Brob

32기 김효주

역시 포너블 문제이다 포너블 문제가 은근 많은 것 같은데 한 번도 안 풀어봐서 그냥 찍먹하는 수준으로 파일을 열어봐야겠다...

먼저 문제 설명을 보니 bof + probability라고 적혀 있다

Bof는 버퍼 오버플로우로, 메모리의 경계를 초과해 데이터를 쓰려고 할 때 발생하는 취약점이다

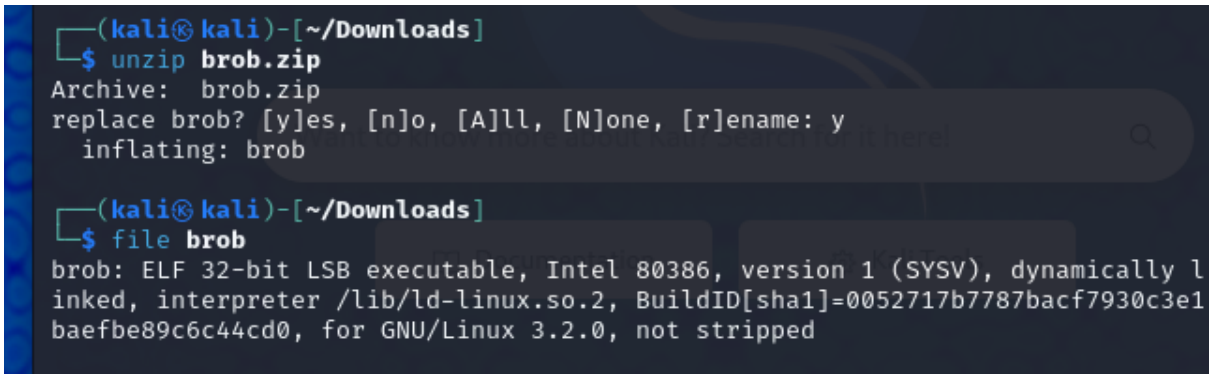
ctf 문제에서 버퍼 오버플로우가 언급된다면 메모리를 초과하게 입력해 악용해야 한다고 한다

다음으로 확률...?은 구글링해도 잘 안 나오는데, 여러 번 시도해봐야 한다는 뜻일까? 잘 모르겠다

아무튼 문제 파일을 다운받아보자

역시 파일 형식이 안 보인다 일단 칼리로 열어보자

칼리에서 brob.zip을 다시 다운받고, 압축을 푼 다음 file 명령어를 사용해 파일 타입을 확인했다



이 파일은 32비트 리눅스 실행 파일인 ELF 파일이다

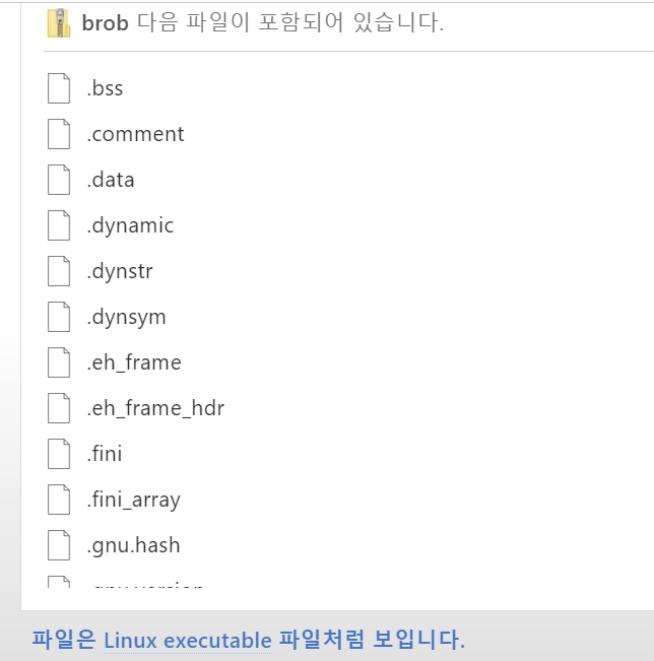
인텔 80386 아키텍쳐를 대상으로 만들어졌고, 동적으로 링크되어 있다고 한다

