Challenge: Hunting License

# Challenge Description :

**STOP! Adventurer, have you got an up to date relic hunting license? If you don't, you'll need to take the exam again before you'll be allowed passage into the spacelanes!**

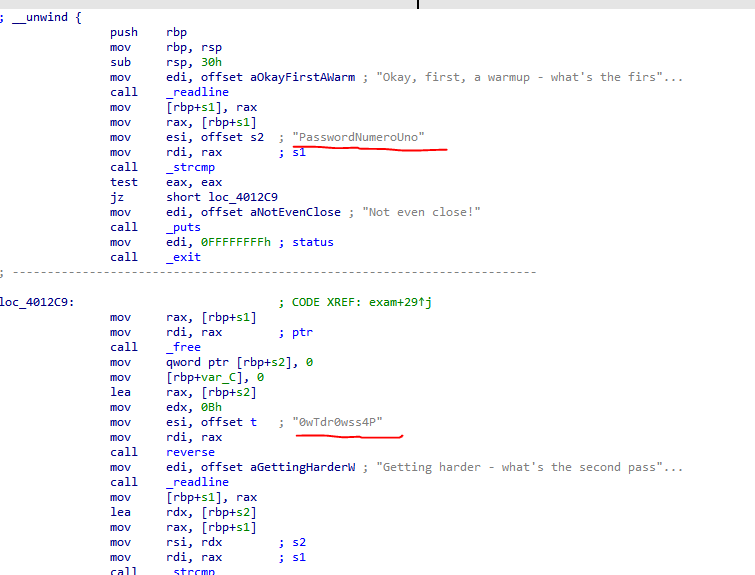
# Context :

## Analyze a Compiled File, to get three passwords hidden within itself, one is in the open, one is in reverse and one has XOR encryption.

## After gaining the password you need to answer a small questionnaire with the password requested at the end to gain the flag.

# Flag :

* First Install the files and start decompiling the File. The first two passwords should be really easy to get as it's really noticeable. Depending on the tool you use.

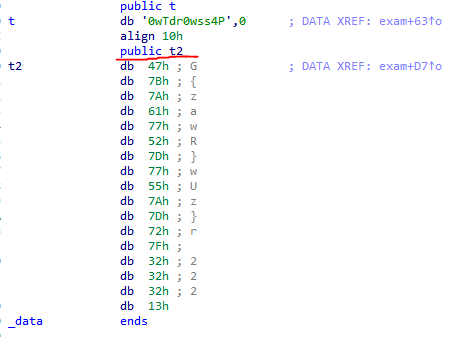


* The first flag is correct by default, for the second one you will need to reverse the string so it is spelt correctly.

**[ PasswordNumeroUno ]**

**[ P4ssw0rdTw0 ]**

* The Third flag is a bit harder to get, its under a name called “**T2**”



* Reading some of the Decompiled code and its binary suggested that XOR is being used to encrypting the string in “**T2**” with the Key of just “**19**”

**[ 0x47 0x7b 0x7a 0x61 0x77 0x52 0x7d 0x77 0x55 0x7a 0x7d 0x72 0x7f 0x32 0x32 0x32 0x13 ]**

* Deciphering this will give the password needed to complete the questionnaire. By applying the XOR operation with the key 19 to each number in the list, we translate them into a different set of numbers. The transformed numbers represent letters of the alphabet.
* We convert these numbers back into letters. After decoding each number using the key 19, the outcome should reveal the password "**ThirdandFinal!!!**".
* Here is the python code I used to decode this.

Make sure to Add in the Right Array to decode the actual Password

array = [ 0x7a ,0x7d ,0x72, 0x7f ,0x32, 0x32 ,0x32, 0x13]

size\_array = 17

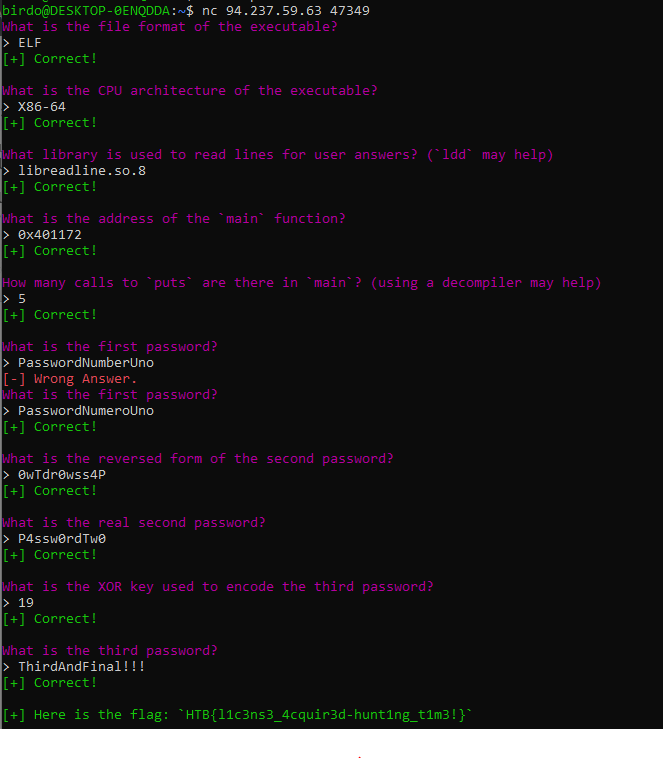
actual\_password = bytearray(17)

for i in range (17):

actual\_password[i] = array[i] ^ 19

print(actual\_password)

* **To get the Flag for this one you will need to start up the Instance and Netcat into the IP:PORT, A TUI should pop-up as a questionnaire, asking questions about the file, these should be straight-foward.**



* **Finishing the Questionnaire should provide you with a flag.**
  + - * **HTB{l1c3ns3\_4cquir3d-hunt1ng\_t1m3!}**