REVERSE ME

En uno de los laboratorios de computación encuentras una máquina apagada con un post-it en el lateral: "/root/Desktop/reto36/reversesecret - Resolver mediante ingeniería inversa". Parece que te animas a encender el ordenador, un viejo pentium que todavía arranca. Guardas el fichero a tu máquina para trabajar cómodamente y empiezas el desafío.

Al reverso del post-it se puede leer: "Enviar flag a mi número personal, se recompensará"

¿Qué condiciones necesitará este binario para que imprima la flag?

Pistas

1. El binario comprueba dos argumentos para validar la flag.

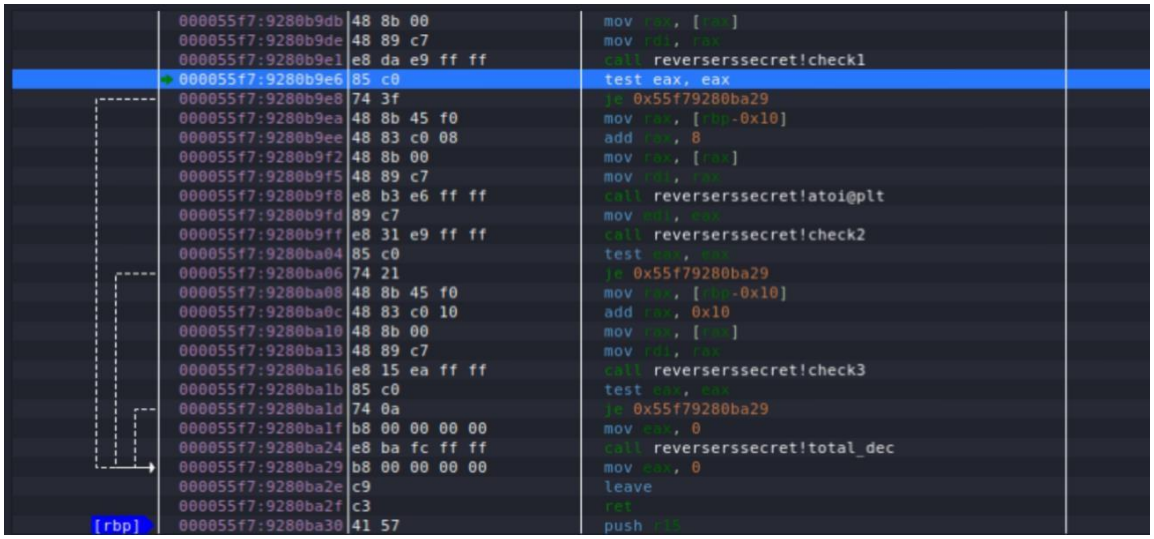
2. El primer argumento comprueba el número de ficheros existentes en el directorio actual.

3. El segundo argumento deberá componerse de una determinada ruta a un fichero existente. Créalo si no existe.

Abrimos el ejecutable con la herramienta “cutter”, una de las posibles elecciones que tenemos para realizar la ingeniería inversa. Al analizar la función main comprobamos que requiere una serie de parámetros, concretamente 2: si argc >= 4 o argc <= 2 salir de la función, es decir, se requiere que argc sea igual a 3: el nombre del ejecutable más 2 parámetros de entrada.

Abrimos el archivo para analizarlo con cutter:

Empezamos a debuggear con F8 y F7 para ver que es lo que hace el código ensamblador del archivo. La idea es llegar a los checks para poder quitarlos y ver si son necesarios o simplemente se pueden ignorar.

