codeengn-basic-L10 풀이

리버싱 문제풀이 / Wonlf / 2022. 3. 31. 22:32

문제는 OEP와 '등록성공'으로 가는 분기점의 OPCODE를 원하고 있다.

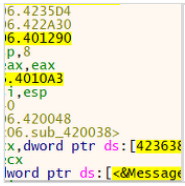
Die에 넣어보겠다.

ASPack패커로 패킹이 되어 있는 모습이다.

ASPack패킹을 해제하는 툴이 UPX처럼 있는 건 아닌 것 같은데 UPX와 동일한 방법으로 패킹을 한다고 하니, 수동으로 OEP를 찾아보겠다.

OEP를 찾는 것은

2022.03.13 - [리버싱 문제 풀이/CodeEngn.com] - codeengn-basic-L06 풀이 OEP알아내기

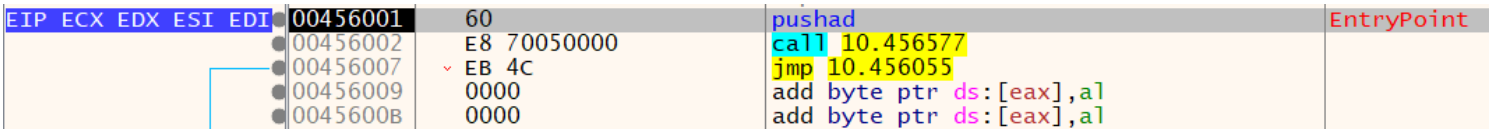


codeengn-basic-L06 풀이 OEP알아내기

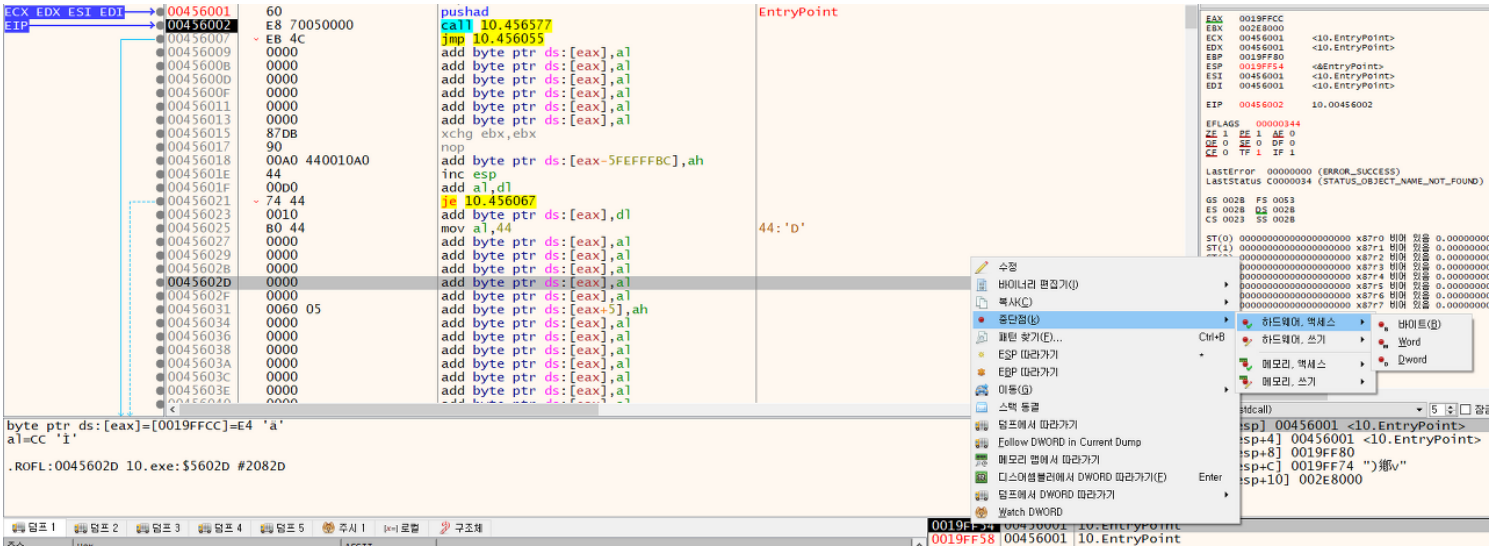
wonlf.tistory.com

위 링크를 참고 하도록 하고

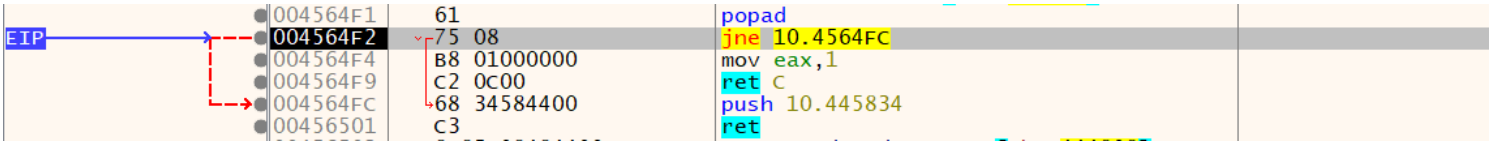
디버거로 열어서 파일을 확인하면,



