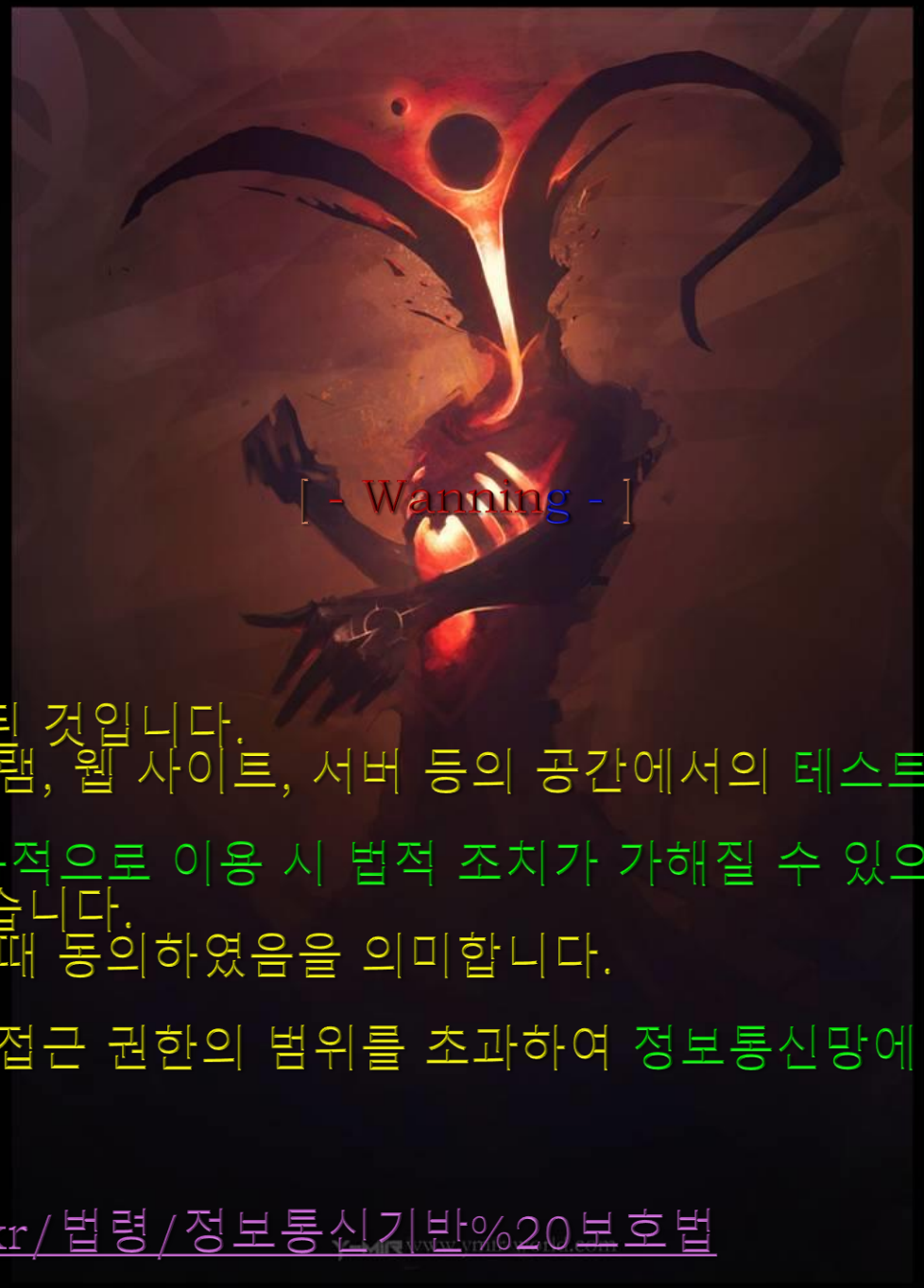


- 본 내용은 연구 목적으로 작성된 것입니다.
- 따라서, 허가 받지 않은 프로그램, 웹 사이트, 서버 등의 공간에서의 테스트를 절대 금지합니다.
- 악의적인 목적이나 상업적인 목적으로 이용 시 법적 조치가 가해질 수 있으며, 이에 발생할 수 있는 법적 책임은 전부 사용자 자신에게 있습니다.
- 이는, 해당 문서를 열람하였을 때 동의하였음을 의미합니다.
- 정당하지 않은 접근 권한이나, 접근 권한의 범위를 초과하여 정보통신망에 침해하는 행위 등은 관련 법률에 따라 처벌 받게 됩니다.
- 정보통신기반 보호법
  ◎ http://www.law.go.kr/법령/정보통신기반%20보호법

