

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

00401000	6A 00	PUSH 0	Style = MB_OK!MB_APPLMODAL
00401002	68 00204000	PUSH 01.00402000	Title = "abex' 1st crackme"
00401007	68 12204000	PUSH 01.00402012	Text = "Make me think your HD is a CD"
0040100C	6A 00	PUSH 0	hOwner = NULL
0040100E	E8 4E000000	CALL <JMP.&USER32.MessageBoxA>	MessageBoxA
00401013	68 94204000	PUSH 01.00402094	RootPathName = "c:\\"
00401018	E8 38000000	CALL <JMP.&KERNEL32.GetDriveTypeA>	GetDriveTypeA
0040101D	46	INC ESI	
0040101E	48	DEC EAX	
0040101F	EB 00	JMP SHORT 01.00401021	
00401021	46	INC ESI	
00401022	46	INC ESI	
00401023	48	DEC EAX	
00401024	3BC6	CMP EAX,ESI	
00401026	74 15	JE SHORT 01.0040103D	
00401028	6A 00	PUSH 0	Style = MB_OK!MB_APPLMODAL
0040102A	68 35204000	PUSH 01.00402035	ASCII "Error"
0040102F	68 3B204000	PUSH 01.0040203B	ASCII "Nah... This is not a CD-ROM D"
00401034	6A 00	PUSH 0	hOwner = NULL
00401036	E8 26000000	CALL <JMP.&USER32.MessageBoxA>	MessageBoxA
0040103B	EB 13	JMP SHORT 01.00401050	
0040103D	6A 00	PUSH 0	Style = MB_OK!MB_APPLMODAL
0040103F	68 5E204000	PUSH 01.0040205E	Title = "YEAH!"
00401044	68 64204000	PUSH 01.00402064	Text = "Ok, I really think that you"

[그림 1. main 함수]

그림 1에서 빨간색 네모로 표시된 부분을 보면 EAX, ESI 레지스터의 값이 같을 경우 40103D 주소로 JMP한다. 그리고 그 곳에는 문제 해결을 알리는 메시지가 있다.

▶ 풀이 1. JMP를 이용한 주소 강제 이동

어떻게든 40103D로 보내야 된다는 사고방식에서 나온 첫 번째 풀이방법. 중간에 코드 한 줄을 조건 없이 JMP 40103D로 바꿔주는 것이다.

00401000	6A 00	PUSH 0	Style = MB_OK!MB_APPLMODAL
00401002	68 00204000	PUSH 01.00402000	Title = "abex' 1st crackme"
00401007	68 12204000	PUSH 01.00402012	Text = "Make me think your HD is a CD"
0040100C	6A 00	PUSH 0	hOwner = NULL
0040100E	E8 4E000000	CALL <JMP.&USER32.MessageBoxA>	MessageBoxA
00401013	68 94204000	PUSH 01.00402094	RootPathName = "c:\\"
00401018	E8 38000000	CALL <JMP.&KERNEL32.GetDriveTypeA>	GetDriveTypeA
0040101D	46	INC ESI	
0040101E	48	DEC EAX	
0040101F	EB 00	JMP SHORT 01.00401021	
00401021	46	INC ESI	
00401022	46	INC ESI	
00401023	48	DEC EAX	
00401024	EB 17	JMP SHORT 01.0040103D	
00401026	90	NOP	
00401027	90	NOP	
00401028	6A 00	PUSH 0	Style = MB_OK!MB_APPLMODAL
0040102A	68 35204000	PUSH 01.00402035	ASCII "Error"
0040102F	68 3B204000	PUSH 01.0040203B	ASCII "Nah... This is not a CD-ROM D"
00401034	6A 00	PUSH 0	hOwner = NULL
00401036	E8 26000000	CALL <JMP.&USER32.MessageBoxA>	MessageBoxA
0040103B	EB 13	JMP SHORT 01.00401050	
0040103D	6A 00	PUSH 0	Style = MB_OK!MB_APPLMODAL
0040103F	68 5E204000	PUSH 01.0040205E	Title = "YEAH!"
00401044	68 64204000	PUSH 01.00402064	Text = "Ok, I really think that you"

