BASIC RCE Level 1

CodeEngn
ReverseEngineering Conference

2013 07/09
Malcook90@naver.com

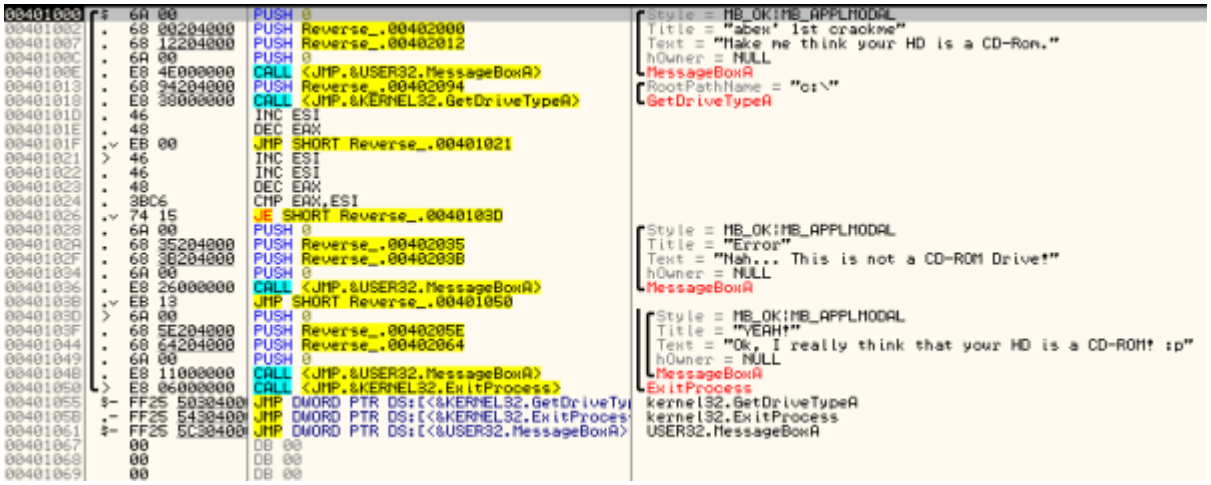
Challenges : Basic 01

Author : abex

Korea :
HDD를 CD-Rom으로 인식시키기 위해서는 GetDriveTypeA의 리턴값이 무엇이 되어야 하는가

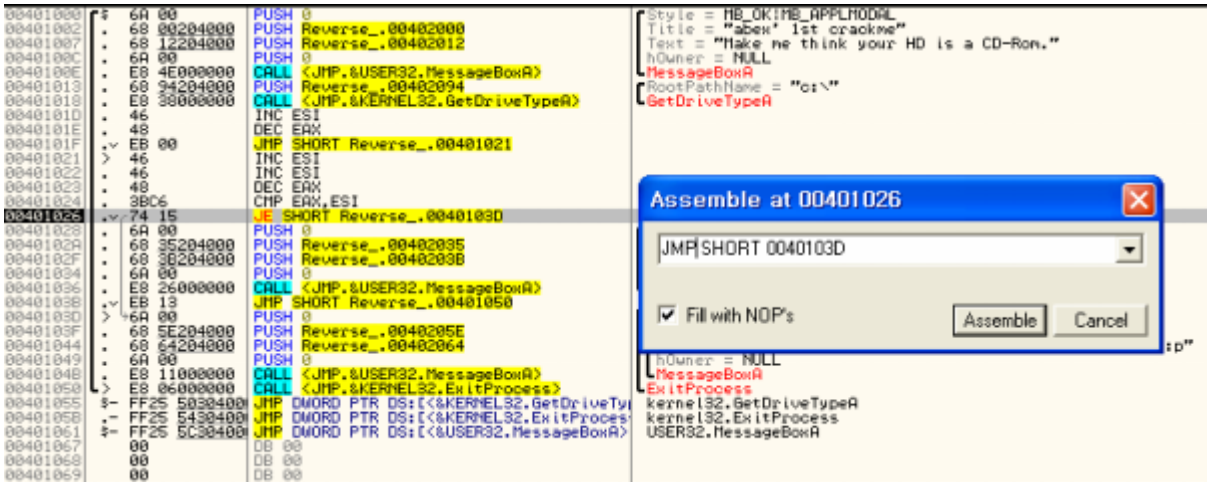
English :
What value must GetDriveTypeA return in order to make the computer recognize the HDD as a CD-Rom

