달고나 문서 이런 거를 읽어라?

시스템해킹의 핵심은 root권한을 따는 것. 그것이 buffer over flow를 통해 많이 시행이된다.

GDB명령어

-disas main을 하면 메인함수의 어셈블리어를 볼수가 있다.

에필로그랑 프롤로그??

굉장히 어렵군.

레지스터들이 어떤 역할을 하는지를 익혀야한ㄷ?

B \*main+64 이게 뭔뜻?

I r

I b

이런 것

그리고 d를 누르면 break point가 전부 초기화

D 그리고 숫자를 누르면 특정 break point만 삭제가능

하아 어렵군

Continue는 다음 break point로 넘어가는 명령어

R “~~”를 하면 ~~가 argument로 넘어가는듯

Ni는 다음번 한 줄?

Si를 하면 함수 안으로 들어가는 것

어셈블리어에 익숙해져야지 overflow공격을 제대로 할 수가 있다.

오늘 과제는 어셈블리어 중심으로 보고 레지스터, 메모리구조를 핵심적으로 보면 된다. 분석하는 것처럼 보는 것을 요구하진 않지만, 흠…뭐 명령어 위주로 봐야하는..? 실습을 해봐라?

그 git은 5과까지 1과는 그냥 거의 무시

근데 달고나는 27까지

에 근데 왜 안되지…gbd 플러그인 설치한거 실행이 다ㅡㄹㄴ데

뭐지 왜 32bit에서는 register에 저장 안하고 stack을 통해서 인자를 전달??