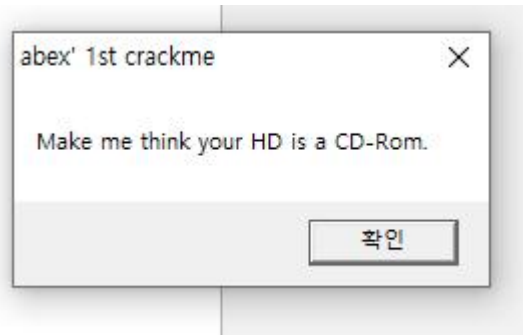
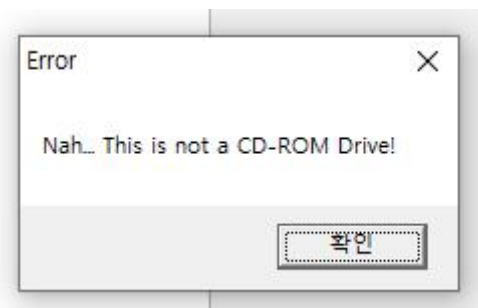


[CodeEngn-basic RCE-01]

C 드라이브를 CD롬으로 인식시키기



1. 그냥 돌리면 Nah...하면서 인식 안해줌.

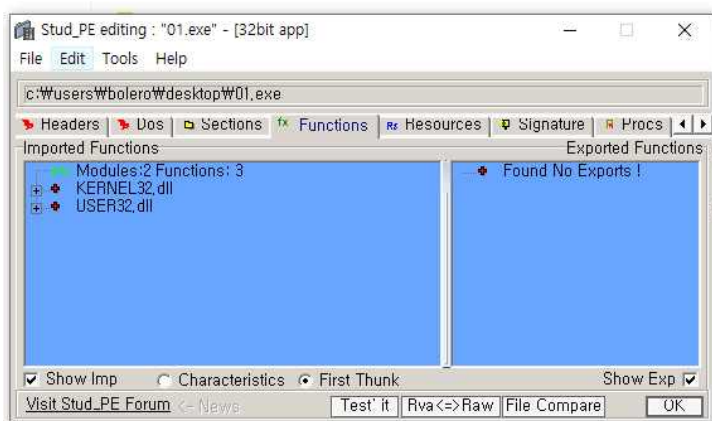


이걸 이제 어떻게?

Olly Dbg로 열어본다.

그전에, 이 파일이 32bit 파일인지 64bit 파일인지 체크해야함 -> STUD PE 프로그램으로 체크

ntdll 없으면 32bit로 보자



32bit 맞는 듯.

olly dbg 로 열면

00401000	6A 00	PUSH 0	Style = MB_OK!MB_APPLMODAL
00401002	68 00204000	PUSH 402000	Title = "abex' 1st crackne"
00401007	68 12204000	PUSH 402012	Text = "Make me think your HD is a CD-Rom."
0040100C	6A 00	PUSH 0	hOwner = NULL
0040100E	E8 4E000000	CALL 00401061	MessageBoxA
00401013	68 94204000	PUSH 402094	RootPathName = "c:\\"
00401018	E8 38000000	CALL 00401055	GetDriveTypeA
0040101D	46	INC ESI	
0040101E	48	DEC EAX	
0040101F	75 00	JMP SHORT 00401021	00401021
00401021	46	INC ESI	
00401022	46	INC ESI	
00401023	48	DEC EAX	
00401024	3BC6	CMP EAX, ESI	
00401025	74 15	JE SHORT 00401030	00401030
00401028	6A 00	PUSH 0	Style = MB_OK!MB_APPLMODAL
0040102A	68 35204000	PUSH 402035	Title = "Error"
0040102F	68 38204000	PUSH 402038	Text = "Nah... This is not a CD-ROM Drive!"
00401034	6A 00	PUSH 0	hOwner = NULL
00401036	E8 26000000	CALL 00401061	MessageBoxA
0040103B	75 13	JMP SHORT 00401050	00401050
0040103D	6A 00	PUSH 0	Style = MB_OK!MB_APPLMODAL
0040103F	68 5E204000	PUSH 40205E	Title = "YEAH!"
00401044	68 64204000	PUSH 402064	Text = "Ok, I really think that your HD is a CD-ROM! :p"
00401049	6A 00	PUSH 0	hOwner = NULL
0040104B	E8 11000000	CALL 00401061	MessageBoxA
00401050	E8 06000000	CALL 0040105B	ExitProcess
00401055	FF25 50304000	JMP DWORD PTR DS:[403050]	KERNEL32.GetDriveTypeA
0040105B	FF25 54304000	JMP DWORD PTR DS:[403054]	KERNEL32.ExitProcess
00401061	FF25 5C304000	JMP DWORD PTR DS:[40305C]	USER32.MessageBoxA
00401067	00	DB 00	

이렇게 나옴.

