codeengn Basic RCE L16



search reference text string

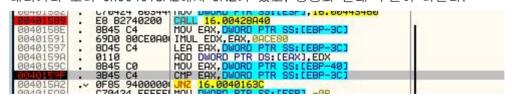
004015BF 004015C2 004015C7 004015CA 004015D2	•		MOV DWORD PTR SS:[ESP],EAX CALL <pre>CALL CALL </pre> <pre>CAMP.&KERNEL32.SetConsoleTextAttribute> SUB ESP,8 MOV DWORD PTR SS:[ESP+4],16.0043B1AB MOV DWORD PTR SS:[ESP+],16.004433C0</pre>	
004015D9 004015DE 004015E6	÷	E8 528D0200 C74424 04 D9 C70424 C0334	CALL 16.0042A330 MOV DWORD PTR SS:[ESP+4],16.004400D9 MOV DWORD PTR SS:[ESP],16.004433C0	ASCII " Good Job†⊡"

good job 앞에 있는 이 함수인거 같아서 bp 설정해봤으나, 걸리지 않음. 실패.

CALL 0043C3D8은 print 인 듯하다.

```
0040159C . 8845 C0 MOU EAX, DWORD PTR SS:[EBP-40]
0040159F . 3845 C4 CMP EAX, DWORD PTR SS:[EBP-3C]
00401592 . 0F85 9400000 UNZ 16.0040163C
00401598 . C70424 F5FFF MOV DWORD PTR SS:[ESP], -08
00401598 . E8 8CF60000 CALL < UMP.&KERNEL32.GetStdHandle>
00401594 . 93EC 04 SUB ESP, 4
00401597 . C74424 04 00 MOU DWORD PTR SS:[ESP]
```

내려가다 보니 0x004015A2에서 JNZ가 있고, 성공과 실패 구문이 나뉜다.



CMP에서 무엇과 무엇을 비교하는지를 중점적으로 살펴보자.

이것저것을 계속 대입해본 결과, EAX에는 내가 패스워드로 입력한 숫자가 들어감을 알 수 있었다. 반면, DWORD PTR [EBP-3C]는 항상 고정된 값이 들어가는 것을 확인하였다.



참고로 여기에는 패스워드로 '12345678'을 입력하였고, 이를 16진수로 표현한 값이 'BC614E'이다. 따라서 ebp-3c의 값을 10진수로 변환해서 패스워드로 넣어주면 정답이다. 정답은 3838184855!