[- Team: 없음 -]

Author: bl4ck4rk Blog: bl4ck4rk.tistory.com E-Mail: bl4ck4rk@gmail.com

CodeEngn - Basic RCE

Contents

Contents

CodeEngn - Basic RCE

Basic RCE 01

Basic RCE 01

❖ Hint

Challenges : Basic 01

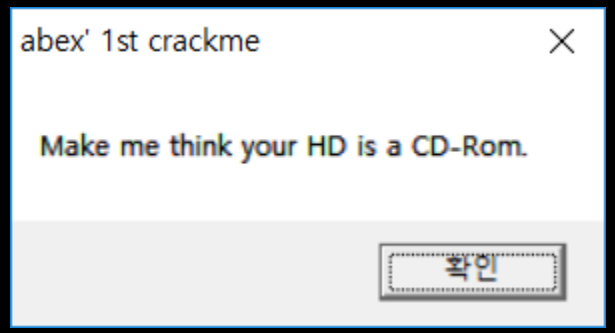
Author : abex

Korean :
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

Basic RCE 01

❖ Basic 01.exe 실행



➤ 해당 파일 형식을 HDD 파일 Type이 아닌 CD-ROM 파일 Type으로 변경시키라는 MessageBox 팝업

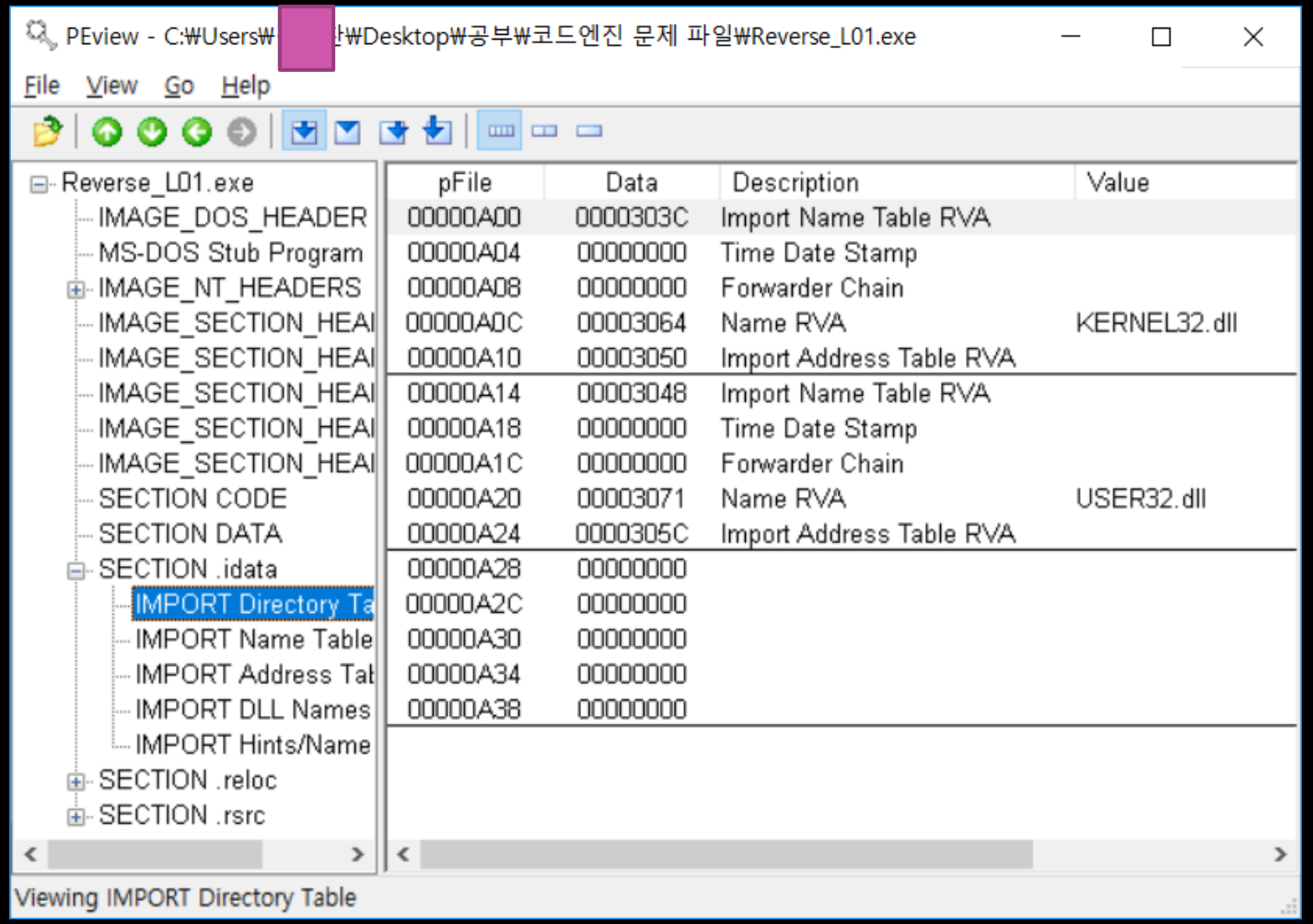
Basic RCE 01

❖ Basic 01.exe 실행

➤ 현재 파일은 CD-ROM Type이 아니라는 MessageBox 팝업

Basic RCE 01

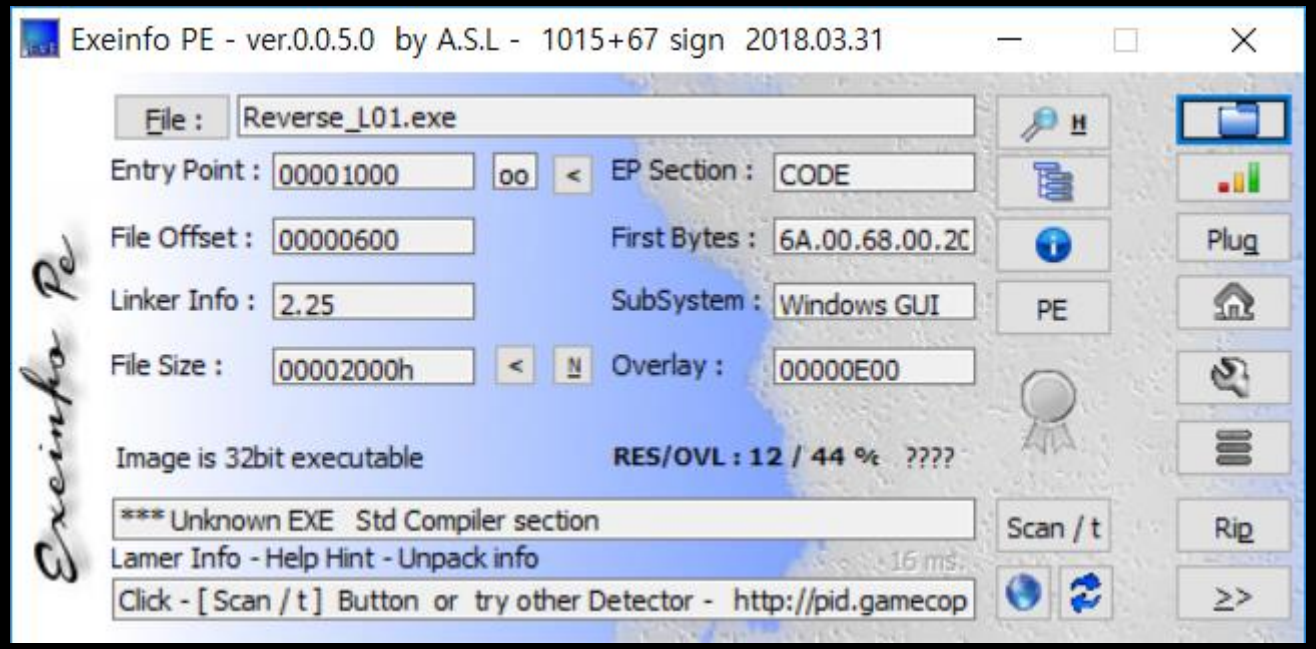
- PEview



- IAT가 깨지지 않았음을 확인

Basic RCE 01

- Exeinfo PE



- 분석 불가: 분류 불가능한 형식의 파일
- Assembly로 만들어진 프로그램으로 추측

Basic RCE 01

❖ start() - (0x00401000 ~ 0x00401050)

```
CODE:00401000 ; Attributes: noreturn
CODE:00401000
CODE:00401000                 public start
CODE:00401000 start           proc near
CODE:00401000                 push    0               ; uType
CODE:00401002                 push    offset Caption  ; "abex' 1st crackme"
CODE:00401007                 push    offset Text     ; "Make me think your HD is a CD-Rom."
CODE:0040100C                 push    0               ; hWnd
CODE:0040100E                 call    MessageBoxA
CODE:00401013                 push    offset RootPathName ; "c:\\"
CODE:00401018                 call    GetDriveTypeA
CODE:0040101D                 inc     esi
CODE:0040101E                 dec     eax
CODE:0040101F                 jmp     short $+2
```

