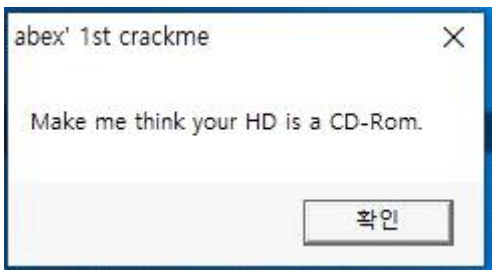
[CodeEngn Challenges Basic RCE L01 - abex crackme 1]

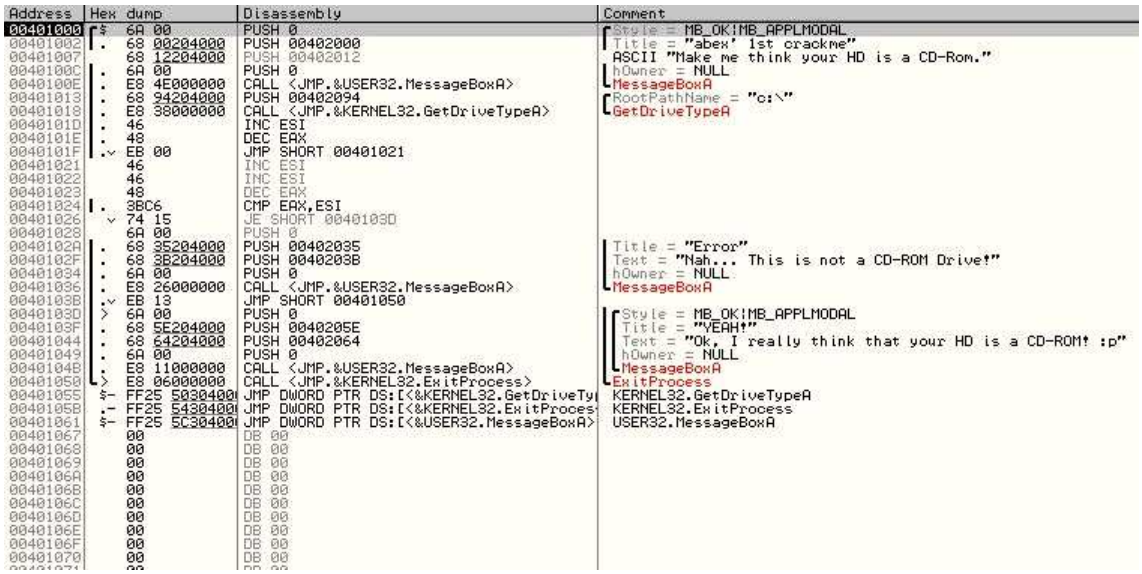
문제 내용: HDD를 CD-Rom으로 인식시키기 위해서는 GetDriveTypeA의 리턴값이 무엇이 되어야 하는가?

먼저 코드엔진 사이트에서 파일을 내려 받아 실행해봅니다.



실행하게 되면 Make me think your HD is a CD-Rom. 이라고 메세지 박스가 나옵니다. 해당 내용을 해석 해보면 너의 하드를 CD롬으로 인식하게 만들어라 라는 내용인 듯 합니다. [확인]을 눌러보니 Error창으로 해당 드라이브는 CD 롬이 아니라고 나옵니다.

자 이제 내부 소스를 확인해봅시다.



일단 보기에도 소스 내용이 적어보입니다. 해당 내용만 보았을 때 어셈블리어로만 작성 된다는 걸 추측할 수 있습니다. 그 이유는 C로 작성하였을 경우 Stub code가 추가 되어 복잡해져야 하는데 깔끔하게 직관적인 코드를 확인 할 수 있고, EP(Entry Point)에 main함수가 바로 나타난 걸로 어셈블리어로 작성 했다는 걸 알 수 있습니다.
소스를 간단히 살펴보면 아까 봤던 Make me think your HD is a CD-Rom 문구와 확인을 눌렀을 때 나온 에러메세지 박스 문구가 보입니다. 그 밑에 바로 CD-Rom으로 인식 시켰을 경우의 문구도 있습니다.

우리는 에러메세지 박스가 아닌 그 밑에 있는 박스 메세지가 나와야합니다.

소스를 한번 그냥 쭉 실행 해보면 그냥 프로그램을 따로 실행 했던 것과 같은 결과가 나오게 됩니다. 그 생각을 가지고 소스를 보면 CD롬 인식이 되었다는 메세지 박스의 코드가 실행이 되지 않고 끝난다는건데 여기서 문제를 풀 수 있는 방법이 여러가지로 나뉘게 됩니다.
1. 어셈블리어 소스 자체는 건들지 않고 값(Data)를 패치해서 성공시킨다.
2. 어셈블리어 코드 변경으로 진행한다.