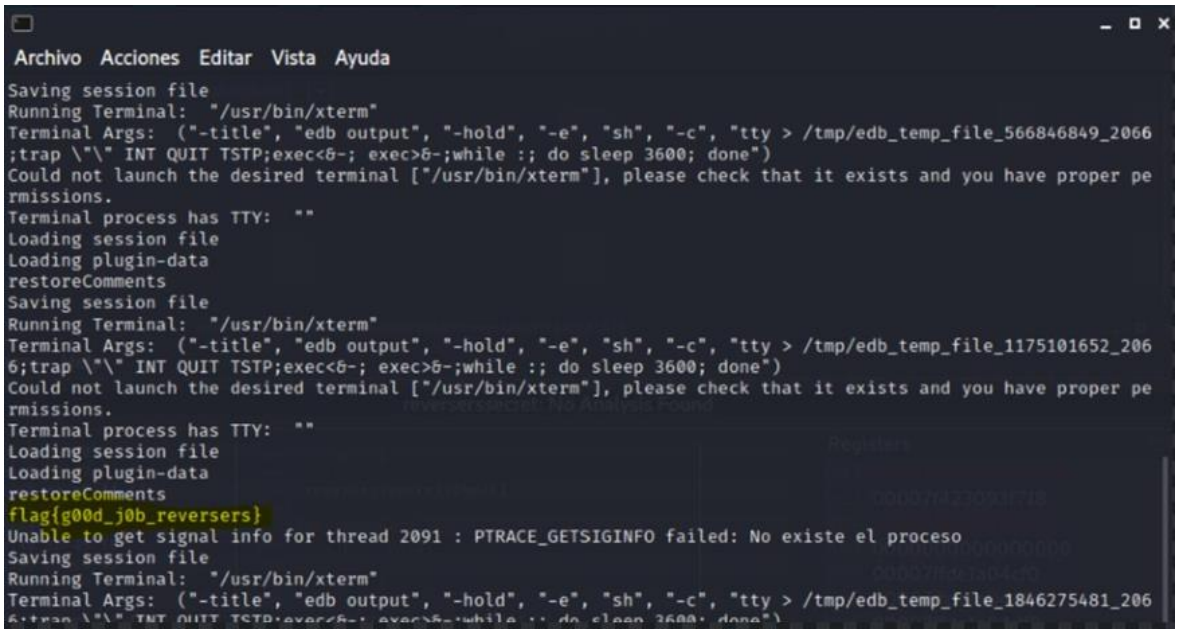


Con F8 llegamos hasta las rutinas de ejecución y sus correspondientes JE. Pasamos y cuando llegamos a los JE hacemos click en el botón derecho del ratón, luego en Edit y finalmente en Fill with NOPs:

Esta acción la hacemos en los 3 primeros checks y seguimos con F8:

Finalmente, el programa acaba con un return 0 sin fallos y vemos que en el log que aparece en la ventana del propio programa hay un mensaje oculto

fiag{g00d_j0b_reversers}


Archivo Acciones Editar Vista Ayuda
Saving session file
Running Terminal: "/usr/bin/xterm"
Terminal Args: ("-title", "edb output", "-hold", "-e", "sh", "-c", "tty > /tmp/edb_temp_file_566846849_2066
;trap \"\" INT QUIT TSTP;exec<&-; exec>&-;while :; do sleep 3600; done")
Could not launch the desired terminal ["/usr/bin/xterm"], please check that it exists and you have proper pe
rmissions.
Terminal process has TTY: ""
Loading session file
Loading plugin-data
restoreComments
Saving session file
Running Terminal: "/usr/bin/xterm"
Terminal Args: ("-title", "edb output", "-hold", "-e", "sh", "-c", "tty > /tmp/edb_temp_file_1175101652_206
6;trap \"\" INT QUIT TSTP;exec<&-; exec>&-;while :; do sleep 3600; done")
Could not launch the desired terminal ["/usr/bin/xterm"], please check that it exists and you have proper pe
rmissions.
Terminal process has TTY: ""
Loading session file
Loading plugin-data
restoreComments
flag{g00d_j0b_reversers}
Unable to get signal info for thread 2091 : PTRACE_GETSIGINFO failed: No existe el proceso
Saving session file
Running Terminal: "/usr/bin/xterm"
Terminal Args: ("-title", "edb output", "-hold", "-e", "sh", "-c", "tty > /tmp/edb_temp_file_1846275481_206