

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"

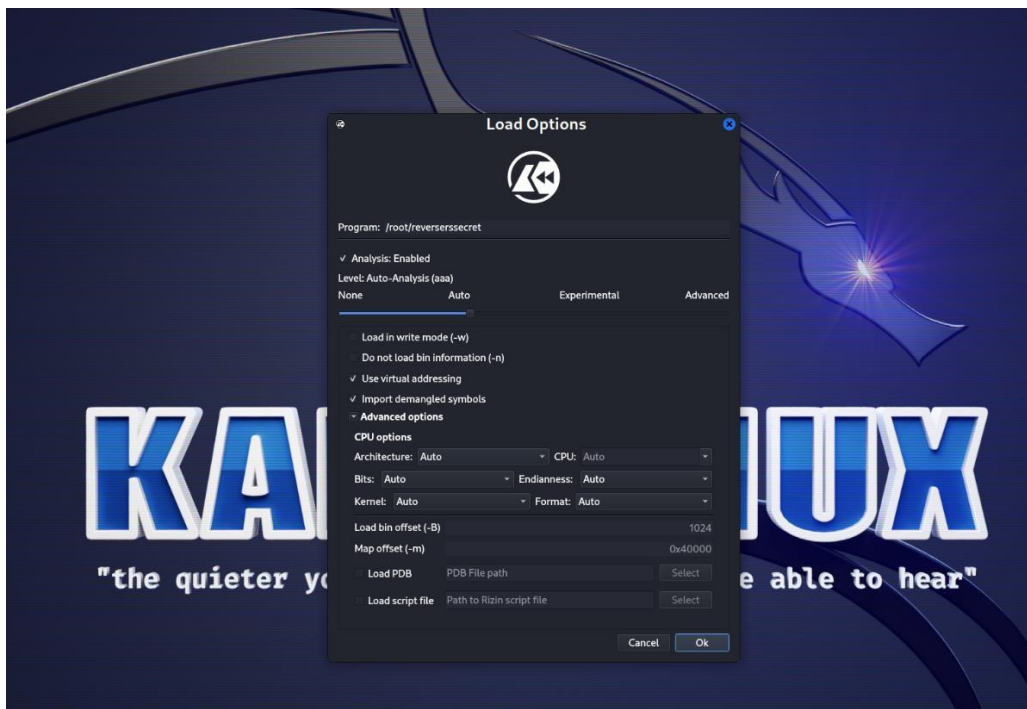
¿Qué condiciones necesitará este binario para que imprima la flag?

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.

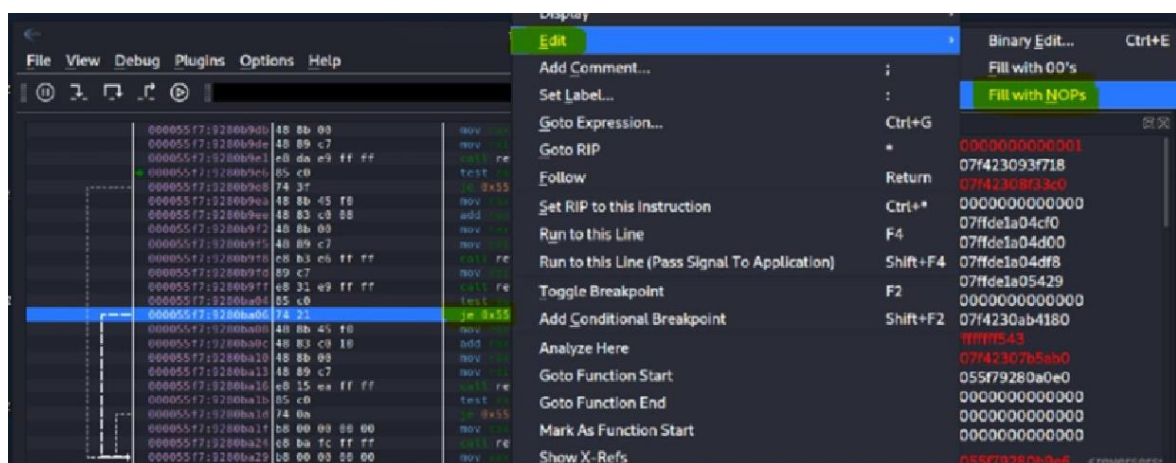
Abrimos el archivo para analizarlo con cutter:



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.

000055f7:9280b9db	48 8b 00	mov rax, [rax]
000055f7:9280b9de	48 89 c7	mov rdi, rax
000055f7:9280b9e1	e8 da e9 ff ff	call reverserssecret!check1
000055f7:9280b9e6	85 c0	test eax, eax
000055f7:9280b9e8	74 3f	je 0x55f79280ba29
000055f7:9280b9ea	48 8b 45 f0	mov rax, [rbp-0x10]
000055f7:9280b9ee	48 83 c0 08	add rax, 8
000055f7:9280b9f2	48 b0 00	mov rax, [rax]
000055f7:9280b9f5	48 89 c7	mov rdi, rax
000055f7:9280b9f8	e8 b3 e6 ff ff	call reverserssecret!atoi@plt
000055f7:9280b9fd	89 c7	mov rdi, rax
000055f7:9280b9ff	e8 31 e9 ff ff	call reverserssecret!check2
000055f7:9280ba04	85 c0	test eax, eax
000055f7:9280ba06	74 21	je 0x55f79280ba29
000055f7:9280ba08	48 8b 45 f0	mov rax, [rbp-0x10]
000055f7:9280ba0c	48 83 c0 10	add rax, 0x10
000055f7:9280ba10	48 b0 00	mov rax, [rax]
000055f7:9280ba13	48 89 c7	mov rdi, rax
000055f7:9280ba16	e8 15 ea ff ff	call reverserssecret!check3
000055f7:9280ba1b	85 c0	test eax, eax
000055f7:9280ba1d	74 0a	je 0x55f79280ba29
000055f7:9280ba1f	b8 00 00 00 00	mov eax, 0
000055f7:9280ba24	e8 ba fc ff ff	call reverserssecret!total_dec
000055f7:9280ba29	b8 00 00 00 00	mov eax, 0
000055f7:9280ba2e	c9	leave
000055f7:9280ba2f	c3	ret
000055f7:9280ba30	41 57	push rbp

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 permissions.
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_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 permissions.
reversers3c3c3c No Analysis found
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_2066;trap \"\" INT QUIT TSTP;exec<&-; exec>&-;while ;; do sleep 3600; done")
Registers
00007f423093f718
00000000
00007f423093f718
```