Challenge 02

Flag: FLAG{"D1ff1cu1t_M3hhhhhhhh?"}

Tldr: Change date to 12/12/2018 , “BlackSheepWall”

Decompile binary.exe using Ghidra. Look for the string “What is the Magic Word: ”

After looking through the decompiled code, I realise that the first validation is checking if the input is “BlackSheepWall”

I open up OllyDbg. Run it once setting my breakpoint at the CMP address and key in “BlackSheepWall”. Slowly, I stepped into the next CMP instruction, CMP EAX,7E2 . This is the next validation.

My EAX has a value of 7E3(2019d) and is compared to 7E2(2018d). I am not supposed to JUMP, so my EAX should have a value of 2018d.

Let’s see how EAX is derived. EAX is first obtained from 3 instructions before, by moving a stack value into EAX. The value is 0x77(119d). Then it is added with 0x76C(1900). Not much is understood from here. Let’s go back to Ghidra.

In Ghidra, same few instructions in the decompiled view seems to be related to year, month and day. 2018 and 2019 are like year values for this and last year. Could it be related to setting my OS year?

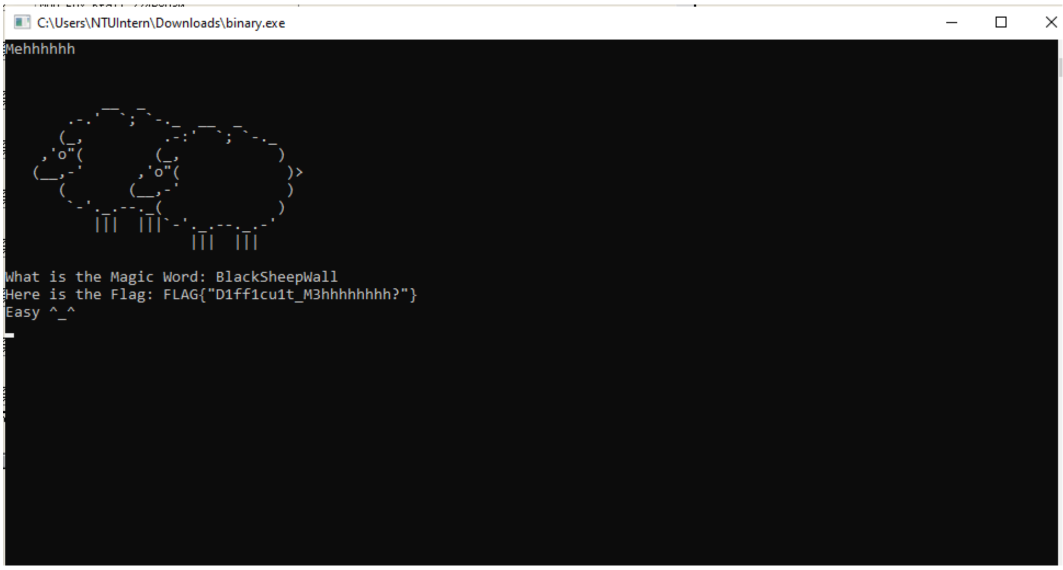
I changed my current year to 2018 and go back to debug using Ollydbg. Indeed, the comparison skips the JNZ instruction.

Next CMP instruction. CMP EAX,0C. 0C is 12d and EAX contains 9d. Currently it’s September(9th Month). I changed my current month to December. EAX is now 12d. Skips the JNZ instruction.

Another CMP instruction. This time it must be the day. EAX is compared with a value in a stack, 0x1A(26d). This value is my current day. My day needs to be the same as my month value in order to proceed.

I set my OS date to 12/12/2018. Open up OllyDbg and run binary.exe. Keyed in “BlackSheepWall”.

FLAG{"D1ff1cu1t_M3hhhhhhhh?"}



C:\Users\NTUIntern\Downloads\binary.exe

```
Mehhhhhh



           __  _
       .-.'  `; `-._  __  _
      (_,         .-:'  `; `-._
    ,'o"(        (_,           )
   (__,-'      ,'o"(            )>
      (       (__,-'            )
       `-'._.--._(             )
          |||  |||`-'._.--._.-'
                     |||  |||

What is the Magic Word: BlackSheepWall
Here is the Flag: FLAG{"D1ff1cu1t_M3hhhhhhhh?"}
Easy ^_^
```