda y si no coinciden la bomba ya está desactivada. Después compara el resultado del tercer and con 1, y si es distinto del mismo estaría desactivada, si no, explotaría.

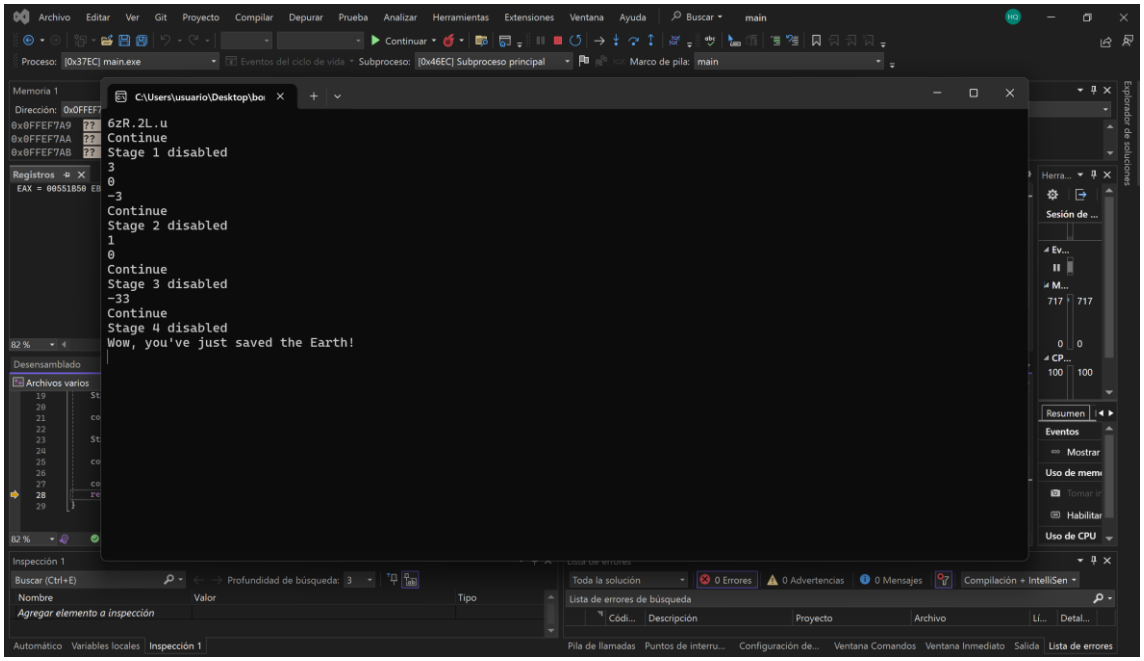
Si el primer numero tiene a 1 el bit 18 y el segundo tiene a 1 el 14 el número es incorrecto y por tanto explota.

Si el primer numero tiene a 1 el bit 10 también explotaría.

Por lo que necesitamos dos números que no cumplan alguna de estas condiciones.

Hemos estado mirando bien por la memoria la ultima fase pero no logramos entenderla muy bien, además la falta de tiempo y de compañeros nos han limitado a tener más ideas, por ello nos hemos quedado aquí. Probando hemos obtenido una respuesta valida, que es que se tiene que introducir un numero de 2 cifras negativo, ambas cifras iguales, pero no sabemos muy bien cuál es la justificación.

Tras desactivar todas las bombas el programa luciría así:



Horas totales desempeñadas:

-Al ser solo dos personas hemos hecho todo el trabajo juntos, no dividiéndonoslo por partes ya que si no seria casi imposible. Ambos hemos desempeñado 11 horas.