Andres Villavicencio

Lab Ollydbg

Necesitarán: Winidows, Ollydbg, y un .exe

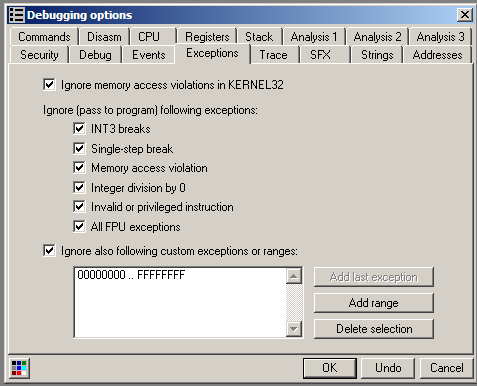
Ejecutar el programa ollydbg

Configurar el debugger para que no muestre excepciones y nos enseñe ciclos.

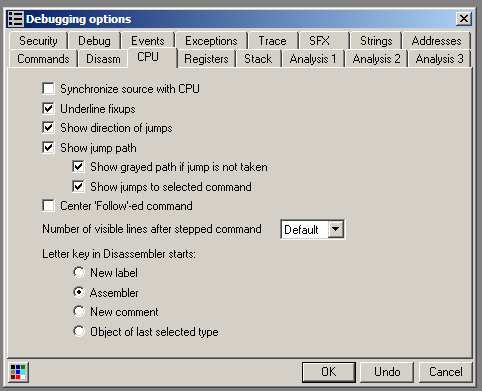
En el menu de opciones vaya a Options -> Debugging options y despues abra el tab de Exceptions.

Asegurese de que quede como la imagen a continuacion

Para agregar un rango seleccione add range e introduzca (00000000) y (FFFFFFFF)



Despues vaya a la pestaña de CPU y configure para que se vea de la siguiente manera



El siguiente paso es abrir el archivo CrackMeDemo pueden intentar correrlo y les enviara una ventana diciendoles que el tiempo de prueba ha expirado.

Para abrirlo en la herramienta arrantren el archivo a la ventana principal.

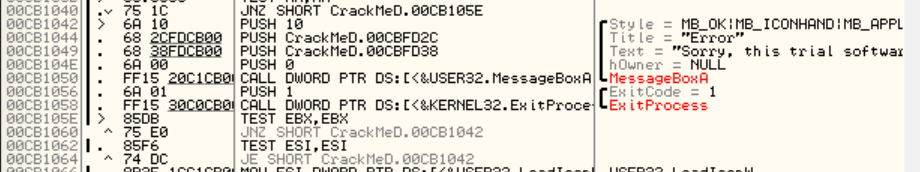
Se encuentra con el codigo binario de la aplicación.

Lo siguiente es correr el debugger para esto pulsen el comando F9

Lo siguiente que deberiamos hacer es abrir el stack para revisar que hay para esto usa el comando alt+k

Despues den click derecho sobre la pantalla de CPU vayan a la opcion de View , les apareceran una lista de modulos. El modulo interesante es el CrackMeD den click sobre el.

Entre los mensajes de error debe aparecer el siguiente:



seleccionen el principio de el proceso (Push 10)

podran ver que una linea roja nos indica los procesos que llegan ahí ( JNZ Short …) y (Je Short..)

para hacer que el programa se salta este proceso lo que debemos de hacer es seleccionar JNZ click derecho y seleccionar binary -> Fill with N0Ps

Esto lo que hace es cambiar la instrucción de salto a NOP (no operation) instruction, para evitar que llegue a esta instrucción.

Repetir el mismo proceso con Je short

Para guarder las modificaciones click derecho en la ventana de CPU click en “Copy to Ejecutable”, y seleccionar “All Modifications”. Presionar en “Copy all”.

Aparece otra ventana dar doble click y seleccionar  “Save File”, es recomendable guardar el Nuevo archive con otro nombre para diferenciar del original.

Una vez acabado con esto correr el Nuevo programa y debe abrirse una ventana indicando que el archive se abrió con éxito.

Bibliografía:

https://erichokanson.me/2015/04/17/reverse-engineering-with-ollydbg/