크게 2가지로 볼 수 있고 더 좋은 방법들도 있을 것 같습니다.
우선 1번 방법으로 진행해보겠습니다.

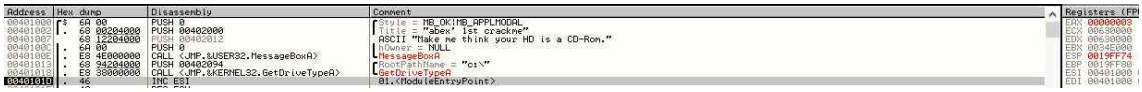
해당 소스에서 중요한 부분은 GetDriveTypeA 부분입니다. 해당 부분의 리턴값이 무엇이 되어야 하는지를 묻는 문제입니다. 구글에 GetDriveTypeA 가 뭔지 검색해봅시다.

Return Value

The return value specifies the type of drive, which can be one of the following values.

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.

검색을 해보니 CDROM 값은 5라고 나와 있습니다. 자 이제 본격적으로 소스를 분석해보겠습니다.
코드를 한 줄 한 줄 실행(빠른 확인을 위해 F8)하다 보면 GetDriveTypeA 함수를 지나칠 때 EAX값이 3으로 리턴 된다는 걸 확인 할 수 있습니다.



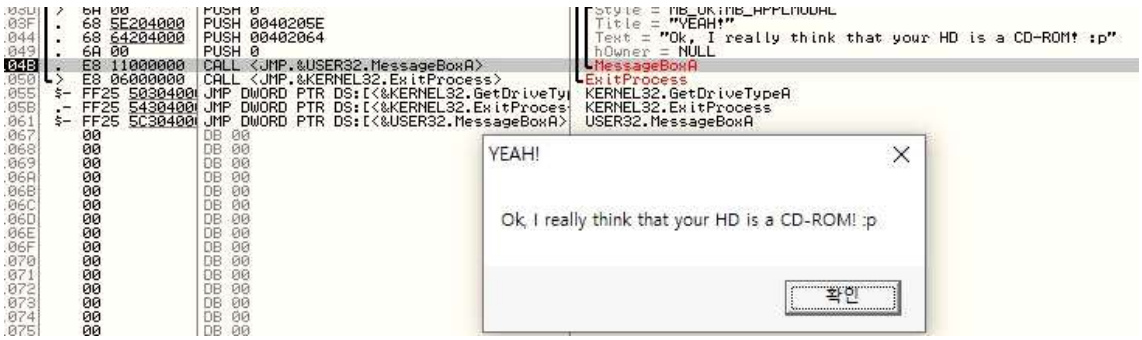
3이면 위에 GetDriveTypeA 구글 검색을 통해 확인한 이미지를 보면 DRIVE_FIXED 3 하드 디스크입니다.
저희가 리턴 받아야 하는 건 CDROM으로 값이 5가 나와야 할 텐데 말이죠 저희는 이 리턴값을 패치 해야 합니다.

이후 코드들을 유심히 봐주세요

```
INC ESI // ESI를 1증가 시켜라.
DEC EAX // EAX를 1감소 시켜라.
JMP SHORT 00401021 // 401021이 바로 밑에 있는 INC ESI 주소입니다. 즉, 이 코드는 의미 없습니다.
INC ESI // ESI를 1증가 시켜라. 해당 코드 실행 후 ESI값 2
INC ESI // ESI를 1증가 시켜라. 해당 코드 실행 후 ESI값 3
DEC EAX // EAX를 1감소 시켜라. 해당 코드 실행 후 EAX값 1
CMP EAX,ESI // EAX와 ESI를 비교하라. EAX = 1, ESI = 3
JE SHORT 0040103D // JE(Jump Equal) 비교 하는 두 값이 같으면 40103D 주소로 점프하고, 다르면 그
```

EAX와 ESI값이 같아야 저희가 원하는 CD롬 인식 메세지 박스 코드로 갈 수 있습니다.
현재 EAX값이 1이므로 2가 더 증가해야 ESI와 값이 같아질 수 있습니다.
리턴값에서 레지스터 영역에서 직접 3을 5로 변경하고 위 소스를 진행하면
결국 EAX는 5에서 2가 감소되어 3이 되어 점프를 할 수 있게 됩니다.

* 위 코드 JE는 ZF(Zero Flag)가 1이면 점프된다는 의미입니다.
CMP로 비교했을 때 두 값이 동일하다면 SUB결과는 0이고 연산 명령 후 결과 값이 0이면 ZF는 1로 세팅됩니다.

