



[- Wanning -]

- 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

Basic RCE 01

Basic RCE 02

Basic RCE 03

Basic RCE 04

Basic RCE 05

Basic RCE 06

Basic RCE 07

Basic RCE 08

Basic RCE 09

Basic RCE 10

Basic RCE 11

Basic RCE 12

Basic RCE 13

Basic RCE 14

Basic RCE 15

Contents

Basic RCE 16

Basic RCE 17

Basic RCE 18

Basic RCE 19

Basic RCE 20

CodeEngn - Basic RCE

Basic RCE 01

Basic RCE 01

❖ Hint

Challenges : Basic 01

Author : abex

Korean :

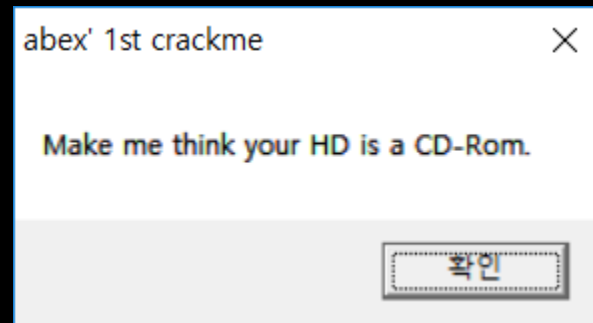
HDD를 CD-Rom으로 인식시키기 위해서는 GetDriveTypeA의 리턴값이 무엇이 되어야 하는가

English :

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

Basic RCE 01

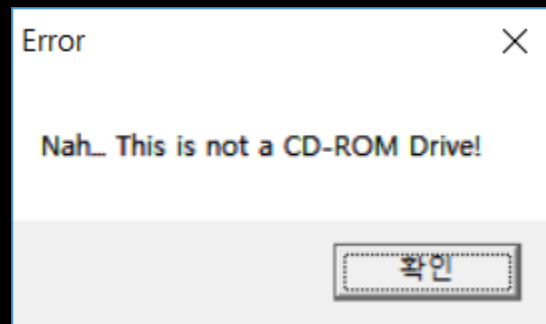
❖ Basic 01.exe 실행



- 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

❖ PView

The screenshot shows the PView application window titled "PView - C:\Users\...\Desktop\공부\코드엔진 문제 파일\Reverse_L01.exe". The left sidebar displays the file structure of the executable, with "SECTION .idata" expanded and "IMPORT Directory Table" selected. The main pane shows a table of import-related data.

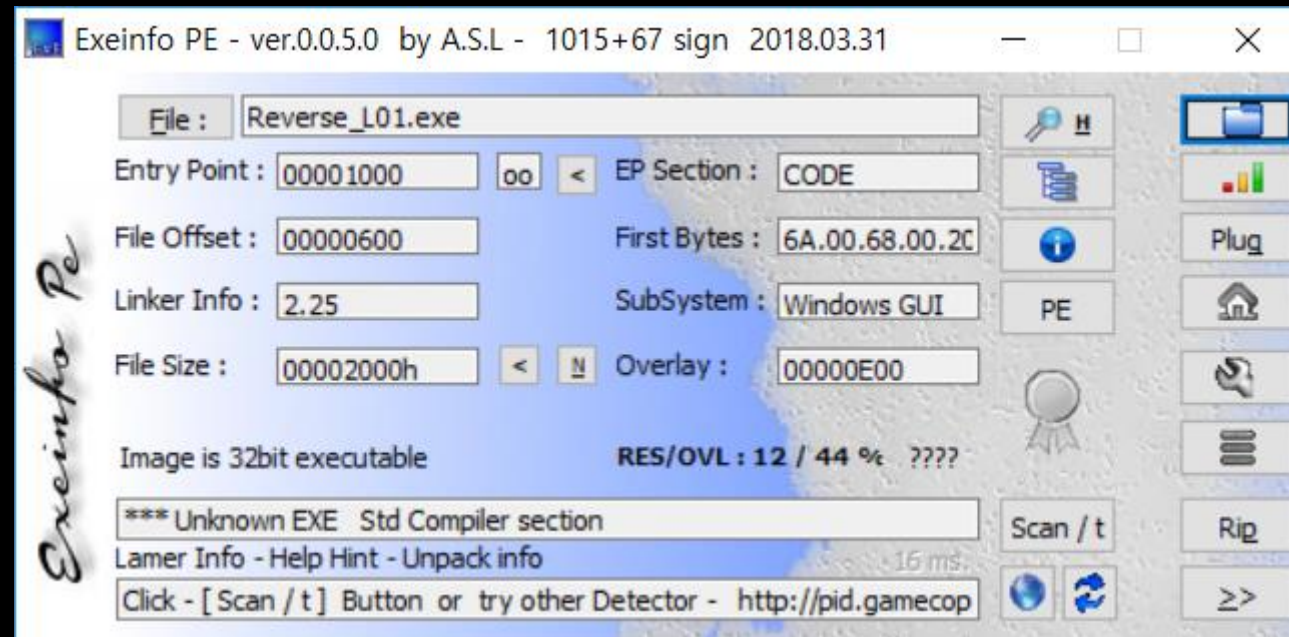
pFile	Data	Description	Value
00000A00	0000303C	Import Name Table RVA	
00000A04	00000000	Time Date Stamp	
00000A08	00000000	Forwarder Chain	
00000A0C	00003064	Name RVA	KERNEL32.dll
00000A10	00003050	Import Address Table RVA	
00000A14	00003048	Import Name Table RVA	
00000A18	00000000	Time Date Stamp	
00000A1C	00000000	Forwarder Chain	
00000A20	00003071	Name RVA	USER32.dll
00000A24	0000305C	Import Address Table RVA	
00000A28	00000000		
00000A2C	00000000		
00000A30	00000000		
00000A34	00000000		
00000A38	00000000		

Viewing IMPORT Directory Table

➤ 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

Immunity Debugger - Reverse_L01.exe - [CPU - main thread, module Reverse_]

File View Debug Plugins ImmLib Options Window Help Jobs

l e m t w h c P k b z r ... s ? Immunity Consulting Services Manager

00401000 \$ 6A 00 PUSH 0
00401002 . 68 00204000 PUSH Reverse_.00402000
00401007 . 68 12204000 PUSH Reverse_.00402012
0040100C . 6A 00 PUSH 0
0040100E . E8 4E000000 CALL <JMP.&USER32.MessageBoxA>
00401013 . 68 94204000 PUSH Reverse_.00402094
00401018 . E8 38000000 CALL <JMP.&KERNEL32.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_.0040103D
00401028 . 6A 00 PUSH 0
0040102A . 68 35204000 PUSH Reverse_.00402035
0040102F . 68 3B204000 PUSH Reverse_.0040203B
00401034 . 6A 00 PUSH 0
00401036 . E8 26000000 CALL <JMP.&USER32.MessageBoxA>
0040103B . EB 13 JMP SHORT Reverse_.00401050
0040103D > 6A 00 PUSH 0
0040103F . 68 5E204000 PUSH Reverse_.0040205E
00401044 . 68 64204000 PUSH Reverse_.00402064

Style = MB_OK|MB_APPLMODAL
Title = "abex' 1st crackme"
Text = "Make me think your H..."
hOwner = NULL
RootPathName = "c:\
GetDriveTypeA

Registers (FPU)
EAX 00000001

00401000 \$ 6A 00 PUSH 0
00401002 . 68 00204000 PUSH Reverse_.00402000
00401007 . 68 12204000 PUSH Reverse_.00402012
0040100C . 6A 00 PUSH 0
0040100E . E8 4E000000 CALL <JMP.&USER32.MessageBoxA>
00401013 . 68 94204000 PUSH Reverse_.00402094
00401018 . E8 38000000 CALL <JMP.&KERNEL32.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_.0040103D
00401028 . 6A 00 PUSH 0
0040102A . 68 35204000 PUSH Reverse_.00402035
0040102F . 68 3B204000 PUSH Reverse_.0040203B
00401034 . 6A 00 PUSH 0
00401036 . E8 26000000 CALL <JMP.&USER32.MessageBoxA>
0040103B . EB 13 JMP SHORT Reverse_.00401050
0040103D > 6A 00 PUSH 0
0040103F . 68 5E204000 PUSH Reverse_.0040205E
00401044 . 68 64204000 PUSH Reverse_.00402064

Style = MB_OK|MB_APPLMODAL
Title = "Error"
Text = "Nah... This is not a
hOwner = NULL
MessageBoxA

Registers (FPU)
EAX 00000005
ECX 006A0000
EDX 006A0000
EBX 002C6000
ESP 0019FF84
EBP 0019FF94
ESI 00401003 Reverse_.00401003
EDI 00401000 Reverse_.<ModuleEntryPoint>
EIP 00401024 Reverse_.00401024
C 0 ES 002B 32bit 0 (FFFFFFFF)
P 0 CS 0023 32bit 0 (FFFFFFFF)
A 0 SS 002B 32bit 0 (FFFFFFFF)
Z 0 DS 002B 32bit 0 (FFFFFFFF)
S 0 FS 0053 32bit 2C9000 (FFF)
T 0 GS 002B 32bit 0 (FFFFFFFF)
D 0
O 0 LastErr ERROR_SUCCESS (00000000)
EFL 00000202 (NO,NB,NE,A,NS,PO,GE,G)
ST0 empty g
ST1 empty g
ST2 empty g

Address Hex dump ASCII
00402000 61 62 65 78 27 20 31 73 74 20 63 72 61 63 6B 6D abex' 1st crackm
00402010 65 00 4D 61 6B 65 20 6D 65 20 74 68 69 6E 6B 20 e.Make me think
00402020 79 6F 75 72 20 48 44 20 69 73 20 61 20 43 44 2D your HD is a CD-
00402030 52 6F 6D 2E 00 45 72 72 6F 72 00 4E 61 68 2E 2E Rom..Error.Nah..
00402040 2E 20 54 68 69 73 20 69 73 20 6E 6F 74 20 61 20 . This is not a
00402050 43 44 2D 52 4F 4D 20 44 72 69 76 65 21 00 59 45 CD-ROM Drive!.YE
00402060 41 48 21 00 4F 6B 2C 20 49 20 72 65 61 6C 6C 79 AH!.Ok, I really
00402070 20 74 68 69 6E 6B 20 74 68 61 74 20 79 6F 75 72 think that your
00402080 20 48 44 20 69 73 20 61 20 43 44 2D 52 4F 4D 21 HD is a CD-ROM!

[19:44:40] Breakpoint at Reverse_.00401024 <<ModuleEntryPoint>+24

Address Hex dump ASCII
00402000 61 62 65 78 27 20 31 73 74 20 63 72 61 63 6B 6D abex' 1st crackm
00402010 65 00 4D 61 6B 65 20 6D 65 20 74 68 69 6E 6B 20 e.Make me think
00402020 79 6F 75 72 20 48 44 20 69 73 20 61 20 43 44 2D your HD is a CD-
00402030 52 6F 6D 2E 00 45 72 72 6F 72 00 4E 61 68 2E 2E Rom..Error.Nah..
00402040 2E 20 54 68 69 73 20 69 73 20 6E 6F 74 20 61 20 . This is not a
00402050 43 44 2D 52 4F 4D 20 44 72 69 76 65 21 00 59 45 CD-ROM Drive!.YE
00402060 41 48 21 00 4F 6B 2C 20 49 20 72 65 61 6C 6C 79 AH!.Ok, I really
00402070 20 74 68 69 6E 6B 20 74 68 61 74 20 79 6F 75 72 think that your
00402080 20 48 44 20 69 73 20 61 20 43 44 2D 52 4F 4D 21 HD is a CD-ROM!

Style = MB_OK|MB_APPLMODAL
Title = "YEAH!"
Text = "Ok, I really think

Registers (FPU)
EAX 00000005
ECX 006A0000
EDX 006A0000
EBX 002C6000
ESP 0019FF84
EBP 0019FF94
ESI 00401003 Reverse_.00401003
EDI 00401000 Reverse_.<ModuleEntryPoint>
EIP 00401024 Reverse_.00401024
C 0 ES 002B 32bit 0 (FFFFFFFF)
P 0 CS 0023 32bit 0 (FFFFFFFF)
A 0 SS 002B 32bit 0 (FFFFFFFF)
Z 0 DS 002B 32bit 0 (FFFFFFFF)
S 0 FS 0053 32bit 2C9000 (FFF)
T 0 GS 002B 32bit 0 (FFFFFFFF)
D 0
O 0 LastErr ERROR_SUCCESS (00000000)
EFL 00000202 (NO,NB,NE,A,NS,PO,GE,G)
ST0 empty g
ST1 empty g
ST2 empty g

0019FF84 74708494 RETN RETURN to KERNEL32.BaseTh
0019FF88 002C6000 .
0019FF8C 74708470 RETN KERNEL32.BaseTh
0019FF90 A67A5E81 ??
0019FF94 0019FFDC ?
0019FF98 77B741C8 RETN RETURN to ntdll.
0019FF9C 002C6000 .
0019FFA0 C8F8DE8B RETN
0019FFA4 00000000
0019FFA8 00000000

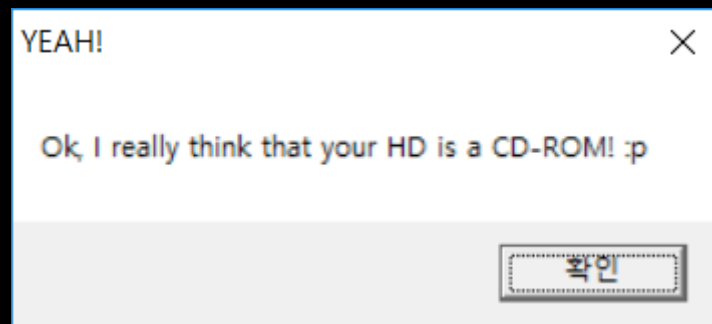
[20:57:37] Breakpoint at Reverse_.00401024 <<ModuleEntryPoint>+24

Paused

➤ EAX를 5로 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>