

Solution to F-crackme by Tk334

Overview

There are two ways to find out the password for this crackme. First, just by opening up the application, you are asked to input a username. More often than not, this means that the password has some relationship to whatever name you input. This gives us an idea of what to look for in the code. The tool I used is the IDA disassembler.

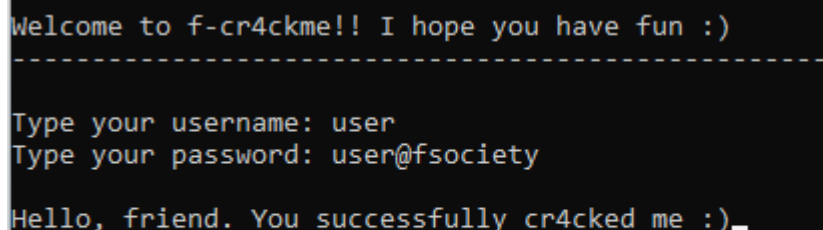
Method 1:

This method is very simple. It consists of viewing the pseudocode of the program. Through this code, we can clearly see that the password is the username input concatenated with another string.

```
_main(argc, argv, envp);
message();
printf("Type your username: ");
scanf("%20s", Destination);
v8 = checkUsername(Destination);
if ( v8 )
{
    if ( v8 != 1 )
        exit(0);
    strcpy(Source, "Mr.");
    strcat(Source, Destination);
}
else
{
    strcpy(Source, "@fsociety");
    strcat(Destination, Source);
    strcpy(Source, Destination);
}
printf("Type your password: ");
scanf("%30s", Str2);
if ( strcmp(Source, Str2) )
    printf("\nI'm sorry. You are not supposed to be here.");
else
    printf("\nHello, friend. You successfully cr4cked me :)");
return 0;
```

The checkUsername function simply outputs 1 if the username input is above 8 characters, and 0 if it is below. You can read this code by clicking on "checkUsername(Destination)". By looking at the code above, we can deduce that if the username is above 8 characters, the password is "Mr." concatenated with whatever the username input it. If the username is below 8 characters, the password is the username input concatenated with "@fsociety".

Example:



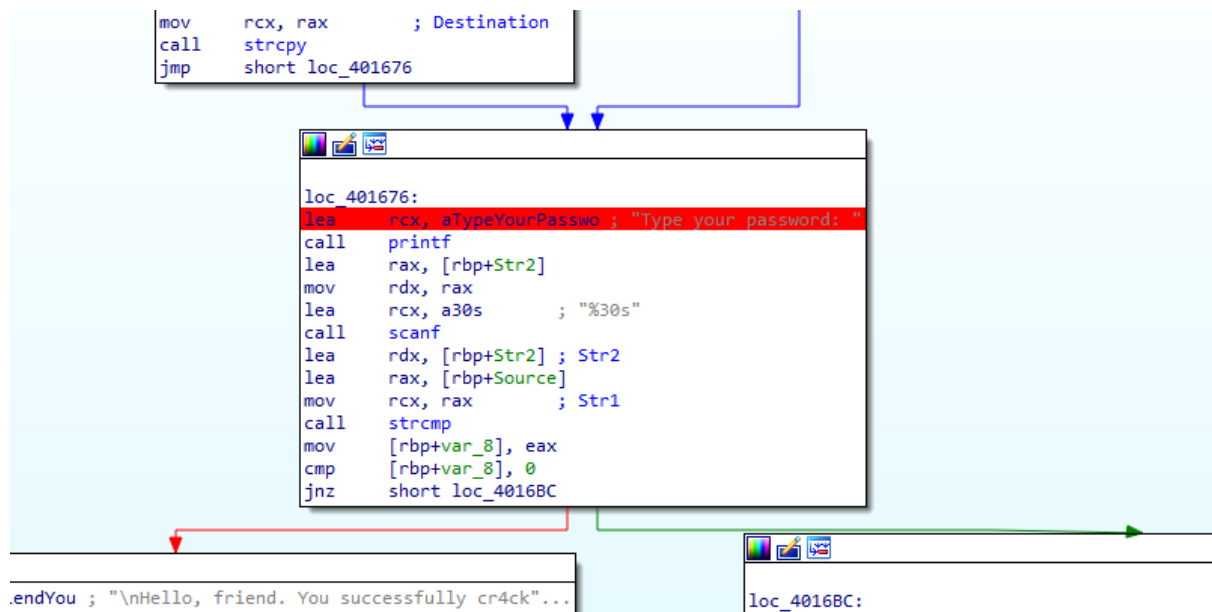
```
Welcome to f-cr4ckme!! I hope you have fun :)
-----

Type your username: user
Type your password: user@fsociety

Hello, friend. You successfully cr4cked me :)_
```