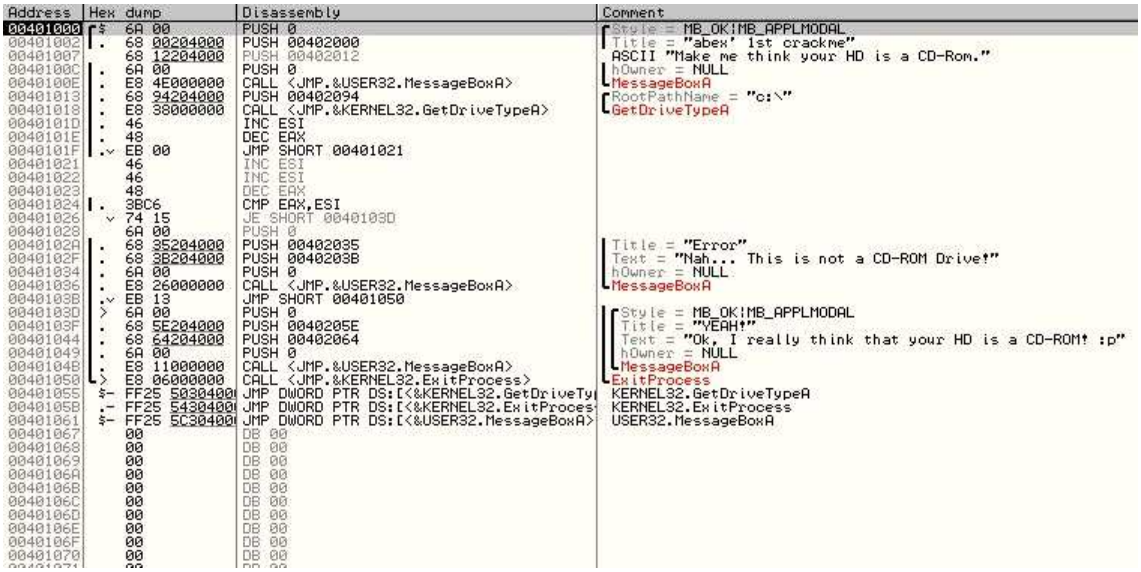


이후 쭉 코드를 실행하면 CD롬에 인식되었다는 메세지 박스를 확인 할 수 있습니다 !
마우스 우클릭 Copy to executable 기능을 통해 패치한 소스 프로그램을 따로 저장하여 실행 할 수 있습니다.

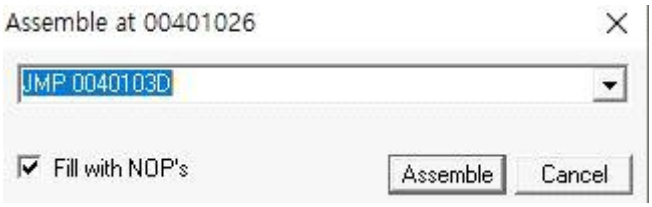
GetDriveTypeA 리턴 값은 5가 정답입니다.

[다른 풀이 방법]

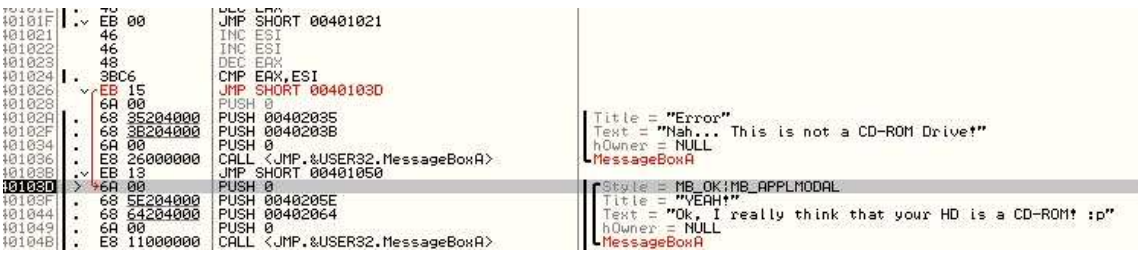
이번에는 더 간단한? 풀이 방법입니다.



프로그램 소스를 다시 보시면 CMP EAX, ESI 비교 후에 JE SHORT 0040103D 로 EAX와 ESI가 같으면 점프가 진행 되도록 되어있습니다. 이 어셈블리어 코드를 직접 수정해서 위 조건 없이 그냥 바로 점프되도록 변경하겠습니다.



Space키를 누르면 어셈블리어 코드를 직접 넣을 수 있는 창이 나옵니다.
여기서 앞에 JE 를 지우고 JMP로 변경해줍니다.



수정 후 코드를 진행하면 바로 원하는 코드로 점프 되시는 걸 확인 할 수 있습니다.

이렇게 다양하게 풀어볼 수 있지만 여기서 중요한 점은 우선 문제 내용은 GetDriveTypeA 함수 리턴 값을 물었기 때문에 정답은 첫 번째로 풀이 한 방법이 정답입니다. 해당 문제 내용이 다르게 나왔을 시 두 번째 방법으로 풀어도 정답이 될 수 있다는 걸 확인과 다양한 풀이를 익히기 위해 두 가지 방법 다 해봤습니다.

write up by arrester 김주원