jamk.fi

Reverse Engineering TTC6510-3002

Joonatan Ovaska

A K M MAHMUDUL HAQUE
AB0208

Student number: 2110841

Lab02
Date: 13.09.2023

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

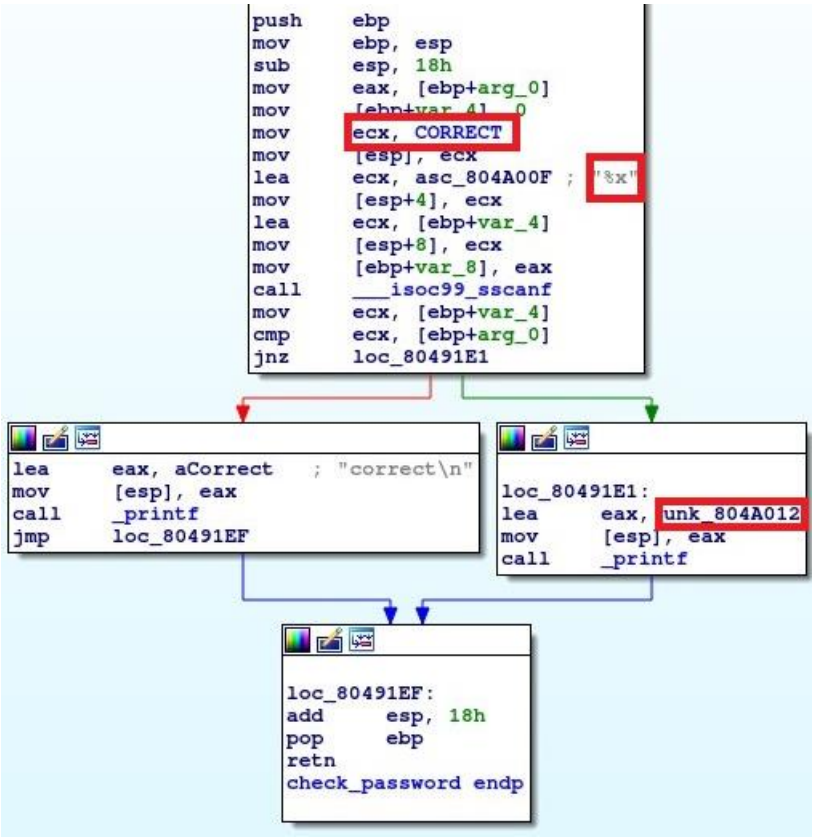
Steps

- At the **Main** function the comment **“Insert password”** grabbed my attention then reading thoroughly gives me confidence when in called for print.

- By **%d** my guess is that the input should be a decimal.

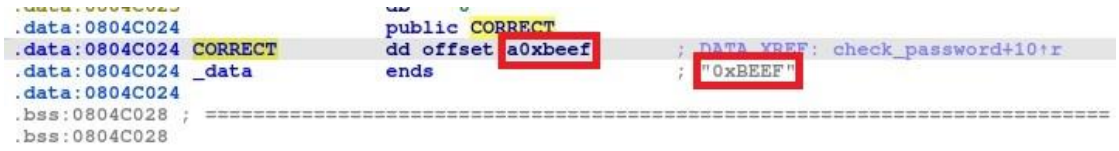
```
push    ebp
mov     ebp, esp
sub     esp, 28h
mov     eax, [ebp+argv]
mov     ecx, [ebp+argc]
mov     [ebp+var_4], 0
mov     [ebp+var_8], 0
lea     edx, aPassword  ; "Password: "
mov     [esp], edx
mov     [ebp+var_C], eax
mov     [ebp+var_10], ecx
call    _printf
lea     ecx, aD         ; "%d"
mov     [esp], ecx
lea     ecx, [ebp+var_8]
mov     [esp+4], ecx
mov     [ebp+var_14], eax
call    ___isoc99_scanf
```

- Next, the action goes to the function call **check_password** where it needs digging.

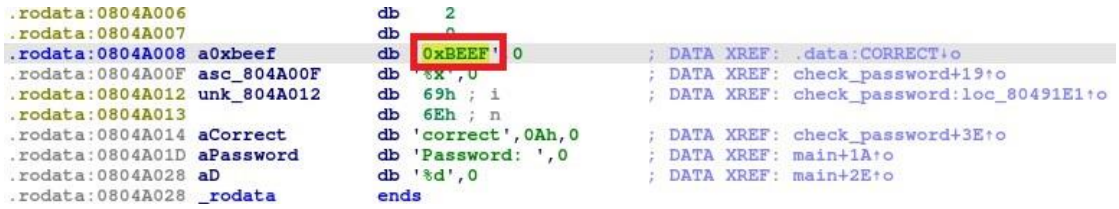


- By **%x** it depicts that the input is converted in string value, so I should look for some string for my guess also.

- Then digging into **Correct** in the **ecx** registry opens up the following where I can see a string OxBEEF (it is also a hexadecimal value, a point of suspicion).



- Later digging into **unk_804A012** also shows the same **OxBEEF** hexadecimal value that can be taken into consideration.



- Converting the hexadecimal **OxBEEF** value into decimal we get **48879,** which later input as the password.

- The above input proves the password.

Topic	**Time**
Lab02	2 hours
Report writing	1 hours