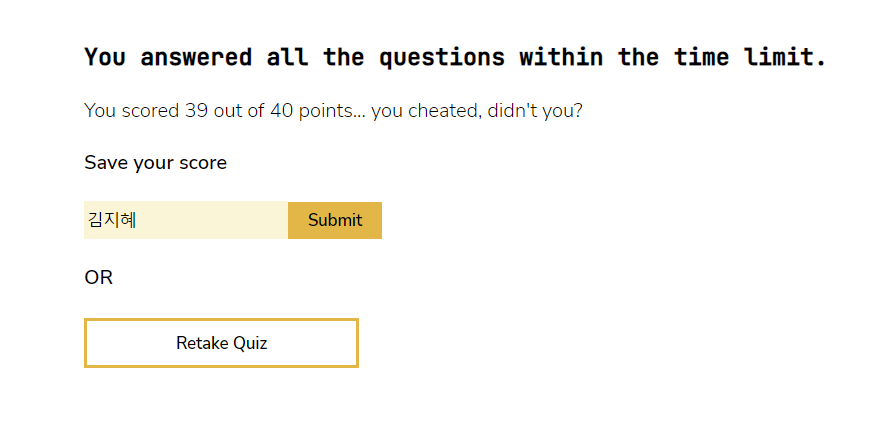
2022 CAT-CERT 스터디 보고서

컴퓨터정보공학부 202221168 김지혜

2022.04.29 #System\_study-1

퀴즈 문제 만점받기..



공유 라이브러리 만들기 및 실습

1. lib.c파일을 만든다

#include <stdio.h>

int add(int a,int b){

int result = 0;

result = a+b;

printf ("add : %d + %d = %d",a,b,result);

return result;

}

2.” gcc -fPIC -c lib.c”을 통해 오브젝트파일을 만든다

(공유라이브러리 함수로 컴파일 할 때는 독립한 코드로 만들기 위해 -fPIC 옵션을 이용한다)

텍스트이(가) 표시된 사진

자동 생성된 설명

3.gcc의 -shared 옵션을 이용해서 공유라이브러리 파일을 만든다

텍스트이(가) 표시된 사진

자동 생성된 설명

4.위에 lib.c에 만든 add함수를 포함하여 소스코드파일을 만든다

#include<stdio.h>

int main() {

int res;

res=add(2,3);

printf("\n result is %d \n", res);

}

5.” gcc -o file file.c -l myshared -L ./”로 컴파일을 한다

**텍스트이(가) 표시된 사진

자동 생성된 설명**

**6.ldd ./file 를 실행시켜준다(라이브러리 로드 확인)**

**->라이브러리 파일을 찾을 수 없다고 뜬다**

**텍스트이(가) 표시된 사진

자동 생성된 설명**

**7. “LD\_LIBRARY\_PATH” 환경변수를 이용하여 공유라이브러리를 설정한다**

**1)’pwd’로 현재 설정되어 있는 라이브러리 경로를 조회한다**

**텍스트이(가) 표시된 사진

자동 생성된 설명**

**2)”** **export LD\_LIBRARY\_PATH=$LD\_LIBRARY\_PATH:** **/home/wlgp9324/system\_lib”를 입력하여 변수값을 지정하여 공유라이브러리의 경로를 설정한다.**

**텍스트이(가) 표시된 사진

자동 생성된 설명**

**8.최종 출력**

**텍스트이(가) 표시된 사진

자동 생성된 설명**

Stage 1,2,3 풀이 작성

Stage1:

텍스트이(가) 표시된 사진

자동 생성된 설명

텍스트이(가) 표시된 사진

자동 생성된 설명

Eax에 scanf를 통해 내가 입력한 값을 받고

Cmp에서 eax와 edx를 비교한다

->edx에 내가 찾는 비밀번호가 담겨있다는 것을 알 수 있음

Cmp에 break를 걸고 실행시키고,

레지스터 상태 정보를 출력하면 edx에 ‘201821274’가 있는 걸 알 수 있다

Stage2:

텍스트이(가) 표시된 사진

자동 생성된 설명

텍스트이(가) 표시된 사진

자동 생성된 설명

main함수에서는 비교하는 명령어가 없기 때문에 check함수의 어셈블리 코드를 본다

check함수에는 cmp 명령어가 있고 cmp 명령어가 있는check+49에 break를 걸면 eax에 찾는 비밀번호가 있다

Stage3:

텍스트이(가) 표시된 사진

자동 생성된 설명

텍스트이(가) 표시된 사진

자동 생성된 설명

반복문을 돌면서 eax에 있는 값이 3씩 증가함

Cmp에 al의 값은 윗줄의 eax값이고

그 eax값은 0x804a040에 3씩 더한 주소에서 가져온 문자값이다

‘0x804a040’의 길이 만큼 반복문을 돌면서 3의배수인 부분만 값만 가져온다

-> for(i=0; i<len; i++){

If(i%3==0){

Printf(“pw[i]”);

}

}

으로 나타낼 수 있다.

