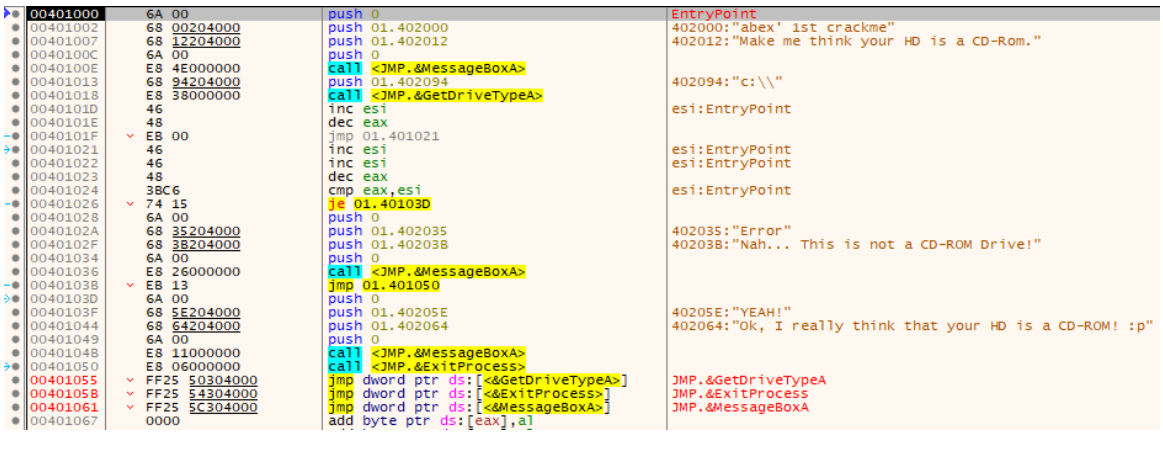
[Code_Engn] Basic RCE L01

생성일	@2022년 11월 29일 오전 11:21
태그	Rev

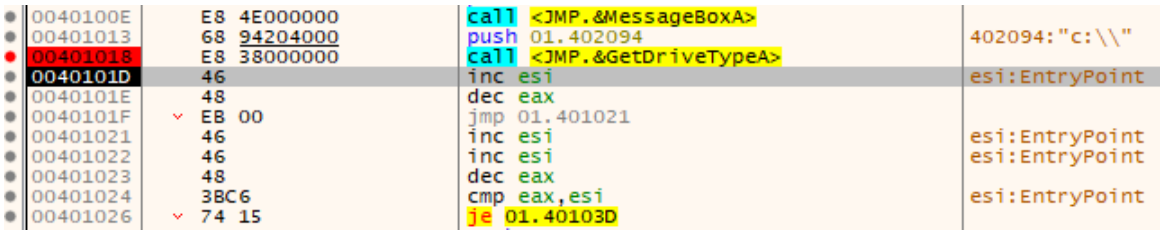
Basic RCE L01

HDD를 CD-Rom으로 인식시키기 위해서는 GetDriveTypeA의 리턴값이 무엇이 되어야 하는가

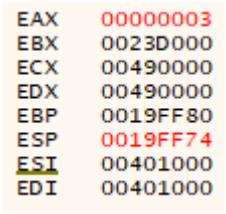
— Author: abex
— File Password: codeengn



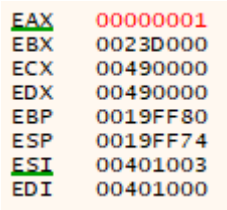
GetDriveTypeA에 브레이크 포인트를 걸고 실행시켜보았다.



끝나고 레지스터를 보면 EAX에는 3이 들어있고, ESI에는 0이 들어있는걸 볼 수 있다.



그리고 cmp구문전 까지 실행시키면 레지스터안에 값들이 아래 처럼 변해있다.



EAX : 3 → 1 | ESI : 0 → 3

이 두값이 같아야 CDROM으로 인식하니 GetDriveTypeA의 리턴값은 5가 되어야 한다.