Codeengn Challenges Advance RCE LEVEL2 풀이

Reverse2 L02 Start

Author : Noble

Korea :

정답은 무엇인가

English :

Find the answer

Down

PEID로 확인 한 결과 VC++ 6.0에서 만들어진 프로그램인 걸 알 수 있었다.

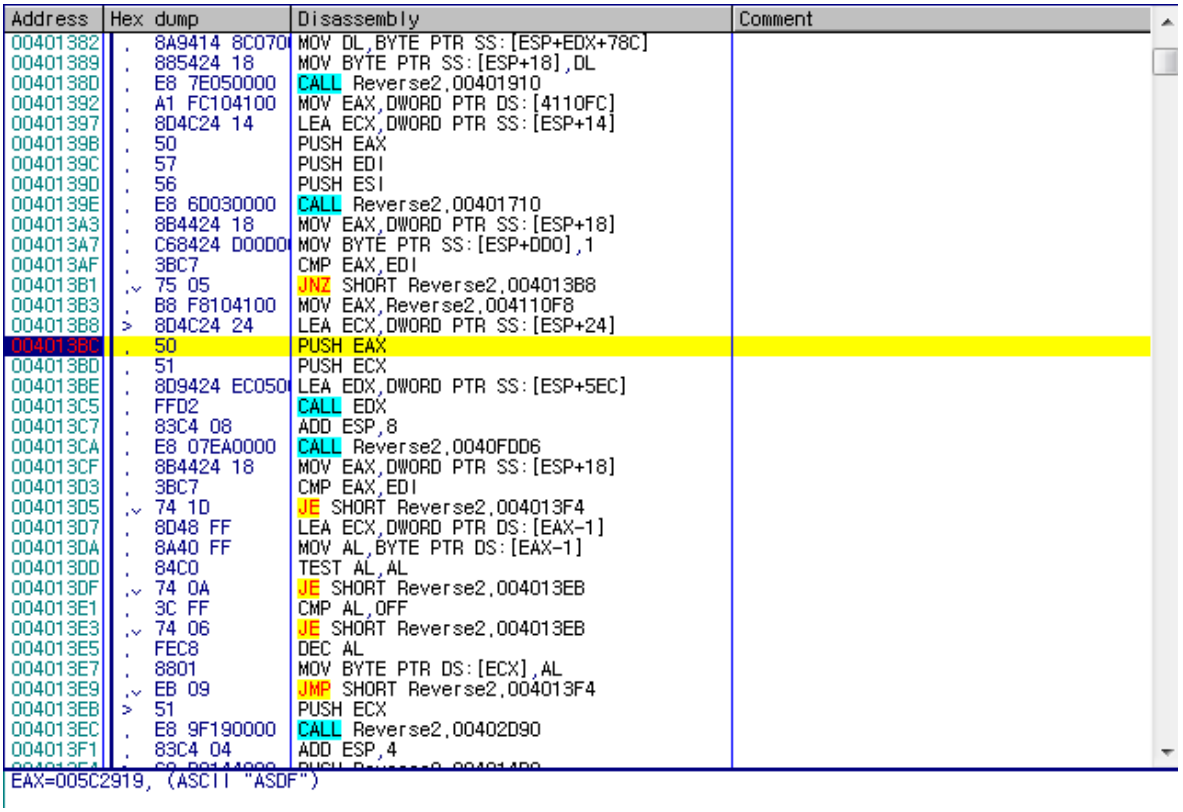
실행을 시켜보니 입력한 키값이 제대로 된 키값이 아니면 꺼지는 프로그램 인 것 같았다.

분석을 위해 올리로 켜보았다.

그리고 Enter Password : 라는 스트링을 찾고, 그 근처에 BP를 걸고 프로그램을 분석해 보았다.

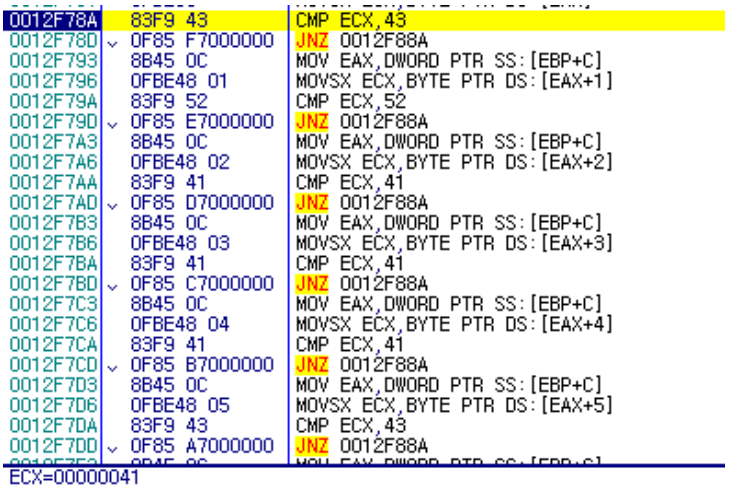
```
004012B3   .  66:AB         STOS WORD PTR ES:[EDI]
004012B5   .  68 30424100   PUSH Reverse2.00414230          ASCII "Enter Password: "
004012BA   .  68 40844100   PUSH Reverse2.00418440
004012BF   .  AA            STOS BYTE PTR ES:[EDI]
004012C0   .  E8 BB0A0000  CALL Reverse2.00401D80
004012C5   .  8D8C24 F8030( LEA ECX,DWORD PTR SS:[ESP+3F8]
004012CC   .  51            PUSH ECX
004012CD   .  68 D0844100   PUSH Reverse2.004184D0
004012D2   .  E8 390D0000   CALL Reverse2.00402010
004012D7   .  83C4 10       ADD ESP,10
004012DA   .  8D9424 88070( LEA EDX,DWORD PTR SS:[ESP+788]
004012E1   .  68 D0144000   PUSH Reverse2.004014D0
004012E6   .  68 40144000   PUSH Reverse2.00401440
004012EB   .  6A 64         PUSH 64
004012ED   .  6A 10         PUSH 10
004012EF   .  52            PUSH EDX
004012F0   .  E8 B0460000   CALL Reverse2.004059A5
004012F5   .  C78424 D00D0( MOV DWORD PTR SS:[ESP+DD0],0
00401300   .  8D9C24 8C070( LEA EBX,DWORD PTR SS:[ESP+78C]
00401307   .  C74424 10 64( MOV DWORD PTR SS:[ESP+10],64
```

입력받은 후 Step Over로 계속 분석을 해나갔다.



그리고 내가 입력한 값을 PUSH하고 함수를 CALL하는 것을 볼 수가 있었었다.

그래서 그 함수를 분석해 보았다.



함수에서 내가 입력한 값과 위의 ASCII값들과 비교해 주는걸 볼 수 있었었다.

저기에 있는 ASCII code들을 문자형태로 변환후 인증하니까 그것이 답이었다! :D