

0040157E	894424 04	MOV DWORD PTR SS:[ESP+4], EAX	
00401582	C70424 603444	MOV DWORD PTR SS:[ESP], 16.00443460	
00401589	E8 B2740200	CALL 16.00428A40	
0040158E	8B45 C4	MOV EAX, DWORD PTR SS:[EBP-3C]	
00401591	69D0 80CE0A00	IMUL EDX, EAX, 0ACE80	
00401597	8D45 C4	LEA EAX, DWORD PTR SS:[EBP-3C]	
0040159A	0110	ADD DWORD PTR DS:[EAX], EDX	
0040159C	8B45 C0	MOV EAX, DWORD PTR SS:[EBP-40]	
0040159F	3B45 C4	CMP EAX, DWORD PTR SS:[EBP-3C]	
004015A2	0F85 94000000	JNZ 16.0040163C	
004015A8	C70424 F5FFFF	MOV DWORD PTR SS:[ESP], -0B	
004015AF	E8 8CF60000	CALL <JMP.&KERNEL32.GetStdHandle>	GetStdHandle
004015B4	83EC 04	SUB ESP, 4	
004015B7	C74424 04 0A00	MOV DWORD PTR SS:[ESP+4], 0A	
004015BF	890424	MOV DWORD PTR SS:[ESP], EAX	
004015C2	E8 89F60000	CALL <JMP.&KERNEL32.SetConsoleTextAttribute>	SetConsoleTextAttribute
004015C7	83EC 08	SUB ESP, 8	
004015CA	C74424 04 A8B	MOV DWORD PTR SS:[ESP+4], 16.0043B1A8	
004015D2	C70424 C03344	MOV DWORD PTR SS:[ESP], 16.004433C0	
004015D9	E8 52800200	CALL 16.0042A330	
004015DE	C74424 04 D900	MOV DWORD PTR SS:[ESP+4], 16.004400D9	ASCII " Good Job!\n"
004015E6	C70424 C03344	MOV DWORD PTR SS:[ESP], 16.004433C0	
004015ED	E8 E6AD0300	CALL 16.0043C308	
004015F2	C74424 04 E500	MOV DWORD PTR SS:[ESP+4], 16.004400E5	ASCII " =)"
004015FA	C70424 C03344	MOV DWORD PTR SS:[ESP], 16.004433C0	
00401601	E8 D2AD0300	CALL 16.0043C308	
00401606	C70424 F50044	MOV DWORD PTR SS:[ESP], 16.004400F5	ASCII "pause > null"

분기문의 첫부분에 비교문이 있다.



선 실행후 password를 11111로 넣어주면

```

EAX 00002B67
ECX 00000000
EDX E4B88080
EBX 00004000
ESP 0028FE90
EBP 0028FF48
ESI 00000000
EDI 00000000
EIP 0040159F 16.0040159F

```

EAX에 11111의 16진수값이 들어가있다.

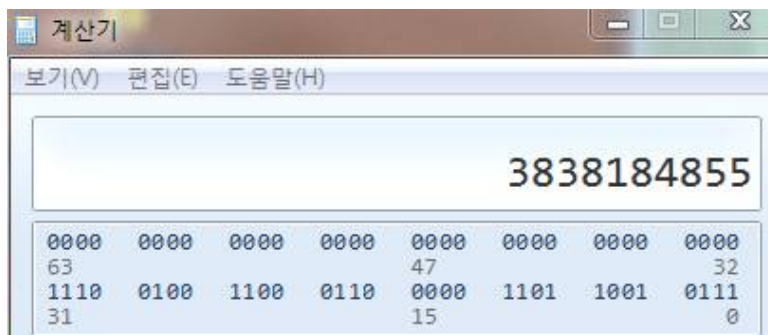
EAX와 EBP-3C값과 비교한다고 하였으니,

```

0028FF08 67 2B 00 00 97 0D C6 E4 97 0D C6 E4 97 0D C6 E4 97 0D C6 E4
0028FF10 24 00 00 00 58 00 00 00 58 00 00 00 58 00 00 00

```

저기 E4C60D97값을 10진수로하면, 정답이다.



정답