

시험기간중ctf Pragmo

1. dead_or_alive

C:\Users\user\Downloads\dead_or_alive.exe

```
*****
          Put a curse on YOU.
진행 중인 시스템 종료가 없으므로 시스템 종료를 취소할 수 없습니다.(1116)
*****

*****

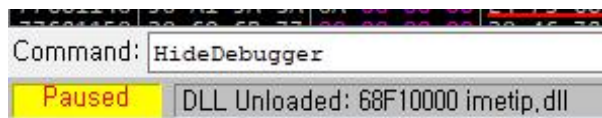
*  It s not easy this time...  *
*      DEAD or ALIVE.        *
*      GOOD LUCK TO YOU      *
*****

Please enter the first password.
=>
```

다운 받고 시작하면 비밀번호 입력창이 뜬다

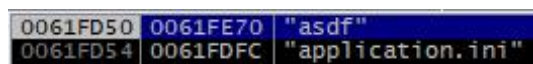
비밀번호를 알아내기 위해 디버거로 실행해주면 종료되는데

메시지 박스를 추적해보면 isdebuggerpresent로 안티디버깅을 구현한 것을 확인할 수 있었음

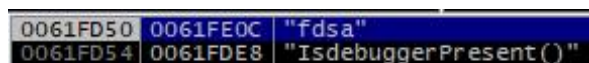


x32dbg의 HideDebugger로 간단하게 우회해준뒤

분석하면 비밀번호 검증 부분을 만날 수 있다



첫 번째 비밀번호와 strcmp하기 직전 스택상태



두 번째 비밀번호와 strcmp하기 직전 스택상태

각각 비밀번호를 맞게 입력해주고 검증을 통과하면



말도 안되는 시간동안 딜레이에 빠지는데 마찬가지로 수정해서 우회하고



프로그램 종료로 빠지는 jmp문까지 조작해서 우회하면
플래그를 보여준다

C:\Users\User\Downloads\dead_or_alive.exe

Put a curse on YOU.

* It s not easy this time... *

* DEAD or ALIVE. *

* GOOD LUCK TO YOU *

Please enter the first password.

=> application.ini

Please enter the second password.

=> IsdebuggerPresent()

FLAG{L0n9_T1M3_n0_S33_Xd}

계속하려면 아무 키나 누르십시오 . . .