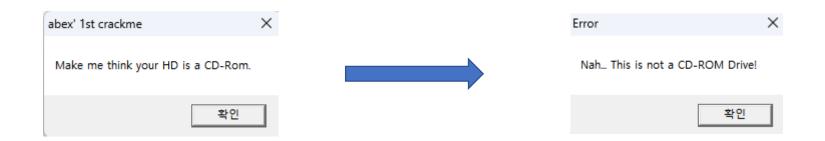
abex' crackme #1



crackme 프로그램은 말 그대로 크랙 연습 목적으로 작성되어 공개된 프로그램 디버거를 실행하기 전에 파일을 실행

```
00401000 ┌$
                                                                         PUSH 0
                                    6A 00
                                                                                                                                                                                                                 MB_OKIMB_APPLMODAL
                                                                         PUSH abexcm1-.00402000
 00401002
                                     68 00204000
                                                                                                                                                                                            Title = "abex' 1st crackme"
 00401007
                                    68 12204000
                                                                         PUSH abexcm1-.00402012
                                                                                                                                                                                            Text = "Make me think your HD is a CD-Rom."
 0040100C
                                     64
                                            00
                                                                         PUSH 0
                                                                                                                                                                                           hOwner = NULL
                                            4E000000
 0040100E
                                                                         CALL
                                                                                      <JMP. &USER32. MessageBoxA>
                                                                                                                                                                                         LMessageBoxA
 00401013
                                             94204000
                                                                         PUSH abexcm1-.00402094
                                                                                                                                                                                         rRootPathName = "c:\"
 00401018
                                     E8
                                                                         CALL  
                                             38000000
                                                                                                                                                                                         └GetDriveTypeA
                                                                        INC ESI
DEC EAX
JMP SHORT abexcm1-.00401021
 0040101D
                                     46
 0040101E
                                     48
0040101F
00401021
00401022
                                     ÉB 00
46
                                                                         INC ESI
                                     46
                                    48
3BC6
 00401023
                                                                         DEC EAX
                                                                         CMP EAX, ESI
 00401024
 00401026
                                    74 15
                                                                         JE SHORT abexcm1-.0040103D
 00401028
                                    6A 00
                                                                         PUSH 0
                                                                                                                                                                                         _Style = MB_OKIMB_APPLMODAL
                                                                                                                                                                                           Iitle = "Error"
 0040102A
                                            35204000
                                                                         PUSH abexcm1-.00402035
 0040102F
                                            3B204000
                                                                         PUSH abexcm1-.0040203B
                                    68
                                                                                                                                                                                            Text = "Nah... This is not a CD-ROM Drive!"
 00401034
                                    64
                                             00
                                                                         PUSH 0
                                                                                                                                                                                           hOwner = NULL
 00401036
                                            26000000
                                                                         -MessageBoxA
                                    EB 13
6A 00
0040103B
0040103D
                                                                         JMP SHORT abexcm1-.00401050
                                                                                                                                                                                           rStyle = MB_OKIMB_APPLMODAL
                                                                         PUSH 0
 0040103F
                                     68 5E204000
                                                                         PUSH abexcm1-.0040205E
                                                                                                                                                                                              Title = "YEAH!"
 00401044
                                    68 64204000
                                                                         PUSH abexcm1-.00402064
                                                                                                                                                                                                Text = "Ok. I really think that your HD is a CD-ROM! :p"
                                                                         PUSH 0
 00401049
                                    64
                                            00
                                                                                                                                                                                              hOwner = NULL
 0040104B
                                    E8 11000000
                                                                         CALL  CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 CALL 
 C
                                                                                                                                                                                            LMessageBoxA
 00401050 ->
                                     E8 06000000
                                                                         CALL  CALL   CALL                                                                                                                                                                                                                                                                                                                                                <pr
                                                                                                                                                                                         LExitProcess
```

Kangnam University

```
MessageBoxA("Make me think your HD is a CD-ROM.", "abex\' 1st crackme")
GetDriveTypeA("C:\\")
...
MessageBoxA("Nah... This is not a CD-ROM Drive!", "Error")
MessageBoxA("OK, I really think that your HD is a CD-ROM!:p", "YEAH!")
```

GetDriveType() API로 C 드라이브의 타입을 얻어오는데(대부분 HDD 타입이리턴) 이걸 조작하여 CD-ROM 타입으로 인식하도록 만들어 "OK, I really think that your HD is a CD-ROM! :p" 메시지 박스가 출력되도록 하는 것

GetDriveTypeA() 호출

Regi	isters		U)
EAX	000000	903	
ECX	004C00	000	
EDX	004C00	900	
EBX	002FD0	000	
ESP	0019FF	78	
EBP	0019FF	84	
ESI	004010	000	abexcm1
EDI	004010	000	abexcm1

리턴 값(EAX)은 3(DRIVE_FIXED)

DRIVE_FIXED

The drive has fixed media; for example, a hard disk drive or flash

drive.