➤ CD-ROM 만들라는 MessageBox() 호출 후 Drive Type 확인을 위한 연산 수행

Basic RCE 01

❖ start - (0x00401000 ~ 0x00401050)

```
CODE:00401021 loc_401021:                             ; CODE XREF: start+1F↑j
CODE:00401021                 inc     esi
CODE:00401022                 inc     esi
CODE:00401023                 dec     eax
CODE:00401024                 cmp     eax, esi
CODE:00401026                 jz      short loc_40103D
CODE:00401028                 push    0               ; uType
CODE:0040102A                 push    offset aError   ; "Error"
CODE:0040102F                 push    offset aNahThisIsNotAC ; "Nah... This is not a CD-ROM Drive!"
CODE:00401034                 push    0               ; hWnd
CODE:00401036                 call    MessageBoxA
CODE:0040103B                 jmp     short loc_401050
```

➤ Drive Type이 CD-ROM Drive일 경우 loc_40103D로 분기하고 아닐 경우 실패 문구가 담긴 MessageBox() 호출

Basic RCE 01

❖ start - (0x00401000 ~ 0x00401050)

```
CODE:0040103D loc_40103D:                             ; CODE XREF: start+26↑j
CODE:0040103D                 push    0               ; uType
CODE:0040103F                 push    offset aYeah    ; "YEAH!"
CODE:00401044                 push    offset aOkIReallyThink ; "Ok, I really think that your HD is a CD"...
CODE:00401049                 push    0               ; hWnd
CODE:0040104B                 call    MessageBoxA
CODE:00401050
CODE:00401050 loc_401050:                             ; CODE XREF: start+3B↑j
CODE:00401050                 call    ExitProcess
CODE:00401050 start           endp ; sp-analysis failed
CODE:00401050
CODE:00401055 ; [00000006 BYTES: COLLAPSED FUNCTION GetDriveTypeA. PRESS CTRL-NUMPAD+ TO EXPAND]
CODE:0040105B ; [00000006 BYTES: COLLAPSED FUNCTION ExitProcess. PRESS CTRL-NUMPAD+ TO EXPAND]
CODE:00401061 ; [00000006 BYTES: COLLAPSED FUNCTION MessageBoxA. PRESS CTRL-NUMPAD+ TO EXPAND]
CODE:00401067                 align 200h
CODE:00401200                 dd 380h dup(?)
CODE:00401200 CODE            ends
CODE:00401200
DATA:00402000 ; Section 2. (virtual address 00002000)
DATA:00402000 ; Virtual size                  : 00001000 (   4096.)
DATA:00402000 ; Section size in file          : 00000200 (    512.)
DATA:00402000 ; Offset to raw data for section: 00000800
DATA:00402000 ; Flags C0000040: Data Readable Writable
DATA:00402000 ; Alignment     : default
```

