Easy_Crack_Me 문제 write-up

강승민

프로그램을 실행시키니 그림과 같은 메시지 박스가 뜨는데 입력란에 들어갈 문구를 찾는게 목표인 것 같다.

IDA를 이용해 바이너리를 열어보니

```
int __stdcall WinMain(HINSTANCE hInstance, HINSTANCE hPrevInstance, LPSTR lpCmdLine, int nShowCmd)
{
  DialogBoxParamA(hInstance, (LPCSTR)0x65, 0, DialogFunc, 0);
  return 0;
}
```

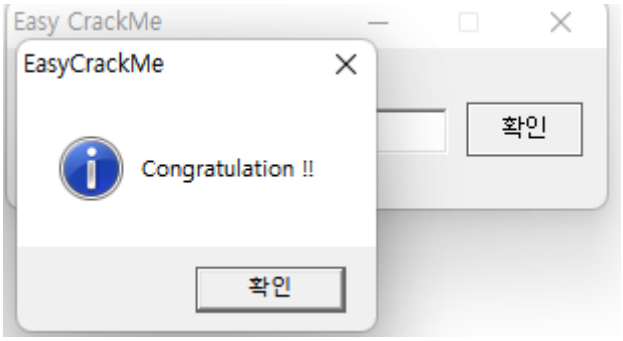
이러한 메시지 박스를 여는 함수가 사용되어 있고 DialogFunc 함수에 들어가보면

```
1  INT_PTR __stdcall DialogFunc(HWND hDlg, UINT a2, WPARAM a3, LPARAM a4)
2  {
3    if ( a2 != 273 )
4      return 0;
5    if ( (unsigned __int16)a3 == 2 )
6    {
7      EndDialog(hDlg, 2);
8      return 1;
9    }
10   else if ( (unsigned __int16)a3 == 1001 )
11   {
12     sub_401080(hDlg);
13     return 1;
14   }
15   else
16   {
17     return 0;
18   }
19 }
```

이렇게 어떤 함수가 실행 되는 것을 볼 수 있다. 이 함수에 들어가보면

```
1  int __cdecl sub_401080(HWND hDlg)
2  {
3    CHAR String[97]; // [esp+4h] [ebp-64h] BYREF
4    __int16 v3; // [esp+65h] [ebp-3h]
5    char v4; // [esp+67h] [ebp-1h]
6
7    memset(String, 0, sizeof(String));
8    v3 = 0;
9    v4 = 0;
10   GetDlgItemTextA(hDlg, 1000, String, 100);
11   if ( String[1] != 97 || strncmp(&String[2], Str2, 2u) || strcmp(&String[4], aR3versing) || String[0] != 69 )
12     return MessageBoxA(hDlg, aIncorrectPassw, Caption, 0x10u);
13   MessageBoxA(hDlg, Text, Caption, 0x40u);
14   return EndDialog(hDlg, 0);
15 }
```

이렇게 입력 문자열과 비교하는 문구가 있고 이를 해석하면 0번째는 E(69를 아스키 값으로), 1번째는 a(97을 아스키 값으로) 그 뒤는 스트링을 비교해서 문구를 출력하고 이를 연결해서 문자열을 만들어 입력해보면



이렇게 Congratulation!! 이라고 뜨며 알맞은 것을 알 수 있다.