- 40101F은 의미 없는 JMP 명령 (garbage code) Garbage code는 디버깅을 방해하고 리버서를 혼란시키기 위해 고의적으로 추가된 것
- 401024에서EAX(1)와 ESI(2)비교 401026-JE(Jump if Equal) 조건 분기 명령, 두 값이 같으면 40103D로 점프하고, 다르면 밑(401028)으로 진행. 40103D 주소는 제작자가 원하는 메시지 박스 출력 코드

```
6A 00
68 35204000
00401028
                                PUSH 0
                                                                                   FStyle = MB_OKIMB_APPLMODAL
                                PUSH abexcm1-.00402035
PUSH abexcm1-.0040203B
PUSH 0
0040102A
                                                                                     Title = "Error"
                   3B204000
0040102F
                                                                                     Text = "Nah... This is not a CD-ROM Drive!"
                6Ā
00401034
                    00
                                                                                     hOwner = NULL
                                CALL JMP.&USER32.MessageBoxA>
JMP SHORT abexcm1-.00401050
                   26000000
00401036
                                                                                   -MessageBoxA
                ĒΒ
0040103B
                    13
                6A
                                PUSH 0
0040103D
                    00
                                                                                     -Style = MB_OKIMB_APPLMODAL
                                PUSH abexcm1-.0040205E
PUSH abexcm1-.00402064
PUSH 0
                68 5E204000
                                                                                      Title = "YEAH!"
0040103F
                                                                                      Text = "Ok, I really think that your HD is a CD-ROM! :p" hOwner = NULL
                68 64204000
00401044
                6Ā
                   00
00401049
                E8 11000000
E8 06000000
                                       <JMP.&USER32.MessageBoxA>
                                                                                    <u>L</u>MessageBoxA
0040104B
                                CALL
                                       <JMP. &KERNEL32.ExitProcess>
00401050
                                                                                    LExitProcess
```

Kangnam University

패치

```
EB 15
6A 00
00401026
                                  JMP SHORT abexcm1-.0040103D
                                                                                      Style = MB_OKIMB_APPLMODAL
Title = "Error"
00401028
                                  PUSH 0
                                 PUSH abexcm1-.00402035
PUSH abexcm1-.0040203B
                68 35204000
0040102A
0040102F
                 68 3B204000
                                                                                        Text = "Nah... This is not a CD-ROM Drive!"
                6A 00
E8 26000000
                                                                                      hOwner = NULL
-MessageBoxA
00401034
                                  PUSH 0
                                 CALL (JMP.&USER32.MessageBoxA)
JMP SHORT abexcm1-.00401050
00401036
                ĒB 13
•6A 00
0040103B
                                                                                        -Style = MB_OKIMB_APPLMODAL
Title = "YEAH!"
0040103D
                                  PUSH 0
                 68 5E204000
0040103F
                                  PUSH abexcm1-.0040205E
                                                                                       Text = "Ok, I really think that your HD is a CD-ROM! :p" hOwner = NULL

MessageBoxA
00401044
                 68 64204000
                                  PUSH abexcm1-.00402064
                6A 00
E8 11000000
00401049
                                  PUSH 0
                                 CALL (JMP.&USER32.MessageBoxA)
0040104B
```

조건 분기(JE) 명령어를 점프 명령어로 바꾼다

00401026 V 75 15 JNZ SHORT abexcm1-.0040103D

조건 분기 명령어 JNE(jump if it's not equal) 사용

스택에 파라미터를 전달하는 방법

```
PUSH 0
00401000|-$
             6A 00
             68 00204000
                                                                              abex' 1st crackme"
00401002
                          PUSH abexcm1-.00402000
                                                                            "Make me think your HD is a CD-Rom."
             68 12204000
00401007
                          PUSH abexcm1-.00402012
                          PUSH 0
0040100C
             6A 00
                          CALL (JMP.&USER32.MessageBoxA)
0040100E
```

401000~40100E 주소 사이의 명령어를 보면 MessageBoxA() 함수를 호출하기 전 4번의 PUSH 명령어를 사용하여 필요한 파라미터를 역순으로 입력

위 어셈블리 코드를 C 언어로 번역하면

MessageBox(NULL, "Make me think your HD is a CD-Rom.", "abex' 1st crackme", MB OK|MB APPLMODAL);

```
        0019FF68
        00000000
        hOwner = NULL

        0019FF6C
        00402012
        Text = "Make me think your HD is a CD-Rom."

        0019FF70
        00402000
        Title = "abex' 1st crackme"

        0019FF74
        00000000
        Style = MB_OKIMB_APPLMODAL
```

C언어 소스코드에서 함수에 넘기는 파라미터의 순서가 어셈블리 언어에서는 역순으로 넘어감 스택은 FILO(First In Last Out) 구조이기에 역순으로 넣어두면 받는 쪽에서 올바른 순서로 꺼냄

Thank you