Not stripped는 디버깅에 유용한 심볼 정보가 포함되어 있다는 것을 의미한다

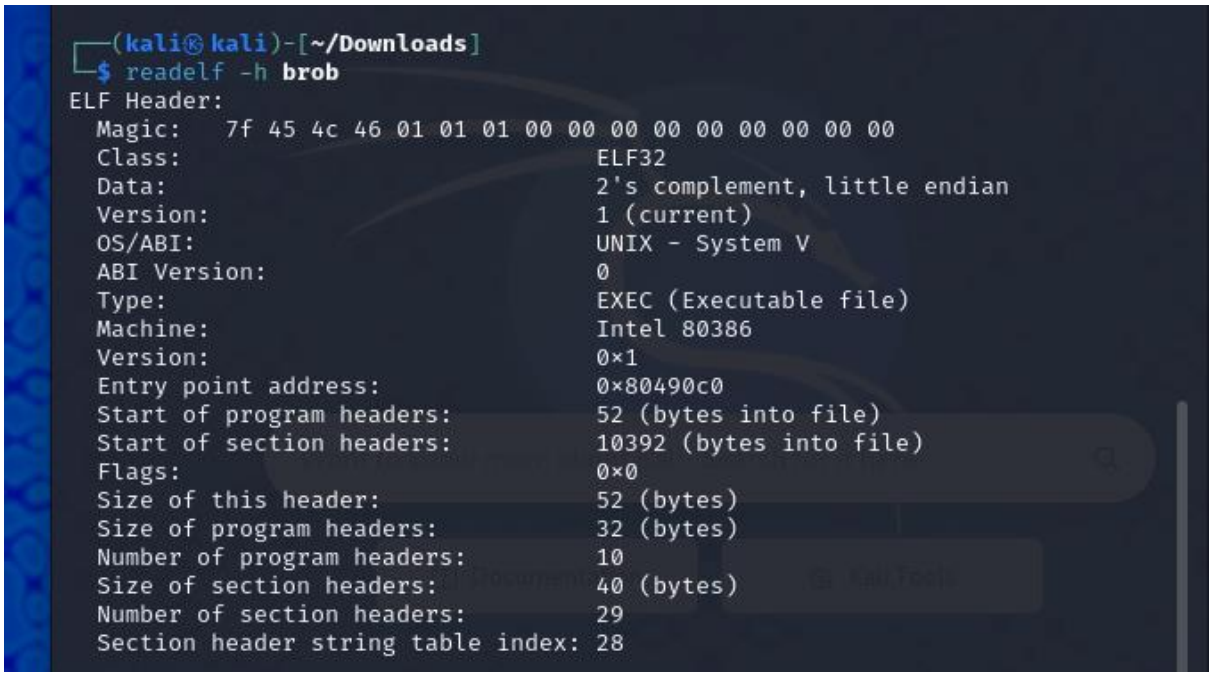
ELF 파일이라는 것을 확인했으니 파일을 열어보자

ELF 파일 변환 사이트가 있길래 이용해 열어보니 어떤 파일들이 포함되어있는지 보여주었다

근데 그 뿐 뭐가 더 없어서 다시 리눅스로 돌아갔다



이제 파일의 헤더 정보를 readelf -h 명령어를 이용해 확인해보자

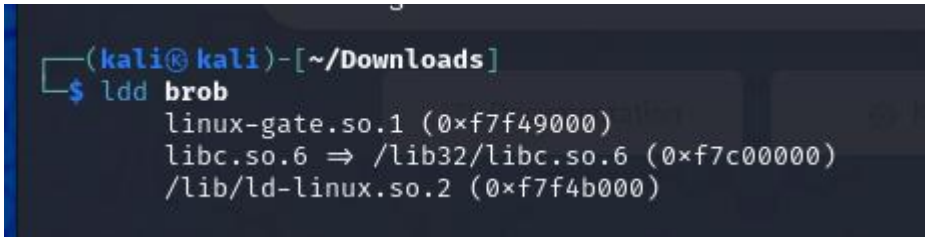


- 파일 타입: 32비트 ELF 실행 파일
- 아키텍처: Intel 80386 (x86)
- 엔디안: 리틀 엔디안
- Entry Point 주소: 0x80490c0 (프로그램 시작 주소)
- 프로그램 헤더: 10개
- 섹션 헤더: 29개

별다른 건 찾지 못했다

이제 이 바이너리가 사용하는 라이브러리를 확인해보자

종속된 라이브러리의 취약점을 활용해 공격이 가능할 수 있기 때문에 확인하는 거라고 한다



brob 파일이 실행될 때 필요한 주요 라이브러리는 다음과 같음을 확인할 수 있다

