#stage1

텍스트이(가) 표시된 사진

자동 생성된 설명

//cmp jmp에서 같지 않으면 110줄로 넘어간다.

//110번째줄에서 "no.. T.T...you're fool.." 출력되고

//만약 같다면 "Wow! you're so smart!" 출력된다.

//

텍스트이(가) 표시된 사진

자동 생성된 설명

//따라서 cmp는 분기점이므로 I r 명령어를 써서 내부를 보면 비교를 했던 eax와 edx의 값을 확인할 수 있다.

텍스트이(가) 표시된 사진

자동 생성된 설명

+

텍스트이(가) 표시된 사진

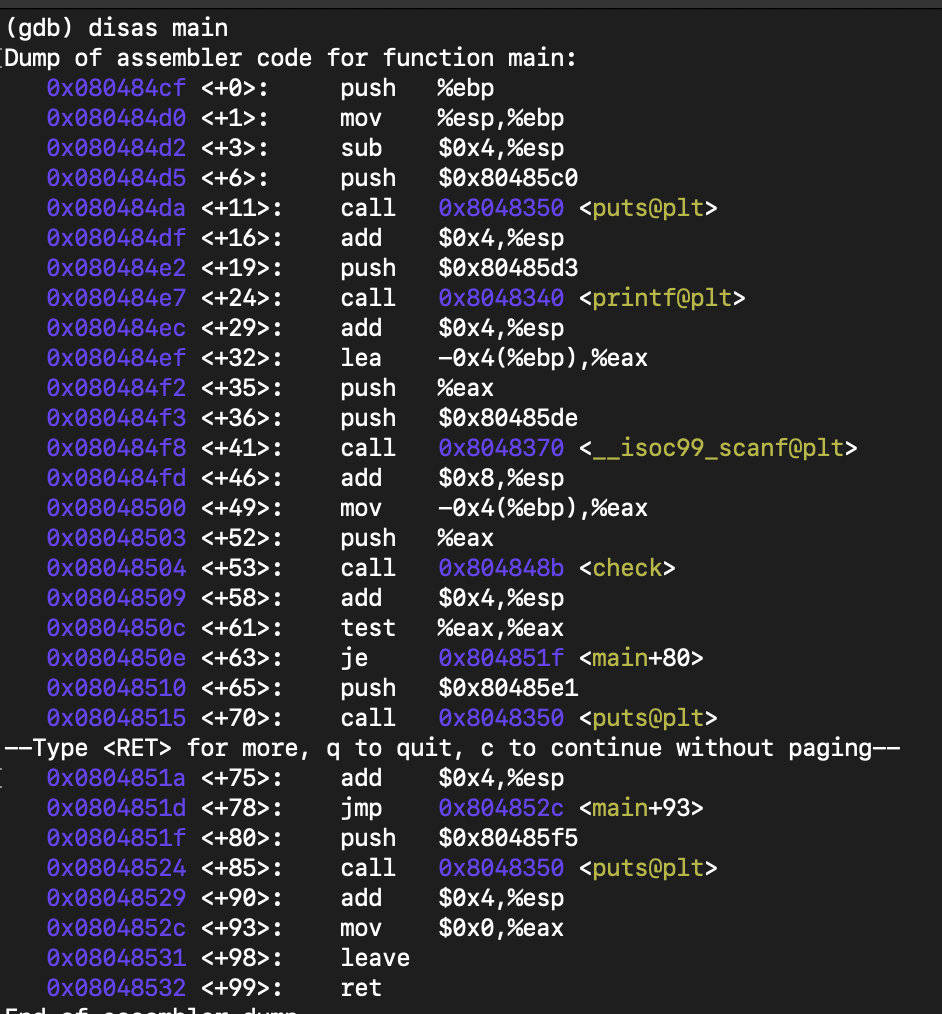
자동 생성된 설명

//eax에는 scanf에서 입력했던 값이 들어있고 edx에는 비밀번호가 들어있다.

//따라서 edx에 있는 값을 비밀번호로 넣을 수 있다.

Pw: 201821274

#stage2



//scanf를 받고 check 함수를 부른다.

//eax값이 0인지 확인하고 80번째 줄에서 "GOOD you're smart"를 출력하고 아니면 "You're fool!!!!!!!!"이 출력된다.

텍스트이(가) 표시된 사진

자동 생성된 설명

//check라는 함수로 들어가기 때문에 check함수 내부를 본다.

//cmp je가 분기점이므로

//breakpoint를 49번째 줄에 넣어주고 실행을 시킨다.

