

BASIC RCE Level 1

Code Engn
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 :

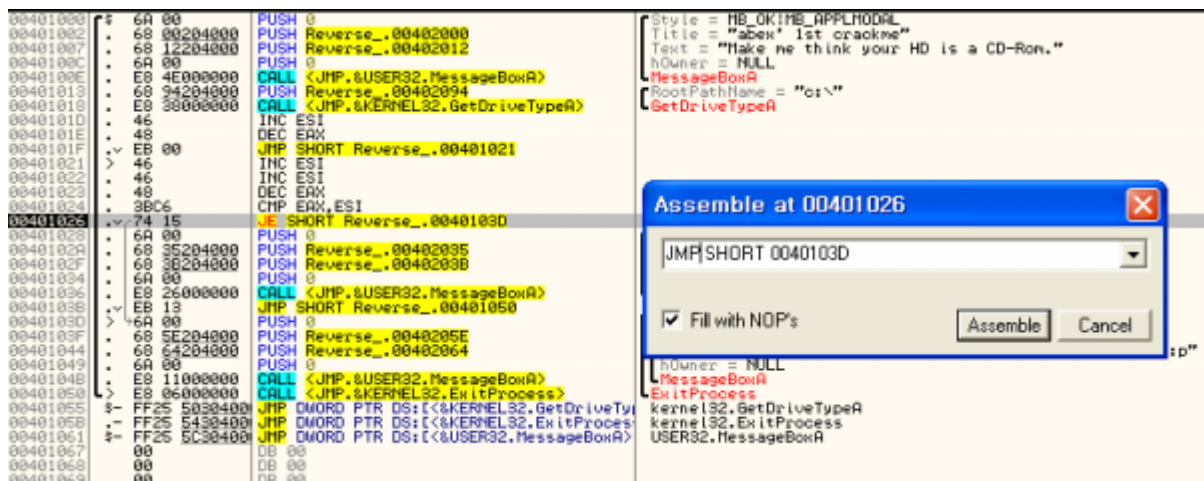
What value must GetDriveTypeA return in order to make the computer recognize the HDD as a CD-Rom