- libc.so.6: 표준 C 라이브러리 (/lib32/libc.so.6)
- ld-linux.so.2: ELF 파일 로더 (/lib/ld-linux.so.2)
- linux-gate.so.1: 커널에서 제공하는 가상 라이브러리

어떤 보안 매커니즘을 사용하는지 알아보기 위해 checksec 명령어로 확인해보자

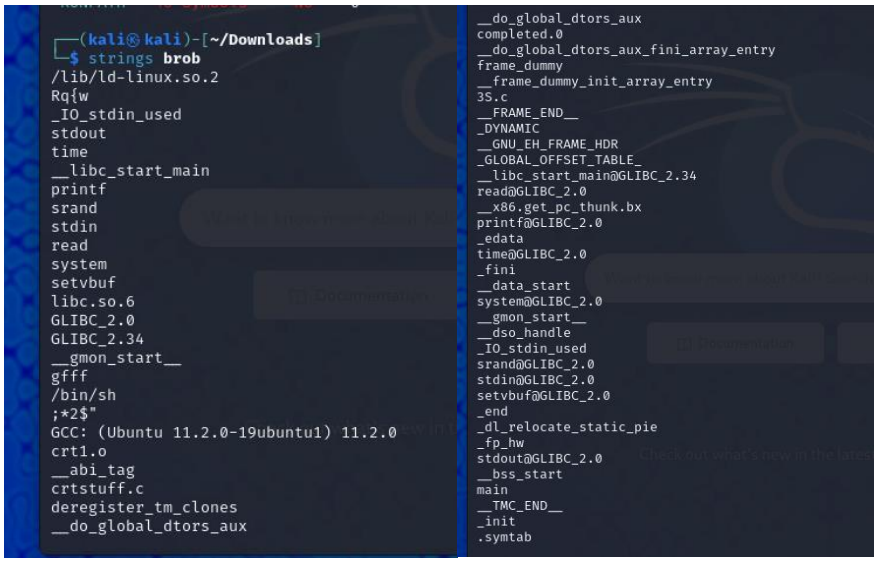
brob 파일의 보안 메커니즘이 거의 없다는 점을 확인할 수 있었다

- RELRO: 미적용 (No RELRO)
- 스택 카나리: 없음 (No canary found)
- NX (Non-Executable Stack): 비활성화 (NX disabled)
- PIE (Position Independent Executable): 미적용 (No PIE)

버퍼 오버플로우 같은 취약점 공격에 취약하므로 그걸 이용해 공격할 수 있는 것 같다

파일에 포함된 문자열을 확인해 혹시 쓸만한 정보가 있는지 찾아보자

이건 걍 맨 처음에 사이트에서 열었던 거랑 똑같이 보이는 듯



구글링하면서 포너블 문제 풀이시 필요한 명령어들을 입력하고 분석해보았는데

그 이상 어떻게 문제를 풀어야 할지 모르겠다