UPX처럼 pushad가 반겨주고 있다.

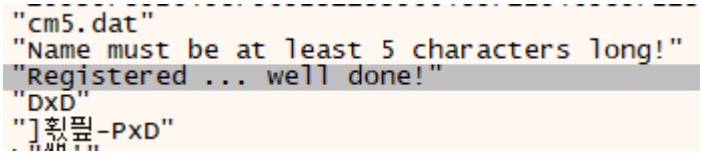


위 링크와 동일한 방법으로 pushad후, 스택에 하드웨어 브레이크 포인트를 걸어주고 OEP를 확인한다.



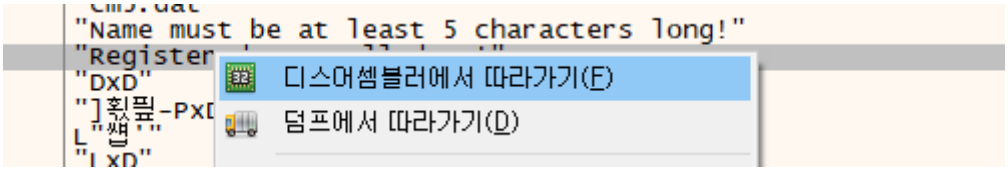
popad가 나오는 모습이고 아래에 push 00445834를 하고 ret까지 실행하고 나면, 실제 EP로 오게 된다.

이제 문자열 찾기를 통해 '등록성공' 구문을 찾아본다.

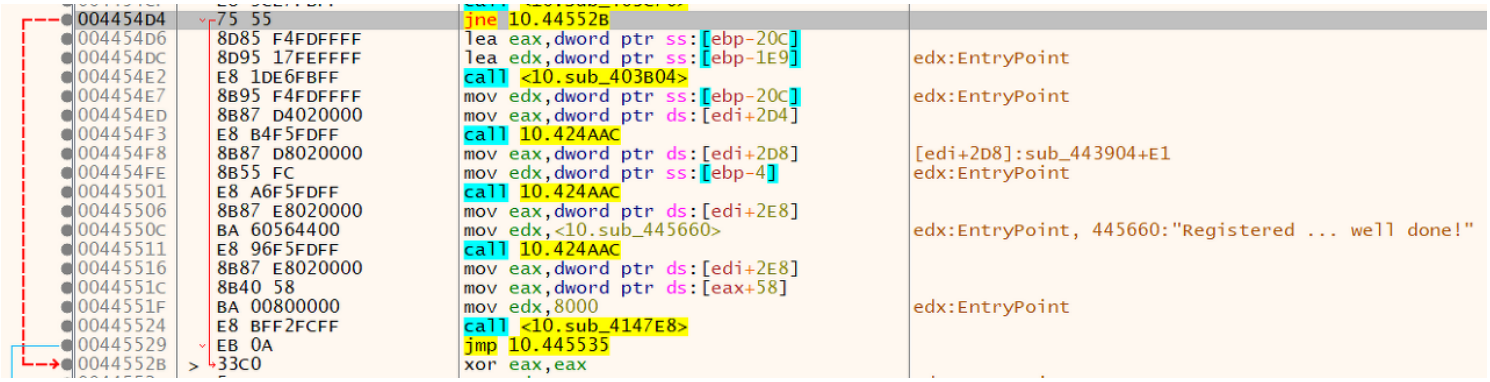


"Registerd ... well done!" 이라는 성공으로 추정되는 문자열이 보인다.

이 문자열을 사용하는 구문을 찾기 위해 디스어셈블러에서 따라가기를 사용한다.



그럼 이러한 구문이 보이는데,



등록 성공으로 가려면 jne에서 점프를 뛰지 말아야 함으로 jne구문을 분기점으로 볼 수 있다.

그렇기 때문에 OEP "00445834" + jne의 OPCODE "7555" 가 플래그가 되겠다.

"004458347555"