기존 abex' crackme 1 과 동일한 파일이군요.. 한번 OllyDbg로 열어 봅시다.

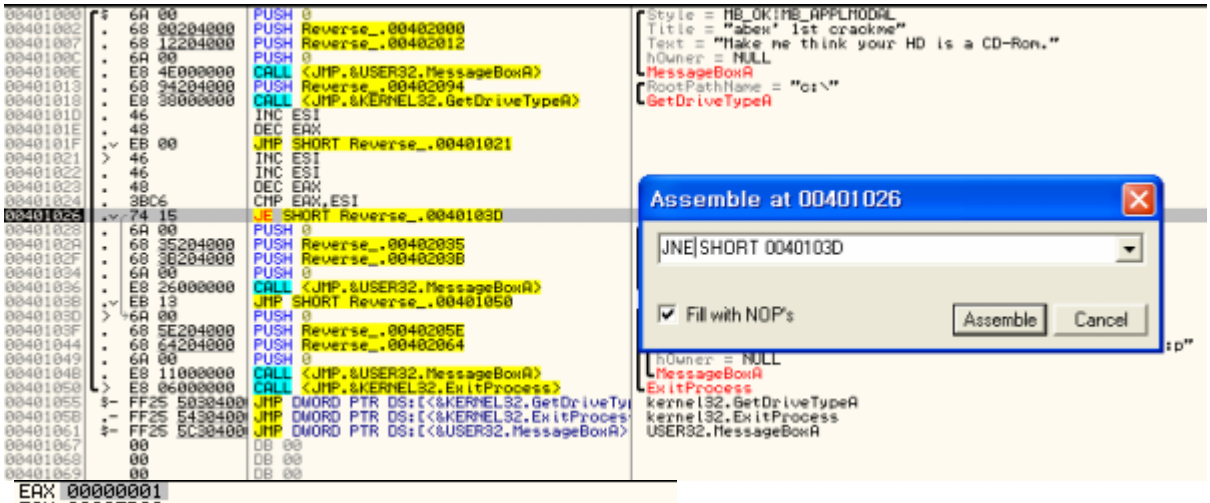


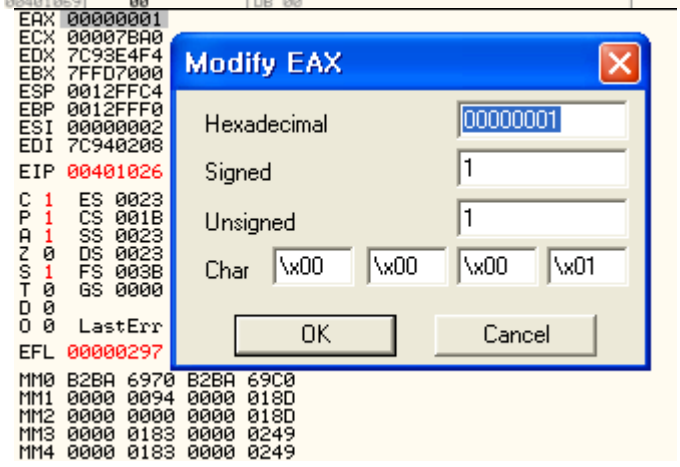
어셈블리어 코드가 딱! 한눈에 들어오니 좋네요(?) ^^;

여기서 F8로 하나하나 실행하면서 넘어가 봅니다.