함수들 보니까

1. MessageBoxA
2. GetDriveTypeA
3. 다시 MessageBoxA
4. ExitProcess

1번은 그냥 문제제시인 것 같고, 2번이 HDD인식 과정? 3번이 결과 메시지 4번이 프로그램 종료

돌러보니까 00401021부터 00401024까지 ESI 두 번 증가(INC)시키고 EAX 한 번 감소(DEC) 시킨다. 그리고 나중에 ESI랑 EAX랑 비교해서 같으면 점프(JE) 어디로? 0040103D -> 정답입니다! 메시지 출력 부분.

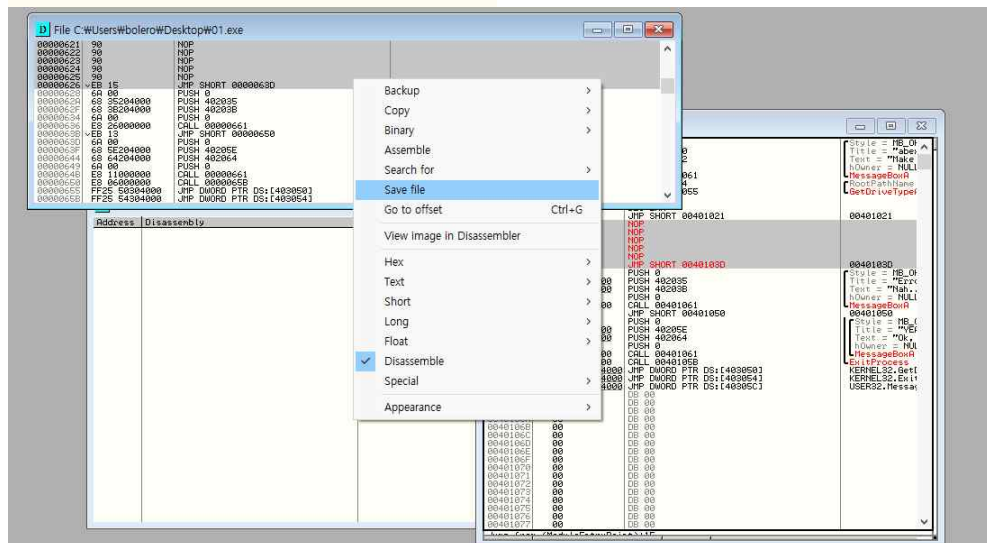
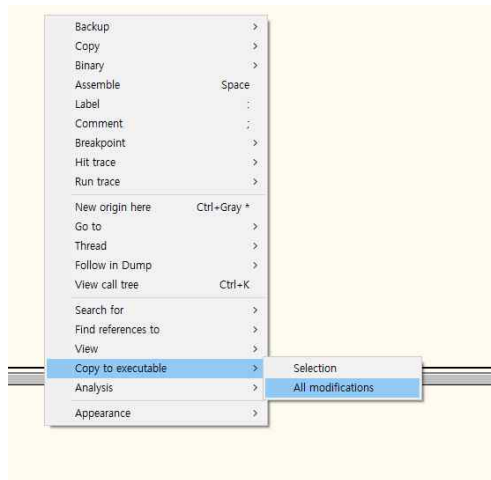
난 그냥 저부분 다 NOP으로 때렸다. 그리고 JE가 아니라 JMP로 바꿈(무조건분기)

00401000	6A 00	PUSH 0	Style = MB_OK!MB_APPLMODAL
00401002	68 00204000	PUSH 402000	Title = "abex' 1st crackne"
00401007	68 12204000	PUSH 402012	Text = "Make me think your HD is a CD-Rom."
0040100C	6A 00	PUSH 0	hOwner = NULL
0040100E	E8 4E000000	CALL 00401061	MessageBoxA
00401013	68 94204000	PUSH 402094	RootPathName = "c:\\"
00401018	E8 38000000	CALL 00401055	GetDriveTypeA
0040101D	46	INC ESI	
0040101E	48	DEC EAX	
0040101F	75 00	JMP SHORT 00401021	00401021
00401021	90	NOP	
00401022	90	NOP	
00401023	90	NOP	
00401024	90	NOP	
00401025	90	NOP	
00401026	75 15	JMP SHORT 0040103D	0040103D
00401028	6A 00	PUSH 0	Style = MB_OK!MB_APPLMODAL
0040102A	68 35204000	PUSH 402035	Title = "Error"
0040102F	68 38204000	PUSH 402038	Text = "Nah... This is not a CD-ROM Drive!"
00401034	6A 00	PUSH 0	hOwner = NULL
00401036	E8 26000000	CALL 00401061	MessageBoxA
0040103B	75 13	JMP SHORT 00401050	00401050
0040103D	6A 00	PUSH 0	Style = MB_OK!MB_APPLMODAL
0040103F	68 5E204000	PUSH 40205E	Title = "YEAH!"
00401044	68 64204000	PUSH 402064	Text = "Ok, I really think that your HD is a CD-ROM! :p"
00401049	6A 00	PUSH 0	hOwner = NULL
0040104B	E8 11000000	CALL 00401061	MessageBoxA
00401050	E8 06000000	CALL 0040105B	ExitProcess
00401055	FF25 50304000	JMP DWORD PTR DS:[403050]	KERNEL32.GetDriveTypeA
0040105B	FF25 54304000	JMP DWORD PTR DS:[403054]	KERNEL32.ExitProcess
00401061	FF25 5C304000	JMP DWORD PTR DS:[40305C]	USER32.MessageBoxA

