jamk.fi

Reverse Engineering TTC6510-3002

Joonatan Ovaska

A K M MAHMUDUL HAQUE
AB0208

Student number: 2110841

Lab01
Date: 06.09.2023

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

First Step

- 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.

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

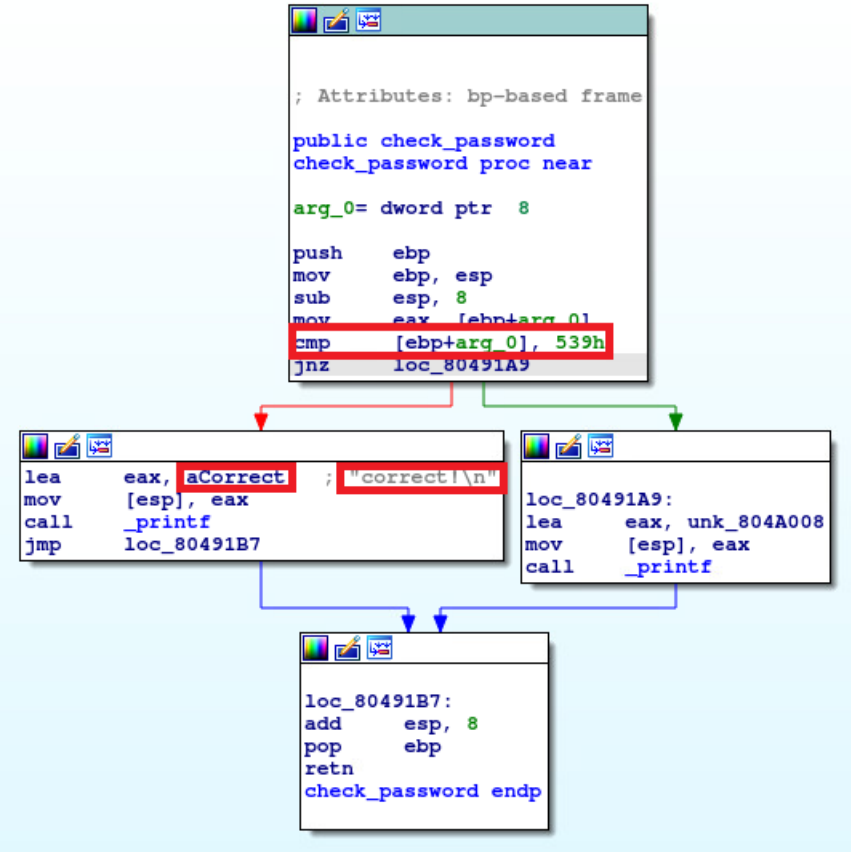
```
public main
main proc near

var_18= dword ptr -18h
var_14= dword ptr -14h
var_10= dword ptr -10h
var_C= dword ptr -0Ch
var_8= dword ptr -8
var_4= dword ptr -4
argc= dword ptr  8
argv= dword ptr  0Ch
envp= dword ptr  10h

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, aInsertPassword ; "Insert 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
mov     ecx, [ebp+var_8]
mov     [esp], ecx
mov     [ebp+var_18], eax
call    check_password
xor     eax, eax
add     esp, 28h
pop     ebp
retn
main endp
```

Second Step

- At the check_password function it basically compares the password in branching with condition if it is correct or incorrect.

- If the input matches with **539h** (which is a hexadecimal value) then it prints correct (clue is found from the comment **“correct! \n”**)

- If it does not match with 539h then it should print incorrect and goes through function jnz **loc_80491A9** which is the case if wrong password is given.



Password

Converting the hexadecimal number 539h to decimal we get 1337 thus, **1337** is the password.

Topic	**Time**
Lab01	5 hours
Report writing	2 hours

Note:

Turning the labranet VPN on and work on VLE may not work sometimes under local network or Wi-Fi even if the VPN perfectly works.