[그림 2. JMP 코드를 삽입한 모습]

0040101D	46	INC ESI	
0040101E	48	DEC EAX	
0040101F	EB 00	JMP SHORT 01.00401021	
00401021	46	INC ESI	
00401022	46	INC ESI	
00401023	48	DEC EAX	
00401024	EB 17	JMP SHORT 01.0040103D	
00401026	90	NOP	
00401027	90	NOP	
00401028	6A 00	PUSH 0	
0040102A	68 3E204000	PUSH 01.00402035	Style = MB_OK!MB_APPLMODAL
0040102F	68 3B204000	PUSH 01.0040203B	ASCII "Error"
00401034	6A 00	PUSH 0	ASCII "Nah... This is not a CD-ROM Drive!"
00401036	E8 26000000	CALL <JMP.&USER32.MessageBoxA>	hOwner = NULL
0040103B	EB 13	JMP SHORT 01.00401050	MessageBoxA
0040103D	6A 00	PUSH 0	Style = MB_OK!MB_APPLMODAL
0040103F	68 5E204000	PUSH 01.0040205E	Title = "YEAH!"
00401044	68 64204000	PUSH 01.00402064	Text = "Ok, I really think that your HD is a CD-ROM!"
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 [<&KERNEL32.GetDriveTypeA>]	kernel32.GetDriveTypeA
0040105B	FF25 54304000	JMP [<&KERNEL32.ExitProcess>]	kernel32.ExitProcess
00401061	FF25 5C304000	JMP [<&USER32.MessageBoxA>]	USER32.MessageBoxA

[그림 3. 40103D 주소로 이동한 모습]

▶ 풀이 2. INC, DEC, NOP 활용

1번 풀이방법이 강제로 주소를 이동시켰다면, 이번엔 조건문에 의한 이동을 해보는 것이다.

[그림 1]의 빨간 네모로 표시된 부분을 보면 EAX와 ESI의 값이 같을 경우 40103D로 이동하게 되어 있다. 아무 것도 건드리지 않고 CMP EAX ESI 명령을 실행할 경우, 값이 다르기 때문에 JE SHORT 01.0040103D를 만났을 때 40103D 주소로 이동하지 않는다.

0040103D	6A 00	PUSH 0	Style = MB_OK!MB_APPLMODAL
00401002	68 00204000	PUSH 01.00402000	Title = "abex" 1st crackme"
00401007	68 12204000	PUSH 01.00402012	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 24204000	PUSH 01.00402094	RootPathName = "c:\\"
00401018	E8 38000000	CALL <JMP.&KERNEL32.GetDriveTypeA>	GetDriveTypeA
0040101D	46	INC ESI	
0040101E	48	DEC EAX	
0040101F	EB 00	JMP SHORT 01.00401021	
00401021	46	INC ESI	
00401022	46	INC ESI	
00401023	48	DEC EAX	
00401024	3BC6	CMP EAX,ESI	
00401026	74 15	JE SHORT 01.0040103D	
00401028	6A 00	PUSH 0	Style = MB_OK!MB_APPLMODAL
0040102A	68 3E204000	PUSH 01.00402035	ASCII "Error"
0040102F	68 3B204000	PUSH 01.0040203B	ASCII "Nah... This is not a CD-ROM Drive!"
00401034	6A 00	PUSH 0	hOwner = NULL
00401036	E8 26000000	CALL <JMP.&USER32.MessageBoxA>	MessageBoxA
0040103B	EB 13	JMP SHORT 01.00401050	
0040103D	6A 00	PUSH 0	Style = MB_OK!MB_APPLMODAL
0040103F	68 5E204000	PUSH 01.0040205E	Title = "YEAH!"
00401044	68 64204000	PUSH 01.00402064	Text = "Ok, I really think that your HD is a CD-ROM!"
00401049	6A 00	PUSH 0	hOwner = NULL

