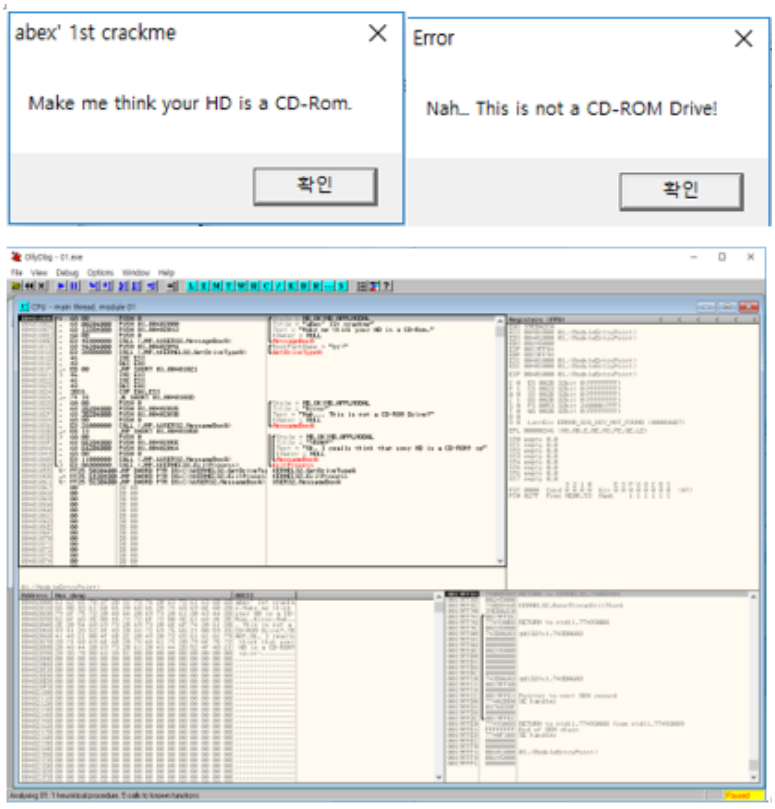
Basic RCE L01

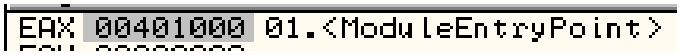
HDD를 CD-Rom으로 인식시키기 위해서는 GetDriveTypeA의 리턴값이 무엇이 되어야 하는가

- Author: abexFile
- Password: codeengn

> https://s3-us-west-2.amazonaws.com/secure.notion-static.com/e7afd1d7-1512-4df4-a552-139755f289d4/01.7z



01.exe를 실행하면 Error메시지 / ollydbg로 실행



packing되지 않은 실행파일은 EntryPoint의 주소가 EAX에 있다.

ctrl + g 로 00401000주소인 EntryPoint(main 함수)로 이동

```
00401000  $ 6A 00          PUSH 0                                  Style = MB_OK|MB_APPLMODAL
00401002  . 68 00204000    PUSH 01.00402000                        Title = "abex' 1st crackme"
00401007  . 68 12204000    PUSH 01.00402012                        Text = "Make me think your HD is a CD
0040100C  . 6A 00          PUSH 0                                  hOwner = NULL
0040100E  . E8 4E000000    CALL <JMP.&USER32.MessageBoxA>          MessageBoxA
00401013  . 68 94204000    PUSH 01.00402094                        RootPathName = "c:\"
00401018  . E8 38000000    CALL <JMP.&KERNEL32.GetDriveTypeA>      GetDriveTypeA
0040101D  . 46             INC ESI
0040101E  . 48             DEC EAX
0040101F  .vEB 00          JMP SHORT 01.00401021
00401021  > 46             INC ESI
00401022  . 46             INC ESI
00401023  . 48             DEC EAX
00401024  . 3BC6           CMP EAX,ESI
00401026  .v74 15          JE SHORT 01.0040103D
00401028  . 6A 00          PUSH 0                                  Style = MB_OK|MB_APPLMODAL
0040102A  . 68 35204000    PUSH 01.00402035                        Title = "Error"
0040102F  . 68 3B204000    PUSH 01.0040203B                        Text = "Nah... This is not a CD-ROM D
00401034  . 6A 00          PUSH 0                                  hOwner = NULL
00401036  . E8 26000000    CALL <JMP.&USER32.MessageBoxA>          MessageBoxA
0040103B  .vEB 13          JMP SHORT 01.00401050
0040103D  > 6A 00          PUSH 0                                  Style = MB_OK|MB_APPLMODAL
0040103F  . 68 5E204000    PUSH 01.0040205E                        Title = "YEAH!"
00401044  . 68 64204000    PUSH 01.00402064                        Text = "Ok, I really think that your
00401049  . 6A 00          PUSH 0                                  hOwner = NULL
0040104B  . E8 11000000    CALL <JMP.&USER32.MessageBoxA>          MessageBoxA
00401050  L> E8 06000000    CALL <JMP.&KERNEL32.ExitProcess>        ExitProcess
```

HDD가 CD-Rom으로 인식 되려면 00401044주소에 보이는 ok, I really think~메시지가 떠야한다.

이 때에 GetDriveTypeA의 리턴값을 묻는 문제니까 일단 GetDriveTypeA까지 실행시켜서 call뒤에 있는 함수의 리턴값을 보자

```
EAX 00000003
```

EAX는 리턴값이 들어가는 레지스터

f2로 GetDriveTypeA뒤 주소에 breakpoint 찍고 f9로 실행

GetDriveTypeA의 리턴값이 3인것을 알았다.

```
EAX 00000001
ECX 005E0000
EDX 005E0000
EBX 002F7000
ESP 0019FF84
EBP 0019FF94
ESI 00000003
```

f8로 EAX와 ESI를 비교하기 전까지 명령어를 쭉 따라가 보면 최종적으로 EAX가 1, ESI 3인 것을 알 수 있다.

```
00401024  .  3BC6          CMP EAX,ESI
00401026  .v 74 15         JE SHORT 01.0040103D
```

EAX의 값과 ESI의 값이 같으면 0040103D로 분기

cmp명령어는 두 개를 뺀 값이 0이면 zeroflag(ZF)에 1 넣는다. default ZF는 0

지금 코드로는 여기서 EAX와 ESI 레지스터의 값이 다르기때문에 ZF가 0이고 따라서 JE명령어가 거짓으로 ok가 있는 0040103D로 분기하지 않는다.

그러면 CMP명령어 실행 때 EAX값이 ESI와 같은 3이 되게 하면 ok가 나올 것이다.

그러려면 GetDriveTypeA의 리턴값인 3에서 CMP명령어에서의 EAX값인 1까지 2가 줄었으므로 GetDriveTypeA의 리턴값을 5로 만들어주면 CMP명령어까지 오면서 2가 줄어 EAX값이 3으로 ESI값과 같아질 것이다.

리턴후의 EAX 값을 5로 바꿈.

f9를 사용하여 실행하면 okay사인이 나온다.