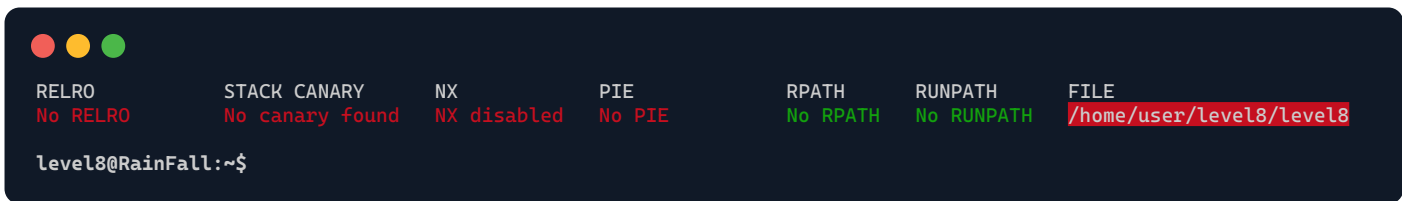


./level8



Decompiled file with *Ghidra*:

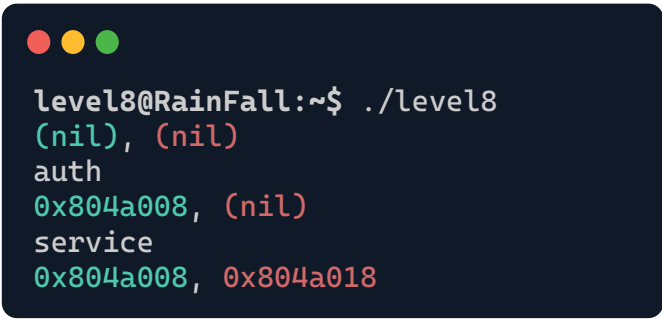
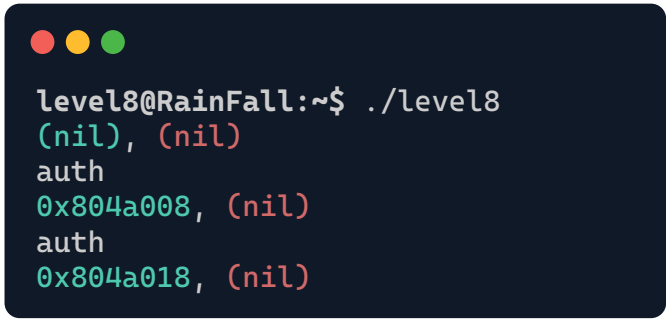


This one was pretty hard, we spent a lot of time looking at the de-compiled file, and this is what we found after relentless efforts.

We have a program that operates within an endless loop, utilizing the **fgets()** function to capture user input. Subsequently, this input undergoes processing and passes through a series of conditional **if** statements. Additionally, we have two pointers whose initial state is set to **null**, and their values are displayed on the screen.



After some experimentation, we observed that employing the **auth** or **service** command results in memory allocation and subsequently shifts the address of the pointer by 16 bytes.



Since the input is restricted to a length of 30 characters, we cannot overflow the 32 bytes we require. To achieve our objective, we will leverage the existing program functions. Our discovery revealed that we must initially allocate our **auth** variable within the program and then employ the **service** command to allocate memory following our address. By repeating this process twice, we can write 32 bytes into the memory, resulting in **auth[8]** being the first character of our "service" string.

