CodeEngn Challenges : Basic 06

대구대학교 정보보호영재교육원 고등전문B 문성훈

2017년 07월 19일 작성

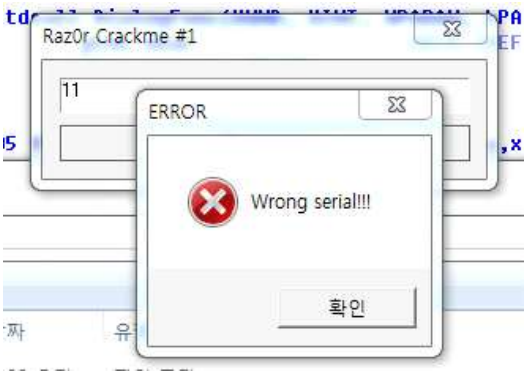
Challenges : Basic 06

Author : Raz0r

Korean :
Unpack를 한 후 Serial를 찾으시오. 정답인증은 OEP + Serial
Ex) 00400000PASSWORD

English :
Unpack, and find the serial. The solution should be in this format : OEP + Serial
Ex) 00400000PASSWORD

Download



프로그램을 실행하고 암거나 입력하고 ok눌러보았다. 하지만 당연히 안되는건 당연하다.
일단 시리얼을 찾기전에 OEP를 찾아야하는데...

unpacking 할때 oep찾는 방법

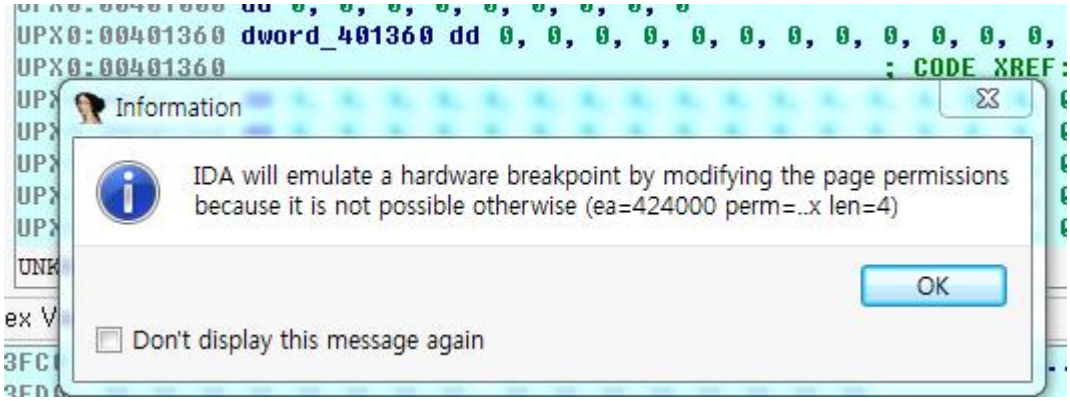
OEP란 UNPACKING에서 제일 중요한 부분으로
packing되기 전으로 돌아간곳.. 덤프를 떠주고 importrec를 구동하여 PACKING 해제된 파일을 만든다

UPX 로 압축을 하면 코드 PUSHAD 와 POPAD 는 한 쌍이 된다.
PUSHAD 실행 후 맨위의 스택 주소를 덤프하여 BYTE H/W BreakPoint를 지정하고 실행하면 POPAD 다음에서 멈추게 된다.이때, JMP 에 있는 주소가 OEP(Original Entry Point)가 된다.

보통 OEP를 찾는 방법은 여러가지가 있다. 단순히 코드를 하나하나 분석해가며 진행하는 방법에서부터
Stack을 이용한 방법, VirtualAlloc()를 이용하는 방법, LoadLibrary()를 이용하는 방법, Exception Handler를
이용하는 방법 등 요령껏 Packer마다의 다양한 방법이 이용될 수 있다.

대충 이렇다고 한다. 나는 그래서 패킹전 프로그램 첫 시작부에 브레이크 포인트를 지정하고 러닝 하니깐...

```
UPX0:00423FFF
UPX1:00424000 ; Section 2. (virtual address 00024000)
UPX1:00424000 ; Virtual size                  : 00006000 (  24576.)
UPX1:00424000 ; Section size in file          : 00005C00 (  23552.)
UPX1:00424000 ; Offset to raw data for section: 00000400
UPX1:00424000 ; Flags E0000040: Data Executable Readable Writable
UPX1:00424000 ; Alignment     : default
UPX1:00424000 ; ===========================================================================
UPX1:00424000
UPX1:00424000 ; Segment type: Pure code
UPX1:00424000 ; Segment permissions: Read/Write/Execute
UPX1:00424000 UPX1            segment para public 'CODE' use32
UPX1:00424000                 assume cs:UPX1
UPX1:00424000                 ;org 424000h
UPX1:00424000                 assume es:nothing, ss:nothing, ds:UPX0, fs:nothing, gs:nothing
UPX1:00424000 dword_424000    dd 9797BAEBh, 28E90CDh, 4019E59h, 0CC09FC9h, 20FFFF59h
UPX1:00424000                                         ; DATA XREF: start+1Ao
UPX1:00424014 ; ---------------------------------------------------------------------------
```



OEP가 가볍게 찾아졌다. OEP는 00401360이다.

이제 시리얼을 찾을 차례이다. 눈감고 UPX언패킹을 한후 Wrong메세지를 검색해 그 근처어셈블리를 뒤져보고자 하였다.

```
call    __chkesp
push    offset String   ; char *
push    offset aAd46dfs547 ; "AD46DFS547"
call    _strcmp
add     esp, 8
test    eax, eax
jnz     short loc_4010A3
mov     esi, esp
push    40h             ; uType
push    offset Caption  ; "Good Job!"
push    offset Text     ; "You got it ;)"
mov     ecx, hWnd
push    ecx             ; hWnd
call    ds:MessageBoxA
cmp     esi, esp
call    __chkesp
```

바로등장.

답은 00401360AD46DFS547