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

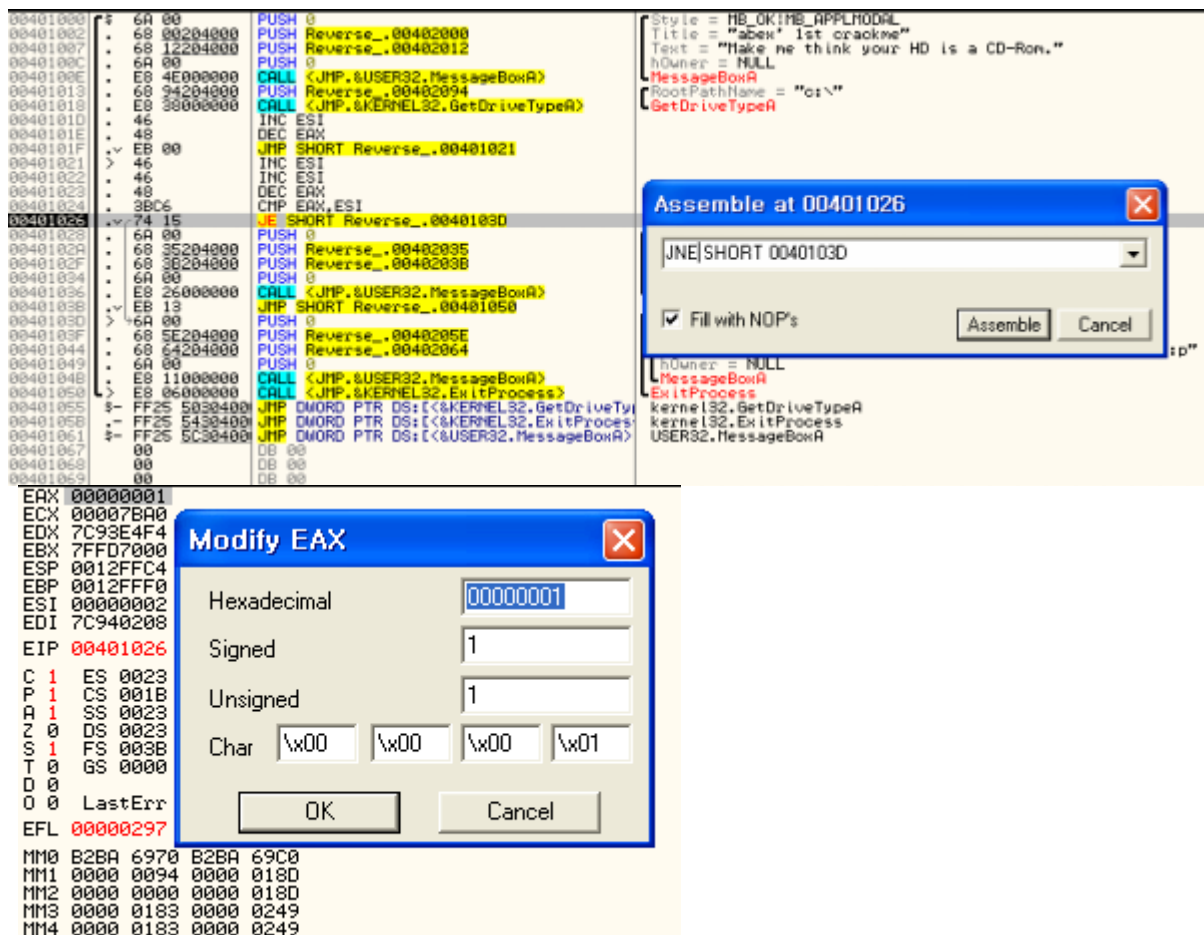
00401000	6A 00	PUSH 0	Style = MB_OK;MB_APPLMODAL
00401002	68 00204000	PUSH Reverse_.00402000	Title = "abex' 1st crackme"
00401007	68 12204000	PUSH Reverse_.00402012	Text = "Make me think your HD is a CD-Rom."
0040100C	6A 00	PUSH 0	hOwner = NULL
0040100E	E8 4E000000	CALL <JMP.&USER32.MessageBoxA>	MessageBoxA
00401013	68 94204000	PUSH Reverse_.00402094	RootPathName = "c:\\"
00401018	E8 38000000	CALL <JMP.&KERNEL32.GetDriveTypeA>	GetDriveTypeA
0040101D	46	INC ESI	
0040101E	48	DEC EAX	
0040101F	EB 00	JMP SHORT Reverse_.00401021	
00401021	46	INC ESI	
00401022	46	INC ESI	
00401023	48	DEC EAX	
00401024	3BC6	CMP EAX,ESI	
00401026	74 15	JE SHORT Reverse_.00401030	
00401028	6A 00	PUSH 0	Style = MB_OK;MB_APPLMODAL
0040102A	68 35204000	PUSH Reverse_.00402035	Title = "Error"
0040102F	68 38204000	PUSH Reverse_.00402038	Text = "Nah... This is not a CD-ROM Drive!"
00401034	6A 00	PUSH 0	hOwner = NULL
00401036	E8 26000000	CALL <JMP.&USER32.MessageBoxA>	MessageBoxA
00401038	EB 13	JMP SHORT Reverse_.00401050	
0040103D	6A 00	PUSH 0	Style = MB_OK;MB_APPLMODAL
0040103F	68 5E204000	PUSH Reverse_.0040205E	Title = "YEAH!"
00401044	68 64204000	PUSH Reverse_.00402064	Text = "Ok, I really think that your HD is a CD-ROM! :p"
00401049	6A 00	PUSH 0	hOwner = NULL
0040104B	E8 11000000	CALL <JMP.&USER32.MessageBoxA>	MessageBoxA
00401050	E8 06000000	CALL <JMP.&KERNEL32.ExitProcess>	ExitProcess
00401055	FF25 50304000	JMP DWORD PTR DS:[&KERNEL32.GetDriveTypeA]	kernel32.GetDriveTypeA
00401058	FF25 54304000	JMP DWORD PTR DS:[&KERNEL32.ExitProcess]	kernel32.ExitProcess
00401061	FF25 5C304000	JMP DWORD PTR DS:[&USER32.MessageBoxA]	USER32.MessageBoxA
00401067	00	DB 00	
00401068	00	DB 00	
00401069	00	DB 00	

