

# REPORT:

## 코드엔진 Basic

### RCE 01 Writeup

COLONY  
1824275 정상지

2021.05.09

<GetDriveTypeA>의 리턴값을 조정하여 HDD를 CD로 인식시키자

<GetDriveTypeA>호출 후 EAX의 값이 3으로 리턴된다

FPU 숨기기		
EAX	00000003	
EBX	003C9000	
ECX	00720000	
EDX	00720000	
EBP	0019FF80	
ESP	0019FF74	)\"
ESI	00401000	<01.EntryPoint>
EDI	00401000	<01.EntryPoint>
EIP	0040101D	01.0040101D
EFLAGS	00000244	
ZE	1	PF 1 AE 0
QF	0	SE 0 DF 0
CF	0	TF 0 IF 1

inc esi // esi에 1을 더한다  
 dec eax // eax에 1을 뺀다  
 inc esi // esi에 1을 더한다  
 inc esi // esi에 1을 더한다  
 dec eax // eax에 1을 뺀다  
 cmp eax,esi // esi와 eax를 비교한다. -> 같을 경우 ZF = 0  
 je 01.40103D // ZF = 1일 경우 뒤의 주소로 이동한다

해당 구문 실행 시  $eax-2=esi+3$ 을 비교하여 ZF에 값이 변경된다  
 따라서 eax의 값이 esi+5의 값으로 리턴되면 je 구문을 통과하여  
 HDD를 CD로 인식시킬 수 있다.

편집

표현식: 00401005

바이트: 05104000

Signed: 4198405

Unsigned: 4198405

ASCII: .@..

확인(O) 취소(C)

esi의 값이 00401000이므로 eax를 00401005로 변경한다

FPU 숨기기		
EAX	00401005	01.00401005
EBX	002B4000	
ECX	005A0000	
EDX	005A0000	
EBP	0019FF80	
ESP	0019FF74	)
ESI	00401000	<01.EntryPoint>
EDI	00401000	<01.EntryPoint>
EIP	0040101D	01.0040101D
EFLAGS	00000244	
ZE	1	PF 1 AF 0
OF	0	SF 0 DF 0
CF	0	TF 0 IF 1

FPU 숨기기		
EAX	00401003	&"abex' 1st crackme"
EBX	002B4000	
ECX	005A0000	
EDX	005A0000	
EBP	0019FF80	
ESP	0019FF74	)
ESI	00401003	&"abex' 1st crackme"
EDI	00401000	<01.EntryPoint>
EIP	00401026	01.00401026
EFLAGS	00000246	
ZE	1	PF 1 AF 0
OF	0	SF 0 DF 0
CF	0	TF 0 IF 1

je 구문 전에 esi값과 eax값이 같아진다

YEAH!

Ok, I really think that your HD is a CD-ROM! :p

확인

따라서 분기문 후에 CD드라이브로 메시지 박스를 출력한다

HDD를 CD-Rom으로 인식시키기 위해서는 GetDriveTypeA의 리턴값이 00401005가 되어야한다