리버싱, 이 정도는 알아야지 2번 챌린지

1. 현재 실행 파일 상태

- 시작하자 마자 종료

2. 달성해야할 실행파일의 상태

- 실행 파일이 “PrintMe”를 cmd창에서 출력하게 할 것

3. 상태 달성 방안

- ollyDbg를 통해 실행파일을 리버싱해 출력되지 않는 원인을 파악, 그 후 어셈블리어를 수정하여 원인제거를 통해 원하는 상태 달성

4. 상태 달성 과정

▼ main 함수 찾기

- 디버거에 올라온 어셈블리어는 main 함수부터 시작하는 것이 아닌 startUp code 부터 시작하므로 main함수를 찾아야 함
- 컴파일 환경에 따라 달라지므로 그에 맡게 정보를 찾아야 함

▼ 라이브러리 로드 에러

- 리버싱을 진행하던 중 존재하지 않는 DLL을 로드하는 오류가 발생하고, 그 여파로 JNZ 코드에서 점프가 수행되지 않음. 그 결과 리턴으로 직행하여 코드가 종료됨
- DLL을 로드하는 CALL을 제거함으로써 해결
- 디버거에서 에러 내용을 확인함으로써 어떤 에러인지 파악할 수 있었음

▼ 과도한 슬립시간

- JNZ 코드를 통해 점프해서 도착하는 주소를 sleep 코드 바로 뒤 코드로 설정함으로써 sleep을 방지

▼ 잘못된 문자열 출력

- 원래의 HEX값에 2를 추가로 더함으로써 잘못된 문자열이 출력되게함

- 메모리에 있는 데이터에서 꺼낸 값(문자열의 문자)을 저장한 레지스터에 2를 더하는 코드를 제거함으로써 해결

5. 무엇을 얻었는가?

- 어셈블리어에 대한 추가적인 이해
- 디버거를 익숙하게 사용하는 것에 조금 더 다가감