텍스트이(가) 표시된 사진

자동 생성된 설명

//I r 명령어로 분기점에서의 eax이 비밀번호임을 알 수 있다.

텍스트이(가) 표시된 사진

자동 생성된 설명

//eax에 비밀번호가 들어있는걸 알 수 있다.

Pw: 980303

#stage3

텍스트이(가) 표시된 사진

자동 생성된 설명

텍스트이(가) 표시된 사진

자동 생성된 설명

//0x804a040을x/s하면 fBUlTHaHTgHH\_BGpTEwRE\_WEAQWRWRERE\_WRYGTOBRU3G\_34HBTEEERtnOeb?ge

이 나온다.

//+79~+83 줄에서 3개씩 건너뛰어야 비밀번호가 있다는 것을 알 수 있어 if i%3==0을 써서 비밀번호를 구한다.

텍스트이(가) 표시된 사진

자동 생성된 설명



텍스트이(가) 표시된 사진

자동 생성된 설명

#조사과제

1. 리눅스 특수 권한 조사 및 실습

텍스트이(가) 표시된 사진

자동 생성된 설명

파일 권한에서

텍스트, 점수판이(가) 표시된 사진

자동 생성된 설명

-사용자 권한의 x-> s(S:실행권한이 없을 경우): SetUID

: 소유자만이 접근 가능한 파일을 일반 유저도 접근할 수 있게 한다.

: 슈퍼유저만 접근 가능한 파일이나 명령어에 대해 일반유저가 접근이 필요할 때 사용

: setuid가 설정된 파일은 실행 순간만 그 파일의 소유자 권한으로 실행

Ex) rws r-x r-x

텍스트, 점수판이(가) 표시된 사진

자동 생성된 설명

-그룹 권한의 x->s (S:실행권한이 없을 경우): SetGID

: 소유 그룹만 접근 가능한 파일에 일반 유저로 접근할 수 있게 한다.

Ex) rwx rws rwx

: 설정한 디렉터리에 새로 생성된 파일들은 디렉터리 그룹 소유권이 아닌 파일 생성자의 그룹 소유권을 얻음.

텍스트, 점수판이(가) 표시된 사진

자동 생성된 설명

-다른 사용자 권한의 x->t (T:실행권한이 없을 경우): Sticky bit

: 특정 디렉토리를 누구나 자유롭게 사용할 수 있게 한다.

파일 생성은 누구나 가능하지만 삭제는 생성한 유저와 디렉토리 소유자만 가능하다.

: 특정 디렉터리를 누구나 자유롭게 사용하기 위해 사용

: 디렉터리에 적용하면 디렉터리 소유자나 파일 소유자 또는 관리자가 아닌 사용자들은 파일을 삭제하거나 이름을 변경하지 못하지만 파일 또는 디렉터리 생성은 가능

Ex) rwx rwx rwt

텍스트, 점수판이(가) 표시된 사진

자동 생성된 설명

-특수권한과 일반권한 차이

일반권한은 rwx rwx rwx 총 9bit이다.

특수권한은 -rwx -rwx -rwx 총 12bit이다.

1. 함수 프롤로그, 에필로그 조사

-함수 호출시:

1. 함수가 사용할 매개변수를 스택에 넣고 함수 시작지점으로 점프
2. 함수 내에서 사용할 스택프레임을 설정 (프롤로그)
3. 함수의 내용을 수행
4. 수행을 마치고 처음 호출한 지점으로 돌아가기 위해 스택 복원 (에필로그)

-스택 프레임: 한 함수가 호출되면 스택에는 함수의 매개변수, 함수에서 선언된 지역 변수등이 저장되는데 그 영역을 스택 프레임이라 한다.

텍스트, 전자기기이(가) 표시된 사진

자동 생성된 설명

-함수 프롤로그

: ebp(베이스 포인터)를 스택에 저장하고 esp(현재 스택포인터)를 ebp에 저장한다.

push ebp

mov ebp,esp

-함수 에필로그

: esp를 ebp로 복구한뒤 ebp를 복구해준다.

mov esp,ebp

pop ebp

pop eip

jmp eip

#공유 라이브러리 만들기

텍스트이(가) 표시된 사진

자동 생성된 설명

//소스코드를 오브젝트 파일(.o)로 바꾼다.

텍스트이(가) 표시된 사진

자동 생성된 설명

//오브젝트 파일을 공유 라이브러리(.so)로 만들어준다.

//소스코드를 컴파일한다.

///.파일명을 통해 실행시킨다

텍스트이(가) 표시된 사진

자동 생성된 설명

// ldd로 라이브러리 로드 확인한다.