BehindTheScenes Overview

Difficulty: Very Easy :D
Points: 10

Challenge Description:
On our regular checkups of our secret flag storage server we found out that we were hit by ransomware! The original flag data is nowhere to be found, but luckily we not only have the encrypted file but also the encryption program itself.

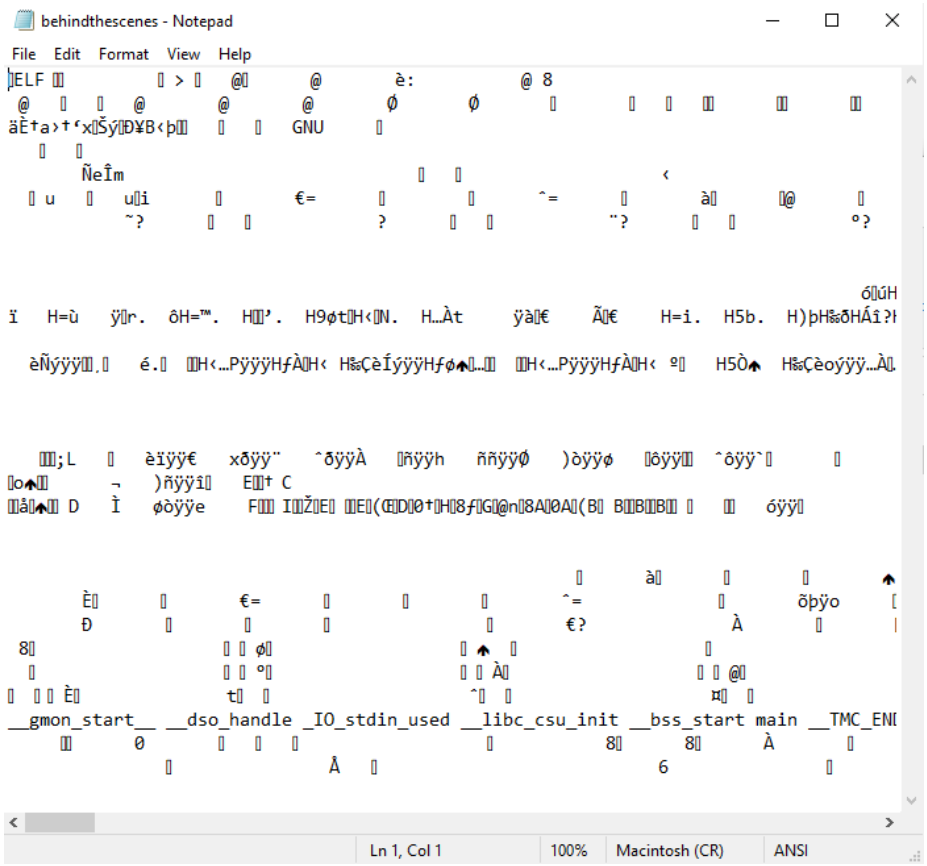
Tools Used

1. Ida FreeWare

Analysis

All we are given is a single file named “behindthescenes”. Let’s take a look into what it is.

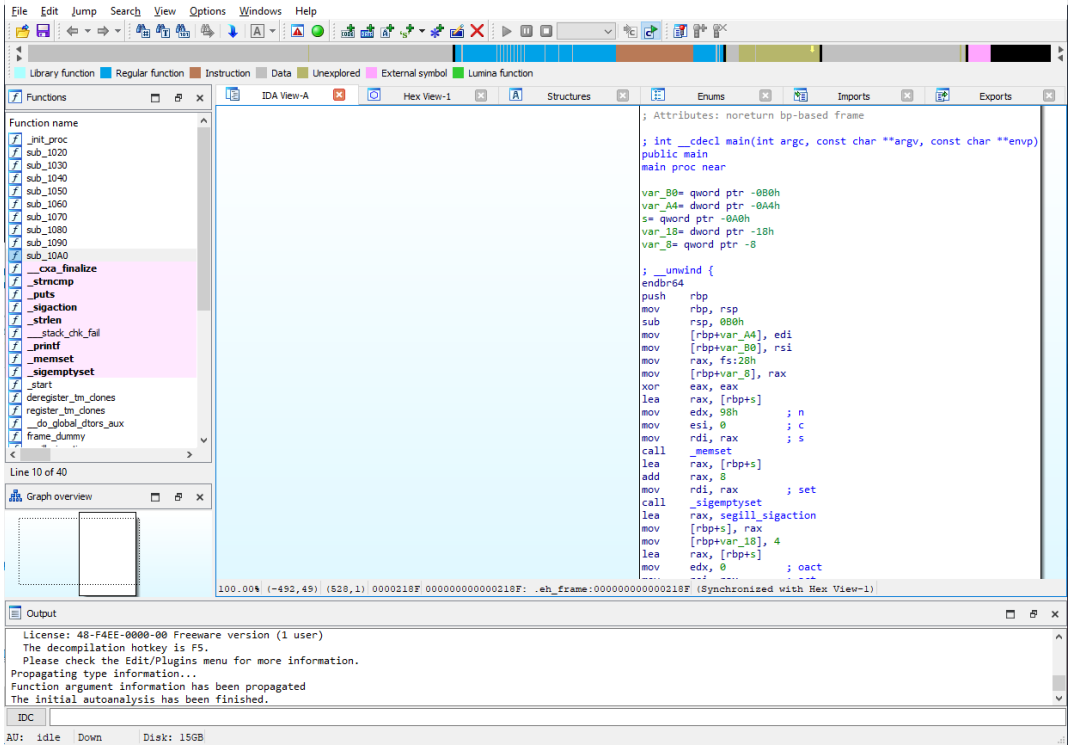
If we open the “behindthescenes” file using something simple such as notepad, we are greeted with this unfortunate-looking screen:



