Crack me 문제 보고서

|  |  |
| --- | --- |
| 문제명 | Abex Crackme 01 |
| 파일명 | abexcm1.exe |
| 풀이자 | 서치원(2011003155) |
| 풀이 기간 | 2016/12/26 ~ 2017/01/01 |
| 문제 내용 | HD rom을 CD rom으로 인식하게 하라 |

문제 풀이:

문제 파일을 실행 시 창 하나가 뜨게됩니다.

￼￼

HD를 CD-Rom으로 인식하게 하라는 메세지가 나오고 확인을 누르면 실패 결과가 뜨게 됩니다.



Ollydbg로 실행한 화면입니다. 실제 코드를 보면 메세지 창이 2개 존재하는데 띄워지는 조건을 변경해 다른 메세지를 띄우는 문제임을 알 수 있습니다.

40101D 실행문 지점에서 GetDriveTypeA 메소드를 실행 후에 EAX register는 3의 값이 들어가있고 ESI register에는 0의 값이 들어가 있습니다. 그 후, INC,DEC 명령으로 EAX, ESI의 값을 변경하는데 ESI는 INC를 3번 실행해 3으로 EAX는 DEC를 2번 실행해 1로 변경됩니다. 그 후, 두 값을 비교해 같으면 정답 Message 로 넘어가고 다르다면 실패 메세지를 띄우게 됩니다.

즉, 401024의 실행 시점에서 EAX, ESI만 같으면 됩니다. 조정하는 방법은 EAX, ESI 값의 변경, 강제 점프 등이 있습니다.



변경해 정답 Message 창을 띄운 모습입니다.