Crack me 문제 보고서

|  |  |
| --- | --- |
| 문제명 | Unpackme 02 |
| 파일명 | Unpackme 02.exe |
| 풀이자 | 서치원(2011003155) |
| 풀이 기간 | 2016/01/10 ~ 2017/01/16 |
| 문제 내용 | \* Unpacking 하여 OEP를 찾아내라. |

문제 풀이:



문제 파일을 실행시 계산기 프로그램이 실행됩니다. 프로그램의 문제 자체는 해결해야하는 요소가 없으므로 unpacking만 진행합니다.



ollydbg로 실행한 첫번째 화면입니다. 만약 UPX로 packing 되어있는 프로그램이라면 PUSHAD - POPAD 구간이 존재할 것입니다.



PUSHAD 구간에 도달한 모습입니다. POPAD 구간에서 PUSHAD에서 쌓인 스택 지점으로 돌아올테니 찾으려면 PUSHAD의 스택 지점을 break 걸어야하는데 방법은 address 지점을 long -> address 형식으로 변경한 후 ESP 레지스터를 follow in dump로 하여 그 지점으로 이동후 break를 걸면 됩니다.



break가 걸려 POPAD에 도달한 모습입니다. POPAD 이후 JMP를 하는 지점이 있는데 JMP로 넘어가는 주소가 프로그램의 시작지점인 OEP 주소입니다.



OEP 지점까지 실행 후 dump를 합니다. 실제 dump를 할 때 Rebuild import는 에러가 날 수 있으므로 해제해줍니다.

이렇게 dump를 뜬 프로그램은 실행시 오류가 나게 되므로 또 다른 프로그램으로 IAT를 복구해야 합니다.