➤ CD-ROM Drive가 맞을 경우의 Routine

Basic RCE 01

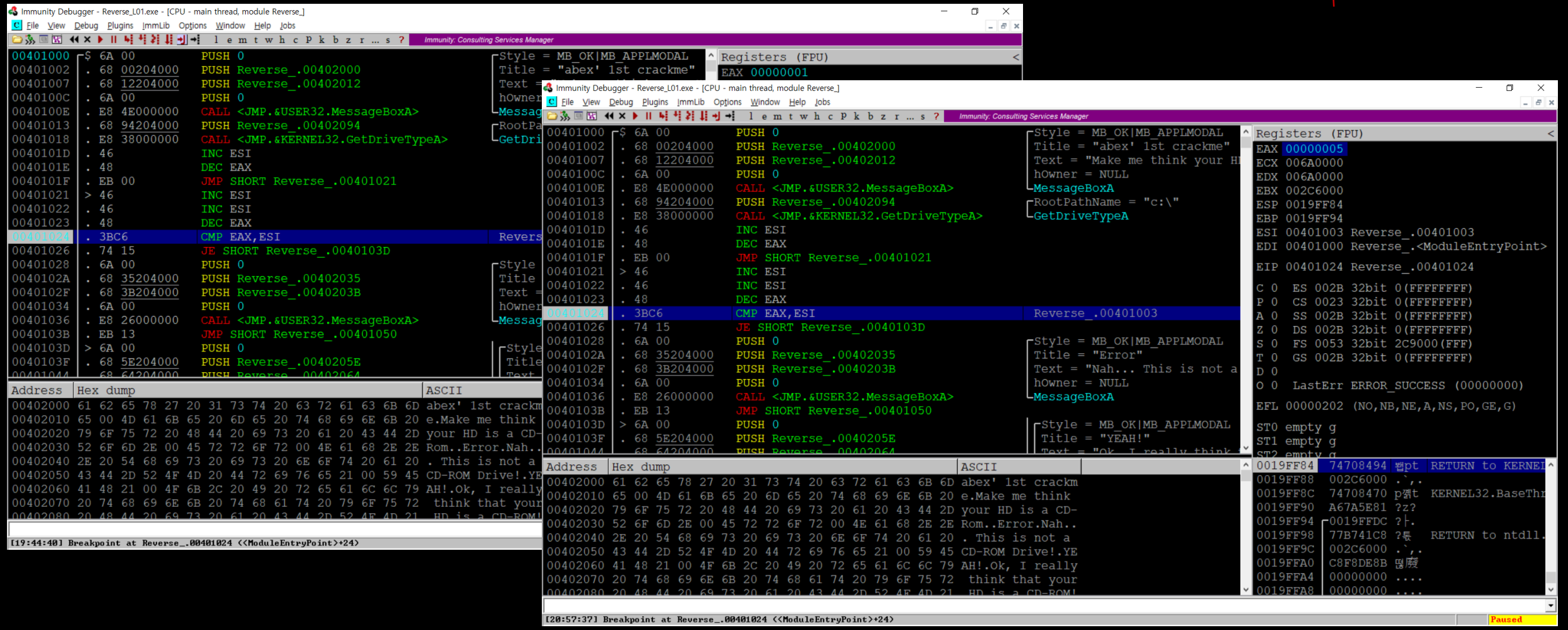
❖ GetDriveType()

DRIVE_UNKNOWN (0)	Drive 유형 결정 불가
DRIVE_NO_ROOT_DIR (1)	잘못된 root 경로
DRIVE_REMOVABLE (2)	플로피, 플래쉬 카드 리더 등
DRIVE_FIXED (3)	HDD, 플래쉬 드라이브 등
DRIVE_REMOTE (4)	원격 드라이브
DRIVE_CDROM (5)	CD-ROM
DRIVE_RAMDISK (6)	RAM 디스크

➤ 리턴 값이 5일 경우 CD Rom Type로 인식

Basic RCE 01

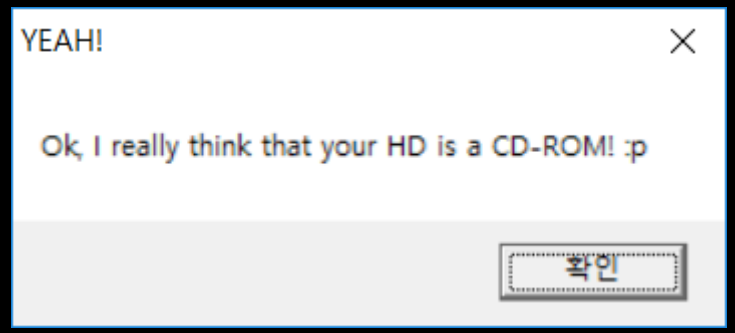
- 조건식 우회



- EAX를 5h로 Patch

Basic RCE 01

- CLEAR !



Basic RCE 01

❖ Source Code로 원복

```
MessageBox(hWnd, "Make me think your HD is a CD-Rom", "abex' 1st crakme", uType);

if ( GetDriveType("C:\\") != 5 )
{
    MessageBoxA(hWnd, "Nah... This is not a CD-ROM Drive!", "Error", uType);
    ExitProcess();
}

MessageBoxA(hWnd, "Ok, I really think that your HD is a CD"..., "YEAH!", uType);
ExitProcess();
```

➤ CD-ROM Drive가 맞을 경우의 Routine

References

References

https://codeengn.com/challenges