위와 같이 JE -> JMP 로 바꾸어져서, 조건과 상관없이 점프 하는 것이 일반적





JNE(Jump Not Equal) 즉, Zero Flag가 0 일때 실행하는 명령어 입니다.

또한 EAX의 값을 임의로 변경하여 ESI와도 맞쳐줄수 있습니다.

하지만 본 문제에서는 GetDriveTypeA 의 리턴값을 알아야 합니다.

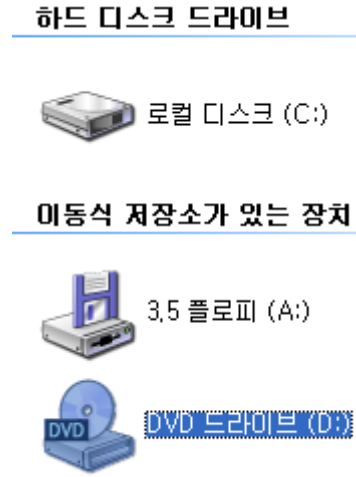
이를 위해, MSDN을 참조해봅시다.

http://msdn.microsoft.com/en-us/library/aa364939%28VS.85%29.aspx

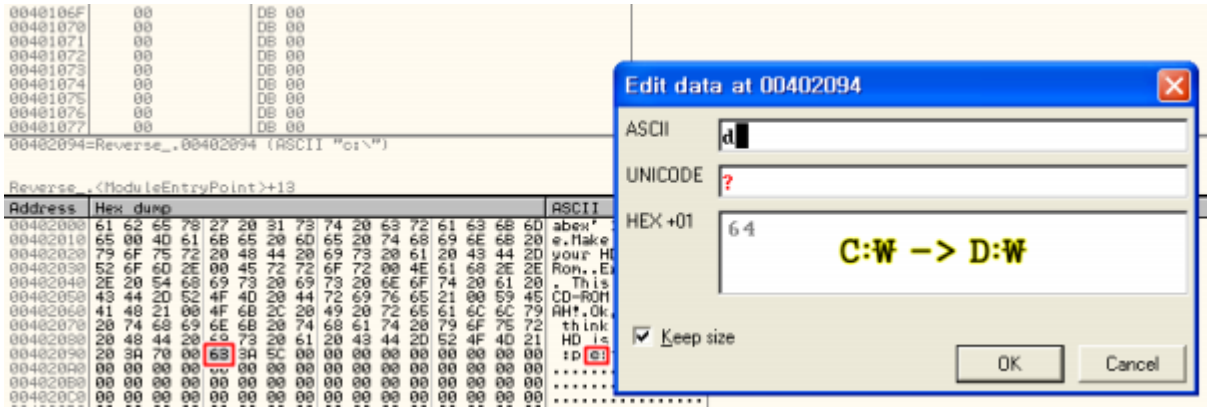
Return code/value	Description
DRIVE_UNKNOWN 0	The drive type cannot be determined.
DRIVE_NO_ROOT_DIR 1	The root path is invalid; for example, there is no volume mounted at the specified path.
DRIVE_REMOVABLE 2	The drive has removable media; for example, a floppy drive, thumb drive, or flash card reader.
DRIVE_FIXED 3	The drive has fixed media; for example, a hard disk drive or flash drive.
DRIVE_REMOTE 4	The drive is a remote (network) drive.
DRIVE_CDROM 5	The drive is a CD-ROM drive.
DRIVE_RAMDISK 6	The drive is a RAM disk.

리턴값 들이 상세히 나와있습니다.

이 표을 보고 다시 수정해보겠습니다.



지금 저의 CD-Rom 은 'D:' 입니다. 이걸 가지고 수정해 보겠습니다.



Dump Window 에서 C:₩(63) -> D:₩(64) 로 변경

GetDriveTypeA 을 참조시 EAX값이 5가 되는 것을 확인할 수 있습니다.

참고로 C:₩ 일때는 EAX값이 3이 됩니다.