리눅스 특수권한 조사 및 실습

rws r-x r-x

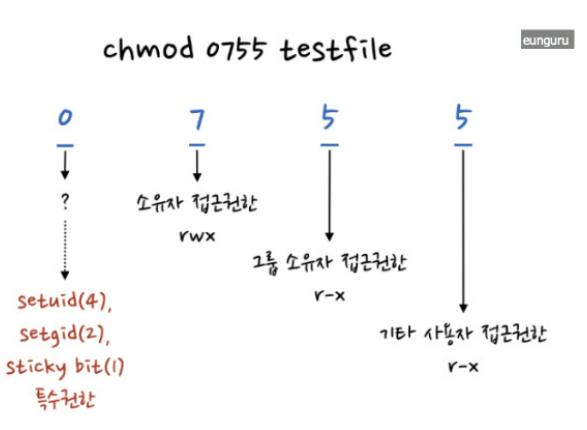
* s가의미하는 것이 특수한 권한

(소유자, 그룹, 다른 사용자에 대한 권한에 어떤자리에 위치하느냐에 따라 용도가 달라짐)

|  |  |  |
| --- | --- | --- |
| SetUID | SetGID | Sticky bit |
| 소유자만 접근 가능한 파일을 일반 유저도 접근할 필요가 있을 때 사용함  (실행한 순간만 파일의 소유자 권한으로 실행함)  User권한의 접근권한(x)자리에 x대신에s가 들어가면 SetUID  \*\*setuid비트가 설정되어있으면 사용자접근권한의 실행권한 자리에 실행권한이 있으면 소문자s, 없으면 대문자S  권한을 읽을땐 기호(u+s)이용하거나 맨 앞에 숫자 ‘4’를 붙인다  Ex)rws rw- r—  =4764  \*\*root권한이 필요없는 프로그램에 소유주가setuid설정된 경우 일반 사용자로 접근하는 경우도 실행가능해지기 때문에 보안상 취약  \*패스워드 설정, 변경시 사용  일반 사용자가 읽을 수 없는 파일 읽기 | 소유그룹만 접근 가능한 파일에 일반 유저도 접근이 필요할 때 사용함  그룹권한의 접근권한(x)자리에 x대신 s가 들어가며 SetGID  \*\*setgid비트가 설정되어 있으면 그룹 소유자 접근 권한자리에 실행권한이 있으면 소문자s, 없으면 대문자 S  권한을 읽을땐 기호(g+s)를 이용하거나 맨 앞에 숫자 ‘2’를 붙임  Ex)rwx rws rw-  =2776 | 특정 디렉토리를 누구나 자유롭게 사용할 수 있도록 하는 것(공용 디렉토리에 사용함)=>공유모드  단, 파일이나 디렉토리 생성은 누구나 가능하지만 삭제는 생성한 유저와 디렉토리 소유자만 가능함  일반 사용자 권한의 접근권한(x)자리에 x대신 t가 들어가면 Sticky bit  \*\*sticky bit가 설정되어 있으면 기타 사용자 접근 권한의 실행 권한 자리에 실행권한이 있으면 소문자 t 없으면 T  권한을 읽을땐 기호(o+t또는 u+t)를 이용하거나 맨 앞에 숫자 1을 붙임  Ex)r-x rw- rwt  =1567 |

특수권한 비트 설정 파일 검색시

-find[디렉토리경로]-perm[접근권한]-ls



SetUID

텍스트이(가) 표시된 사진

자동 생성된 설명

SetGID

텍스트이(가) 표시된 사진

자동 생성된 설명

Sticky bit

텍스트이(가) 표시된 사진

자동 생성된 설명

함수 프롤로그, 에필로그 조사

프롤로그

:함수가 호출될 때 스택프레임을 구성해주는 작업

1. RET(복귀주소)부터 스택 밑(메모리가 가장 높은)에 넣는다
2. SFP는 그 위에, SFP밑부분에 ebp 설정
3. esp값에 ebp 주소 값을 넣는다(push)

에필로그

: 종료되어 나를 호출한 함수로 돌아갈 때 스택을 정리하는 과정

Leave

mov %ebp %esp

pop %ebp

esp레지스터에 ebp주소를 넣고, esp=ebp

* 프롤로그의 3번 상태

ebp를 스택프레임에서 꺼냄

* 프롤로그의 1번 상태

Ret

pop %eip

jmp %eip

esp가 있는곳 (sfp와 ret 사이)에서 4바이트를 복사해 eip에 담게 된다=> ret에 담긴 스택주소를 갖게됨->esp+4

eip레지스터를 스택에서 꺼낸다

다음명령의 주소로 점프->eip에 저장된 주소(ret)로 이동