이렇게!

패치하는 법

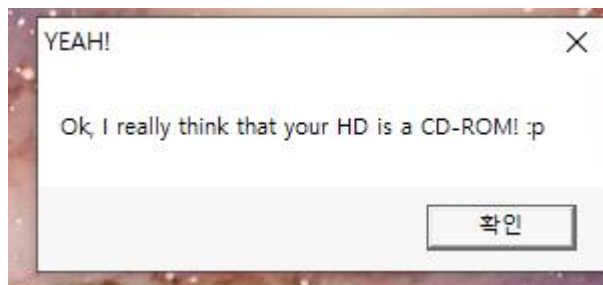
우클릭 -> copy to executable -> All modifications -> Copy All 클릭



우클릭 후 Save file 클릭(창이 보이면 좌측 상단 File~이 있고 우측 하단 CPU - 가 있다. 여기서 좌측 상단에 우클릭 해야함.)

이후 file name 적고 save하면 됨. 난 01\_patch.exe 로 저장.

그러면...



성공!

문제는 GetDriveTypeA의 리턴값이 뭐가 되어야 정상 실행되는가? 인데

리턴값 -> EAX로 들어감.

그럼 GetDriveTypeA 함수 실행된 이후 EAX 값을 봐야 함.

Registers (FPU)	
EAX	00000003
ECX	006A0000
EDX	006A0000
EBX	003D9000
ESP	0019FF74
EBP	0019FF80
ESI	00401000 01.<ModuleEntryPoint>
EDI	00401000 01.<ModuleEntryPoint>
EIP	0040101D 01.0040101D
C 0	ES 002B 32bit 0(FFFFFFFF)
P 1	CS 0023 32bit 0(FFFFFFFF)
A 0	SS 002B 32bit 0(FFFFFFFF)
Z 1	DS 002B 32bit 0(FFFFFFFF)
S 0	FS 0053 32bit 3DC000(FFF)
T 0	GS 002B 32bit 0(FFFFFFFF)

EAX = 3 나왔네?

이후 어셈코드를 보면

INC ESI	01.<ModuleEntryPoint>
DEC EAX	
JMP SHORT 00401021	00401021
INC ESI	
INC ESI	
DEC EAX	
CMP EAX, ESI	0040103D
JE SHORT 0040103D	0040103D
PUSH 0	Style = MB_OK MB_APPLMODAL
PUSH 402035	Title = "Error"
PUSH 40203B	Text = "Nah... This is not a CD-ROM Drive!"
PUSH 0	hOwner = NULL
CALL 00401061	MessageBoxA
JMP SHORT 00401050	00401050
PUSH 0	Style = MB_OK MB_APPLMODAL
PUSH 40205E	Title = "YEAH!"
PUSH 402064	Text = "Ok, I really think that your HD is a CD-ROM! :p"
PUSH 0	hOwner = NULL
CALL 00401061	MessageBoxA
CALL 0040105B	ExitProcess
JMP DWORD PTR DS:[403050]	KERNEL32.GetDriveTypeA
JMP DWORD PTR DS:[403054]	KERNEL32.ExitProcess
JMP DWORD PTR DS:[40305C]	apphelp.74511CC0

DEC EAX가 2번있음.

계속 실행해보자. 소스 보니까 CMP EAX, ESI 비교인데, 저기 코드라인까지 갔을 때 ESI 값도 봐야함.

Registers (FPU)	
EAX	00000001
ECX	006A0000
EDX	006A0000
EBX	003D9000
ESP	0019FF74
EBP	0019FF80
ESI	00401003 01.00401003
EDI	00401000 01.<ModuleEntryPoint>
EIP	00401026 01.00401026

ESI = 3나왔네

EAX = 1이니까... 두 개가 같으면(JE) 정상문구 출력 -> EAX + 2해야 함.

즉, GetDriveTypeA 리턴값이 3이 아니라 5가 된다면...

DEC EAX, DEC EAX 했을 때 3이 나온다.

답 : 5