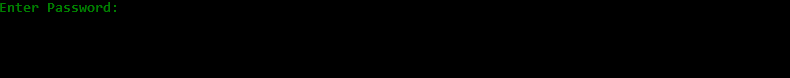
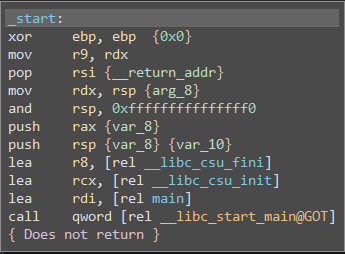
I got the binary file of my friend’s login system. When it is run this is what I see:



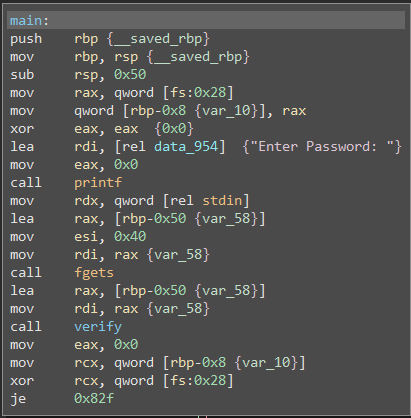


It seems like the program only requires a password in order to get in.

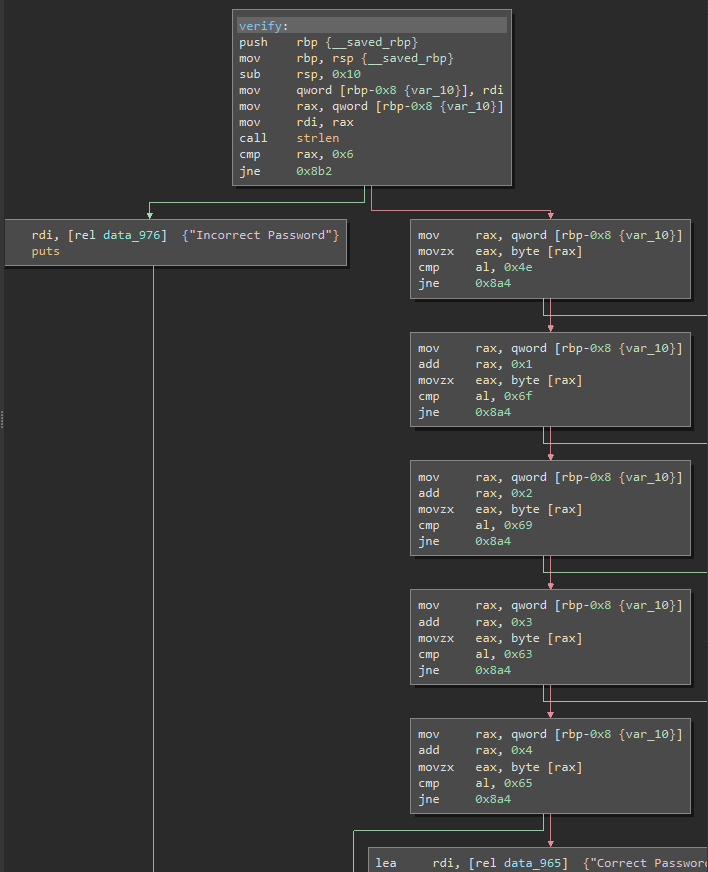
I used Binary Ninja in order to open up and decompile the binary file that was given. I dragged the file in and this is what I saw.



This is what happens on execution of the command. On the third last line, it is loading the main reg32. This means that it is where the main function is loaded and ran. When checking the main function this is what I saw.



I see “{Enter Password:}” which appeared in the very beginning when the program was executed. This means that the password check is somewhere below that line. I see that fgets was also executed which is most likely when the stdin is collected. The call after refers to verify which is most likely where the password is being checked.



At this point am very certain that the password is contained here because there seems to be an if statement in which one leads to “Incorrect Password” and the other leads to “Correct Password”. So I looked in to right hand side of the statement. In each of the segments I realised that there is a “cmp” command which are comparing something. Since there are 5 “cmp”, there are two options. The password is 5 characters long or there are 5 passwords. However, I realised that the cmp’s second argument was not holding an address but it is holding a value which is most likely a hexadecimal.

Hexadecimal: 0x4e, 0x6f, 0x69, 0x63, 0x65

When converted to ASCII: Noice