Method 2:

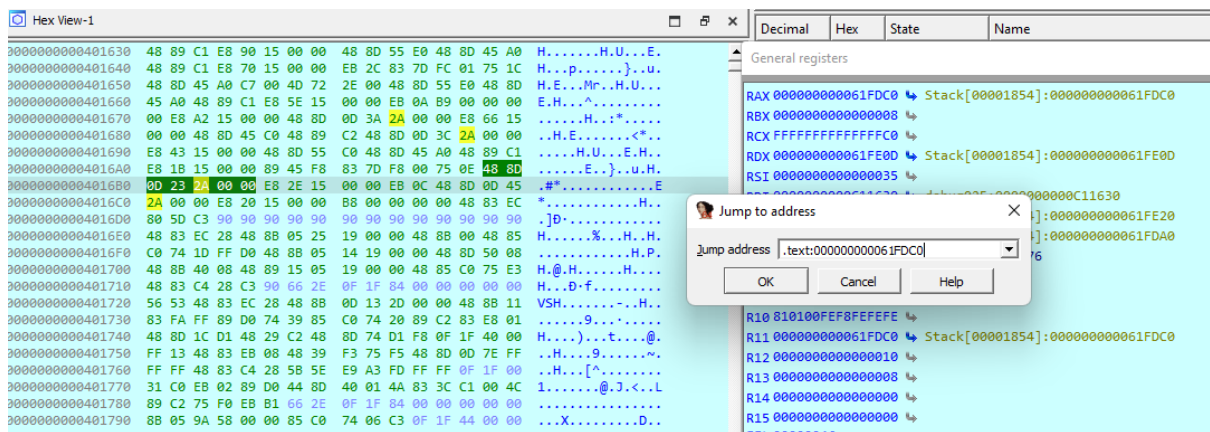
This method makes use of the hex dump on IDA. In order to do this, you should put a breakpoint in an appropriate location. I put mine as shown:



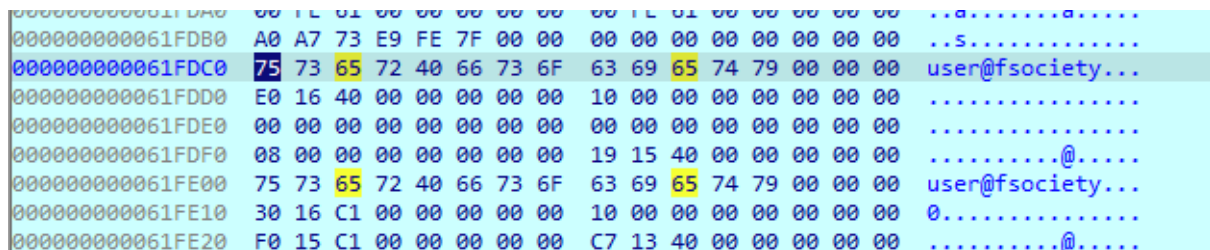
You then run the code as normal (I inputted "user" as my username) so that the program stops at the breakpoint. Then you can look at the general registers. The RAX register should show part of the password.



Now you should be able to deduce the password from this, however, if you want to see the full password. Go to the hex dump (this can be found by going from views >> open subviews > hex dump) if you can't find the hex dump. Once you have done this, press "g" to search for a location. You then copy the RAX location.



Then, simply click “Ok” and you will be taken to the password in the hex dump. As shown below:



Note: If your program keeps stopping before you get a chance to see the congratulating message, put a breakpoint shortly after it.