어셈블리어 코드가 딱! 한눈에 들어오니 좋네요(?) ^^;

여기서 F8로 하나하나 실행하면서 넘어가 봅니다.



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



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

또한 EAX 의 값을 임의로 변경하여 ESI와도 맞춰줄수 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 표를 보고 다시 수정해보겠습니다.

하드 디스크 드라이브



로컬 디스크 (C:)

이동식 저장소가 있는 장치



3.5 플로피 (A:)



DVD 드라이브 (D:)

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

0040106F 00 DB 00
00401070 00 DB 00
00401071 00 DB 00
00401072 00 DB 00
00401073 00 DB 00
00401074 00 DB 00
00401075 00 DB 00
00401076 00 DB 00
00401077 00 DB 00
00402094=Reverse_.00402094 (ASCII "C:\")
Reverse_.<ModuleEntryPoint>+13
Address Hex dump ASCII
00402090 61 62 65 78 27 20 31 73 74 20 63 72 61 63 68 6D abex'
00402091 65 00 40 61 68 65 20 6D 65 20 74 68 69 6E 68 20 e.Make
00402092 79 6F 75 72 20 48 44 20 69 73 20 61 20 43 44 2D your HD
00402093 52 6F 60 2E 00 45 72 72 6F 72 00 4E 61 68 2E 2E Ron.,E
00402094 2E 20 54 68 69 73 20 69 73 20 6E 6F 74 20 61 20 . This
00402095 43 44 2D 52 4F 4D 20 44 72 69 76 65 21 00 59 45 CD-ROM
00402096 41 48 21 00 4F 68 2C 20 49 20 72 65 61 6C 6C 79 AH!,Ok
00402097 20 74 68 69 6E 68 20 74 68 61 74 20 79 6F 75 72 think
00402098 20 48 44 20 63 73 20 61 20 43 44 2D 52 4F 4D 21 HD is
00402099 20 3A 70 00 63 3A 5C 00 00 00 00 00 00 00 00 00 :p (C)
0040209A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040209B 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040209C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Edit data at 00402094
ASCII d
UNICODE ?
HEX +01 64
C:\W -> D:\W
☒ Keep size
OK Cancel

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

00401080 6A 00 PUSH 0
00401082 68 00204000 PUSH Reverse_.00402000
00401087 68 12204000 PUSH Reverse_.00402012
0040108C 6A 00 PUSH 0
0040108E E8 4E000000 CALL <JMP.>USER32.MessageBoxA
00401013 68 94204000 PUSH Reverse_.00402094
00401015 E8 38000000 CALL <JMP.>KERNEL32.GetDriveTypeA
00401016 46 INC ESI
Style = MB_OK!MB_APPLMODAL
Title = "abex' 1st crackme"
Text = "Make me think your HD is a CD-Rom."
hOwner = NULL
MessageBoxA
*RootPathName = "d:\"
*GetDriveTypeA

EAX 00000005
ECX 00008FE0
EDX 7C93E4F4 ntdll.KiFastSystemCallRet
EBX 7FFDE000
ESP 0012FFC4
EBP 0012FFF0
ESI FFFFFFFF
EDI 7C940208 ntdll.7C940208
EIP 0040101D Reverse_.0040101D

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

참고로 C:\W 일때는 EAX값이 3이 됩니다.