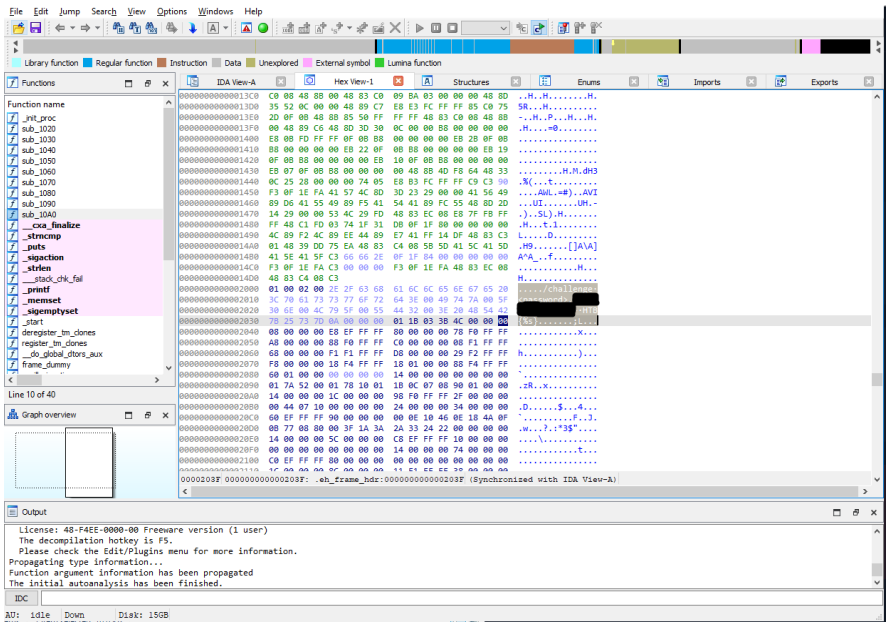
Unfortunately, not that useful.

My first idea after seeing this file was to put it into a disassembler to see if we could find anything hidden that is not available on the surface. I decided to use IDA-Freeware since that is what I have readily available.

Opening the file in IDA is as seen below:

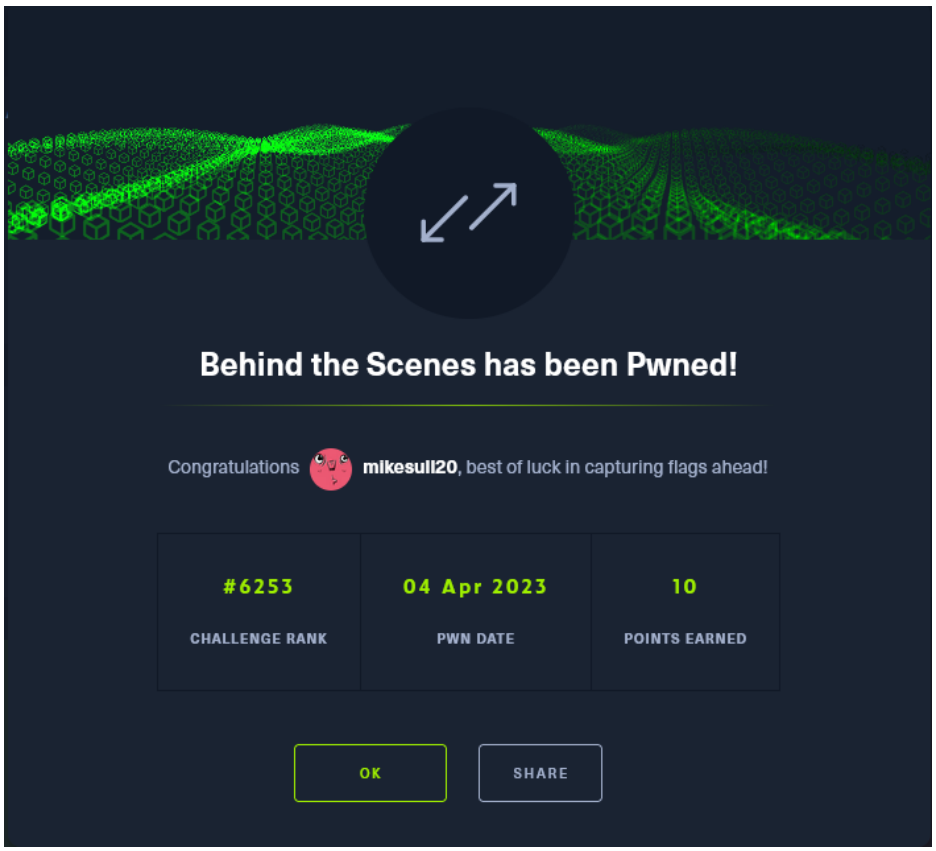


Here we can see the machine code on the main screen, but looking quickly at it, it doesn't seem to be entirely useful. What I decided to move over to next was the Hex view. The goal would be to look through the hex view to see if there is any hidden information within. Sure enough, after scrolling down the hex view, there was the flag.



I have blacked out the key, but I assure you, it is there.

And sure enough:



Conclusion:

In conclusion, this easy reverse engineering challenge on HackTheBox provided a great opportunity to practice reverse engineering skills and gain more experience working with binary files. By using IDA Freeware, we were able to successfully analyze and understand the binary/hex, and ultimately find the solution to the challenge. This challenge was a great learning experience and provides a solid foundation for more advanced reverse engineering challenges. This was a great launch pad for all the other reversing challenges that I hope to complete in the future! Overall, I highly recommend this challenge to anyone looking to improve their reverse engineering skills.

Additional Details: