## REPORT

## **Basic RCE Level 1**

이름 : 신 민 구

제 출일: 2018.06.06

## 1. 문제 분석 및 실행

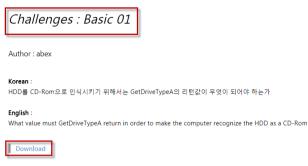


그림 1.1 Problem

Basic 01 의 문제는 'HDD 를 CD-ROM 으로 인식시키기 위해서는 GetDriveTypeA 의 리턴 값이 무엇이 되어야 하는가?' 이다. 처음 문제만 들으면 무슨 소리인지 잘 모를 수도 있다. 그러니 파일을 실행해 보아야 한다.



그림 1.2 실행 모습 1

파일을 실행하여 봤더니 'Make me think your HD is a CD-Rom.' 이라는 문자열이 나온다. 그리고 확인 버튼을 눌러보면 또 다음과 같은 메시지 박스가 나타난다.

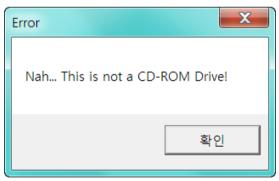


그림 1.3 실행 모습 2

Error 라는 메시지 박스와 'Nah... This is not a CD-ROM Drive!' 라는 문자열이 나타난다. 실행을 시켜 보니 모습일지 예상을 해 볼 수가 있다. GetDriveTypeA 의 값을 바꾸어 Error 가 아닌 정상적인 메시지 박스를 띄우는 것이 목표인 듯 하다.

## 2. OllyDbg 분석

OllyDbg 라는 툴을 이용하여 해당 파일을 열어보도록 하자.

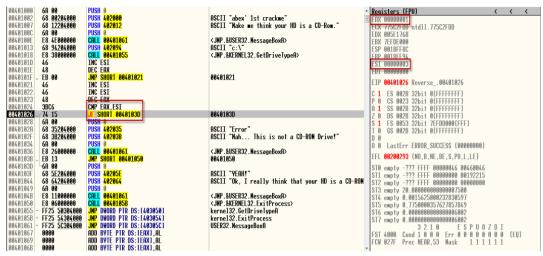


그림 2.1 EntryPoint

위 그림은 EP 이다. EP 란 'EntryPoint'로 파일을 열었을 때 제일 처음 부분을 말한다. 이 EP 를 보면 맨 오른쪽 부분에 우리에게 상당히 익숙한 문자열이 보인다.

맨 위의 문자열은 그림 1.2 의 메시지 박스이다. 그리고 밑에 보면 Error 메시지 박스가 나타나는 부분이 보이고 YEAH! 메시지 박스가 나타나는 부분이 보인다. 그리고 GetDriveTypeA 의 함수도 보인다. YEAH!라는 메시지 박스를 띄우기 위해 EAX 와 ESI를 비교하는데 같으면 YEAH! 메시지 박스로 넘어간다. 그러나 같지 않기 때문에 에러를 발생 시키는 것이다.

이번 문제는 GetDriveTypeA의 리턴 값을 바꿔 YEAH!의 메시지 박스를 출력하는 것이다. 하나하나 실행시켜 가며 분석을 해보자.

00401000 6A 00	PUSH 0	
00401002 68 00204000	PUSH 402000	ASCII "abex' 1st crackme"
00401007 68 12204000	PUSH 402012	ASCII "Make me think your HD is a CD-Rom."
0040100C 6A 00	PUSH 0	-
0040100E E8 4E000000	CALL 00401061	<jnp.&user32.messageboxa></jnp.&user32.messageboxa>
00401013 68 94204000	PIISH 402094	ASCII "c·\"
00401018 E8 38000000	CALL 00401055	<pre><jmp.&kernel32.getdrivetypea></jmp.&kernel32.getdrivetypea></pre>
0040101D 46	INC EST	
0040101E 48	DEC EAX	
0040101F V EB 00	JMP SHORT 00401021	00401021
00401021 46	INC ESI	
00401022 46	INC ESI	
00401023 48	DEC EAX	
00401024 3BC6	CMP EAX, ESI	
00401026 74 15	JE SHORT 0040103D	0040103D
00401028 6A 00	PUSH 0	
0040102A 68 35204000	PUSH 402035	ASCII "Error"
0040102F 68 3B204000	PUSH 40203B	ASCII "Nah This is not a CD-ROM Drive!"
00401034 6A 00	PUSH 0	
00401036 E8 26000000	CALL 00401061	<jnp.&user32.messageboxa></jnp.&user32.messageboxa>
0040103B V EB 13	JMP SHORT 00401050	00401050
0040103D 6A 00	PUSH 0	
0040103F 68 5E204000	PUSH 40205E	ASCII "YEAH!"
00401044 68 64204000	PUSH 402064	ASCII "Ok, I really think that your HD is a CD-ROM
00401049 6A 00	PUSH 0	
0040104B E8 11000000	CALL 00401061	<jmp.&user32.messageboxa></jmp.&user32.messageboxa>
ANAMATASA FR AGAAAAAA	CALL 0040105R	<.IMP &KERNEL 32 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 0000	ADD BYTE PTR DS:[EAX],AL	
00401069 0000	ADD BYTE PTR DS:[EAX],AL	
0040106B 0000	ADD BYTE PTR DS:[EAX],AL	
DS:[00403050]=763BEF85 (kernel32.GetDriveTypeA)		

그림 2.2 GetDriveTypeA

401018 주소에 CALL 을 만나 GetDriveTypeA 로 간다. 그 주소가 401055 인데 그 곳으로 가보니 JMP DWORD PTR DS:[403050]이다. 그리고 이 주소는 정확히 763BEF85 이다. 이 구간은 kernel32.dll 파일 영역으로써 완전 다른 영역으로 넘어 간다.



그림 2.3 GetDriveTypeA Return

RETN 할 때 EAX의 값이 3이었는데 5로 바꾸어주었는데 이는 나중에 JE 명령문을 만났을 때 ESI와 동일한 값으로 만들어 주기 위함이다.



그림 2.5 JE 명령어

JE 명령어를 만나기 까지 EAX와 ESI의 값이 같아짐을 알 수 있다. 이로써 YEAH!라는 성공 메시지 박스를 띄우게 된다.

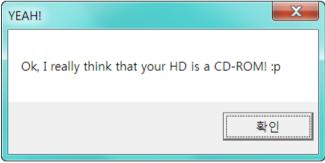


그림 2.6 성공 메시지 박스