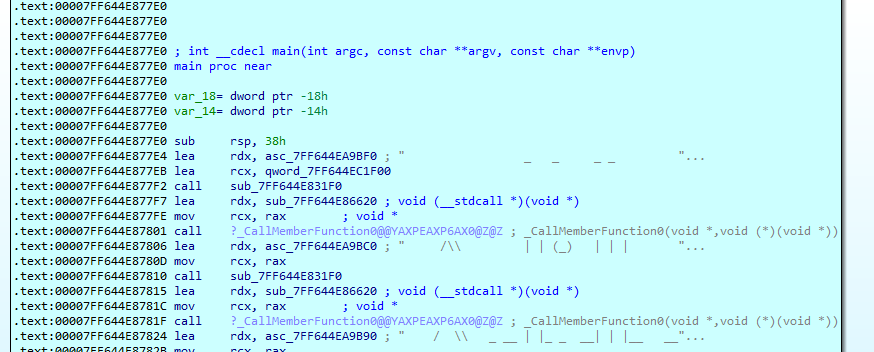
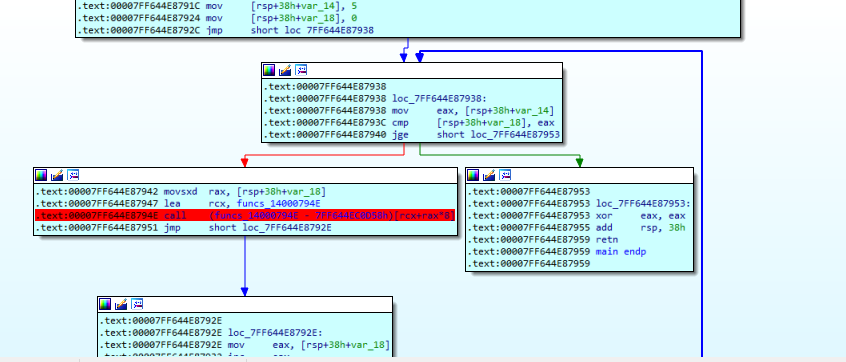
* We has a x64 PE file, use a Debugger (IDA in my case), we get the asm code of it.



The important is there:

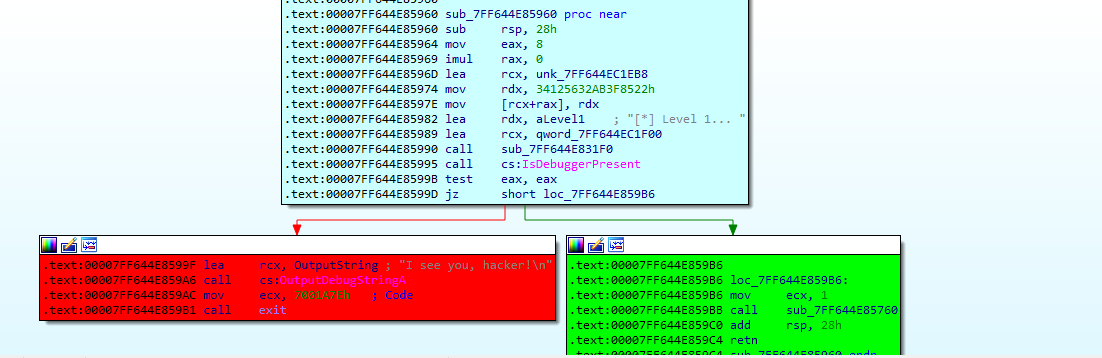


it’s easy to see that this is a loop from 0 to 5 <-> 5 challenges

This pass is the first challenge

Set a breakpoint like the picture above

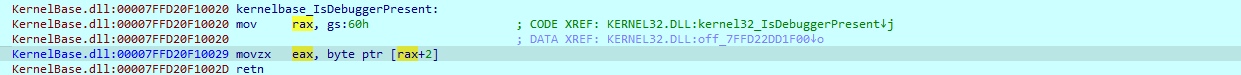
F9 then F7, we jump to the first challenge



First challenge uses IsDebuggerPresent API to test us

(IsDebuggerPresent read a word at [gs:60h] + 2 to determine debugger)

-Set a breakpoint at call IsDebuggerPresent and jump into it



the address value at gs:60h is read into rax

we go to rax then set the value at rax +2 to 0x0000

Easy Bypass the first challenge



go to the address in console window -> we get the flag



(At the first time i tried this challenge, i just fixed the value of rax after going through IsDebuggerPresnt, it still jumps into goodboy, but i didn't get the flag, I don’t know why?)