challenges.re Challenge #30

Challenge Author: Dennis Yurichev

Writeup by scaredandalone

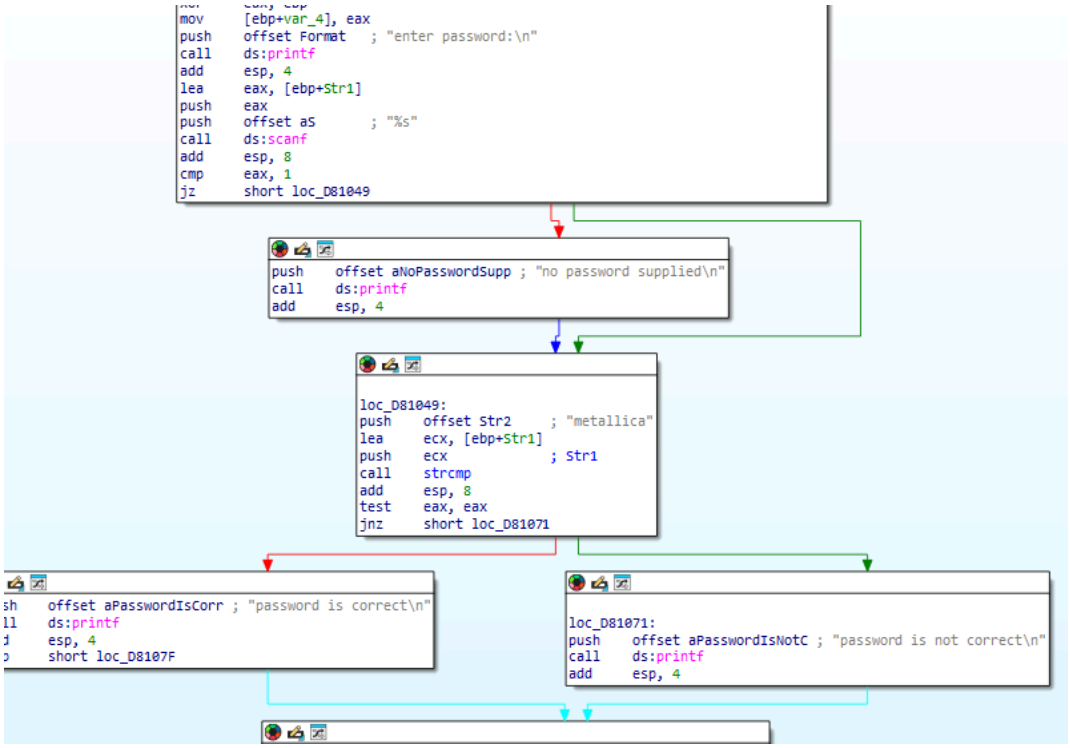
This program requires a password. Try to find it.

As an additional exercise, try to change the password by patching the executable file. Also try using one with a different length. What is the shortest possible password here?

Also try to crash the program using only string input.

Open the executable in your disassembler, I'm using IDA for this challenge.

Figure 1: IDA graph view



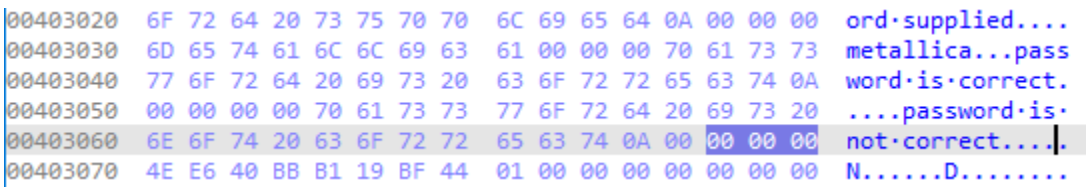
This is just a hard-coded password, as we can see above.

metallica

However, we are asked to patch the file, alter the length and the value of the password and try to crash the program with input.

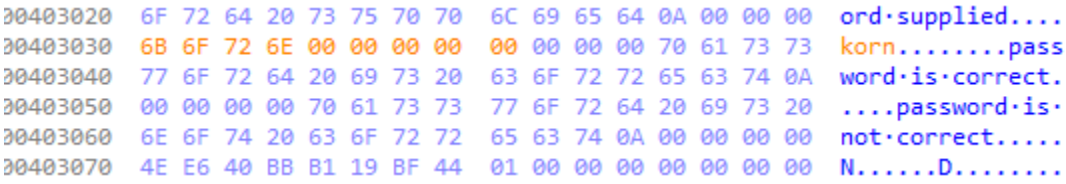
Patching is pretty simple, we can just change the value of the Str2 variable (metallica) to a password of our choosing.

Figure 2: Password location in hex dump



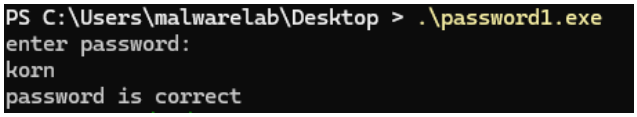
Looking at the hex view, we can see where metallica is stored.

Figure 3: Changing the hex values



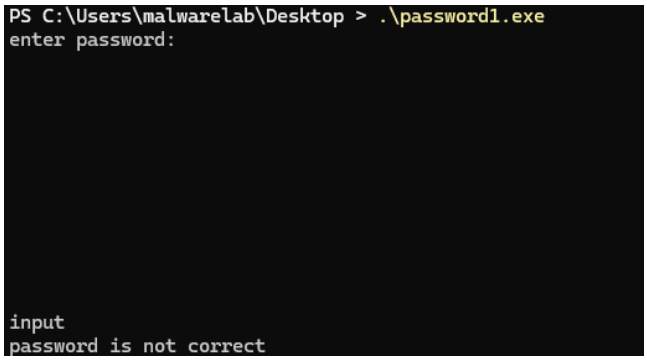
In this example, I am altering the value of the variable to a string that is smaller than the original. This means that we don't really need to adjust the array size, it's already aligned and the remaining bytes can just be null.

Figure 4: Running the program with patched password



The shortest possible password is 1 bytes long. This is because scanf (the function that is used to get the user input) expects non-empty input and loops until input is provided.

Figure 5: Shortest Password

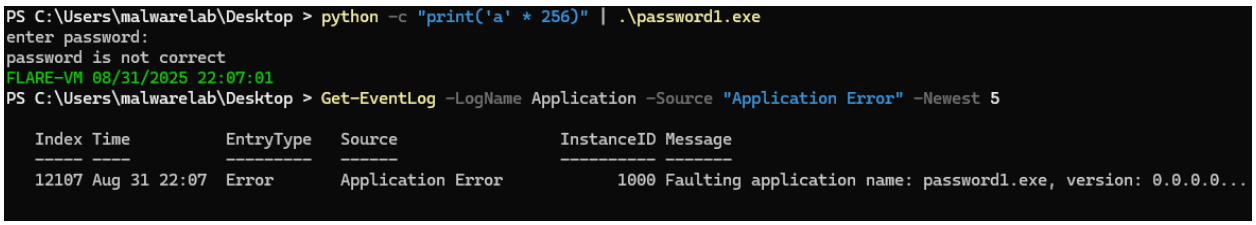


As we can see, it does not allow us to put a null value, and it expects at least one char.

Now it's time to crash the program.

I first tried to overflow the buffer that stores the user input.

Figure 6: Program crash



It looks like it worked and the program crashed. As expected.