Crack me 문제 보고서

|  |  |
| --- | --- |
| 문제명 | UnPackMe\_!EP (EXE Pack) 1.4 |
| 파일명 | UnPackMe\_!EP (EXE Pack) 1.4.exe |
| 풀이자 | 서치원(2011003155) |
| 풀이 기간 | 2016/02/12 ~ 2017/02/19 |
| 문제 내용 | \* Unpacking 하라. |

문제 풀이:

문제 파일을 실행 시 창 하나가 뜨게됩니다.



프로그램 창의 모습은 1.0 문제와 같습니다.



PEiD로 분석해보면 특이하게도 packing 방식을 찾지 못합니다.



Ollydbg로 실행해보면 PUSHAD 대신 CLC라는 명령으로 시작하게 됩니다.



line by line으로 진행하다 보면 PUSHAD 지점에 도달하게 됩니다. 이제 전과 같은 방법으로 POPAD를 찾아봅니다.



좀더 진행해보면 POPAD가 나오고 return을 하게 됩니다.



return을 하면 이 지점으로 오게 됩니다. 이 시점에서 stack 위치가 프로그램 시작 위치와 같으므로 이 지점이 OEP임을 알 수 있습니다.