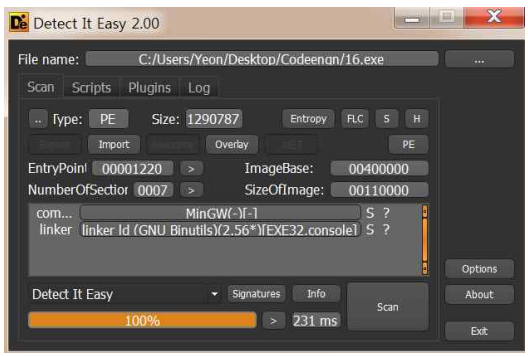
코드 엔진 Challenges: Basic 16

Author: ReWrite
Korean: Name이 CodeEngn일 때 Serial을 구하시오.

14,15와 비슷하게 Name 값에 따라 달라지는 Serial 값을 구하는게 목표이다.

파일을 실행해보면 이런식으로 실행된다 . Name에 CodeEngn을 넣고 임의의 값을 입력했을 때 임의의 값 9를 넣고 실행하자 "Wrong password!" 라는 문구가 뜬다.
먼저 DE를 통해 패킹 여부를 확인 해 보고 분석을 해보자.



올리디버거로 열고 아까 본 메시지의 문자열을 찾고 그 주소로 이동해보자.

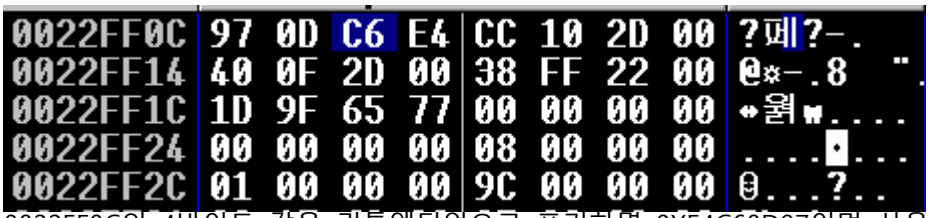
```
0040146F MOV DWORD PTR SS:[ESP+4],16.0044006C    ASCII " * This is my 5th crackme,   *"
00401483 MOV DWORD PTR SS:[ESP+4],16.0044008C    ASCII " * i hope you will enjoy it. *"
00401497 MOV DWORD PTR SS:[ESP+4],16.0044004C    ASCII " ****************************"
004014AB MOV DWORD PTR SS:[ESP+4],16.004400AC    ASCII ""
004014BF MOV DWORD PTR SS:[ESP+4],16.004400AF    ASCII " Enter your Name: "
00401560 MOV DWORD PTR SS:[ESP+4],16.004400C2    ASCII " Enter your Password: "
004015DE MOV DWORD PTR SS:[ESP+4],16.004400D9    ASCII " Good Job!"
004015F2 MOV DWORD PTR SS:[ESP+4],16.004400E5    ASCII " =)"
00401606 MOV DWORD PTR SS:[ESP],16.004400E9      ASCII "pause > null"
00401612 MOV DWORD PTR SS:[ESP],16.004400F6      ASCII "del null"
00401679 MOV DWORD PTR SS:[ESP+4],16.004400FF    ASCII " Wrong password!"
0040168D MOV DWORD PTR SS:[ESP+4],16.00440111    ASCII " =/"
```

추출된 문자열에 아까봤던 "WrongPassword" 뿐만 아니라 "Good Job"이라는 문자열도 있다. 입력한 시리얼값과 이름에 따라 생성된 옳은 시리얼값을 비교해서 점프하는 분기문이

나올 것을 예측할 수 있다. 주소로 이동하여 확인해 보자.

예상이 맞는 것을 확인 할 수 있다. EAX값과 어떤 값을 비교해 같지않으면 0040163C로 이동하여 "Wrong Password"를 출력하는 구문인 것을 확인 할 수있다. 이때 EAX에 무엇이 저장되고 그 비교하는 값은 무엇인지 확인해보자.

BP를 걸고 실행 후 Name에 CodeEngn을 넣고 Password에 9를 입력했을 때 EAX값에 입력한 9가 저장되는 것을 확인 할 수 있다. 따라서 CMP 명령에서 사용되는 EAX가 사용자 입력 값임을 알 수 있고 CMP 명령의 나머지 인자가 의미하는 값만 찾으면 된다 .나머지 인자가 의미하는 값은 [EBP-3C] 주소부터 4바이트 값을 읽어들이는 것이다. 레지스터 창에 적힌 EBP값 0022FF48에서 0000003C 만큼 뺀 0022FF0C로 이동해보자.



0022FF0C의 4바이트 값을 리틀엔디언으로 표기하면 0XE4C60D97이며 사용자 입력값인 EAX와 같은 값이 되기위해서 10진수로 계산해보면 3838184855인 것을 알 수있다.