[그림 4. GetDriveTypeA 함수를 빠져나온 직후의 모습]

GetDriveTypeA 함수를 빠져나왔을 때의 EAX의 값은 3이고 ESI의 값은 0이다. 그 밑의 INC와 DEC 명령을 다 실행하고 비교할 때쯤이면 EAX는 1, ESI는 3이 된다. 때문에, INC, DEC, NOP 명령을 적절히 활용해 EAX와 ESI의 값을 서로 같게 만들어준다.

00401000	6A 00	PUSH 0	Style = MB_OK!MB_APPLMODAL
00401002	68 00204000	PUSH 01.00402000	Title = "abex" 1st crackme"
00401007	68 12204000	PUSH 01.00402012	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 01.00402094	RootPathName = "c:\\"
00401018	E8 38000000	CALL <JMP.&KERNEL32.GetDriveTypeA>	GetDriveTypeA
0040101D	46	INC ESI	
0040101E	90	NOP	
0040101F	EB 00	JMP SHORT 01.00401021	
00401021	46	INC ESI	
00401022	46	INC ESI	
00401023	90	NOP	
00401024	3BC6	CMP EAX,ESI	
00401026	74 15	JE SHORT 01.0040103D	
00401028	6A 00	PUSH 0	Style = MB_OK!MB_APPLMODAL
0040102A	68 35204000	PUSH 01.00402035	ASCII "Error"
0040102F	68 3B204000	PUSH 01.0040203B	ASCII "Nah... This is not a CD-ROM Drive!"
00401034	6A 00	PUSH 0	hOwner = NULL
00401036	E8 26000000	CALL <JMP.&USER32.MessageBoxA>	MessageBoxA
0040103B	EB 13	JMP SHORT 01.00401050	
0040103D	6A 00	PUSH 0	Style = MB_OK!MB_APPLMODAL
0040103F	68 5E204000	PUSH 01.0040205E	Title = "YEAH!"
00401044	68 64204000	PUSH 01.00402064	Text = "Ok, I really think that your HD is a CD-ROM!"

Registers (FPU)	
EAX	00000003
ECX	77882FED ntdll.77882FED
EDX	005D1CE8
EBX	7EFDE000
ESP	0018FF8C
EBP	0018FF94
ESI	00000003
EDI	00000000
EIP	00401024 01.00401024
C 0	ES 002B 32bit 0(FFFFFFFF)
P 1	CS 0023 32bit 0(FFFFFFFF)
A 0	SS 002B 32bit 0(FFFFFFFF)
Z 0	DS 002B 32bit 0(FFFFFFFF)
S 0	FS 0053 32bit 7EFDD000(FFF)
T 0	GS 002B 32bit 0(FFFFFFFF)
D 0	
O 0	LastErr ERROR_SUCCESS (00000000)
EFL	00000206 (NO,NB,NE,A,NS,PE,GE,G)
ST0	empty 0.0
ST1	empty 0.0
ST2	empty 0.0
ST3	empty 0.0
ST4	empty 0.0
ST5	empty 0.0
ST6	empty 1.00000000000000000000

[그림 5와 6. 코드 수정 후 실행]

EAX와 ESI의 값을 3으로 맞춰주고 성공 메시지가 있는 40103D 주소로 이동한다. 하지만 문제에선 GetDriveTypeA 함수에서 리턴값이 몇이 되어야 하냐고 물었다. [\[그림 4\]](#)를 보면 GetDriveTypeA 함수를 빠져나오고 나서 EAX의 값엔 -2를 하고, ESI의 값은 0인 상태에서 +3을 한다. EAX의 값을 3으로 만들어주기 위해선 GetDriveTypeA 함수의 리턴값은 5가 되어야 할 것이다. $(x - 2 = 0 + 3)$