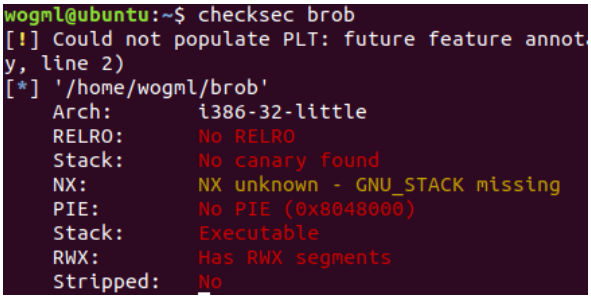
3S CTF

PWN-Brob

SWING 32 기 한재희

포너블을 풀기 위한 준비로 우분투 안에서 pwngdb 를 깔려고 했는데 마지막
단계인 ./setup.sh 여기서 자꾸 오류가 난다..

그래도 일단 checksec 명령어를 사용해서 한번 분석해보자.



Arch : 아키텍처로 32 비트 리틀 엔디언 시스템

RELRO : 동적 링크 라이브러리의 Global Offset Table 이게 쓰기 가능한 상태인데 이게
오버라이팅 공격에 취약할 수 있다고 한다.

Stack : 스택 버퍼 오버플로 공격에 취약할 수 있다고 한다.

NX : 스택의 실행 권한 여부를 알 수 없어서 쉘코드 실행 공격에 취약할 수 있다.

PIE : 주소 공간 배치 무작위화가 적용되지 않아서 주소 예측 공격에 취약할 수 있다.

RWX : 메모리 영역에 읽기, 쓰기, 실행 권한이 모두 있어서 다양한 공격에 취약할 수 있다.

Stripped : 디버깅 정보가 포함되어 있어서 역공학 및 분석이 용이하다.

다양한 보안 취약점을 가지고 있어서 공격자에게 쉽게 악용될 수 있다고 한다.

우선 여기까지 밖에 진행하지 못했다.

플래그를 찾지 못했다.