2025.09.24

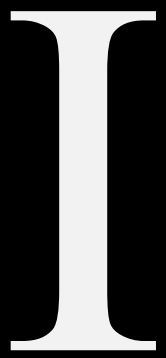
ROP & OOB

가디언 시스템 보안 & 취약점 분석 세미나 3.1

Guardian 2025

Libc

Recap & Details



Libc

A brief recap

C를 위한 라이브러리

Syscall의 wrapper 역할

Exploit의 main target 중 하나

Libc

How does it work?

로더가 런타임에 메모리에 할당

mmap과 유사한 함수 이용

ASLR로 매번 위치가 바뀐다.

→ Leak is necessary

Libc

How does it work?

libc 내부 함수들의 offset 일정

base + offset으로 함수 접근

ASLR이 있어도 base의 하위 12비트 고정

0x??...?000 꼴이다.

pwndbg의 vmmap

Base를 구했는데 000으로 안 끝나면 잘못 구했다는 뜻

실습 [rop]

dreamhack.io/wargame/challenges/354

저번 실습 문제의 바이너리

ROP Techniques

Ret2Main, OneGadget, etc.

II

ROP

Ret2main

기회가 1번이면 ROP 어려움

return to main!

여러번 ROP가 가능하다

ROP 中 RTL

Return To Libc

원하는 gadget이 없다면?

Return To Libc!

libc에 좋은 gadget이 차고 넘친다. system, /bin/sh 까지 다 있다.

굉장히 유명하고 간편함

대신 libc의 시작 주소를 알아야 함.

ROP 中 RTL

One_gadget

libc 에 좋은게 많으니 한번에 쉘을 따자

onegadget ./libc.so.6

조건만 맞으면 한번에 쉘이 나온다.

libc의 버전이 높을수록 onegadget의 제약 조건이 많아진다

Out of Bound

Concept and Exploit

III

Out-of-Bound

PoC

```c
#include <stdio.h>

int main() {
    unsigned long long arr[4] = {1, 2, 3, 4};
    printf("===Array elements===\n");
    for(int i = -1; i < 10; i++) {
        printf("[%d] %x\n", i, arr[i]);
    }
    return 0;
}
```

c에서는 음수 인덱스 접근이 가능하다.

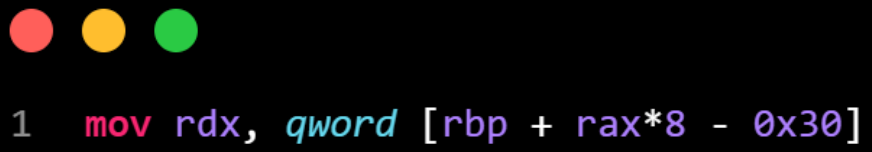
Out-of-Bound

PoC

```
===Array elements===
[-1] 0
[0] 1
[1] 2
[2] 3
[3] 4
[4] 0
[5] 1d315b00
[6] 1
[7] 9636dca8
[8] 3cad0a10
[9] 401146
```

Out-of-Bound

PoC



rax가 oob라면?

어셈블리는 주어진 대로 실행한다.

Boundary check

OOB

요즘 언어는 array-like DT에서 지원

High level language

C는 그런 거 없음

OOB Exploit

AAR / AAW primitive

OOB가 발생한 맥락에 따라 다름

read → AAR

write → AAW

실습 [stacknote]

dreamhack.io/wargame/challenges/1997

I wonder what's below the stack?

Homework [Platform 9½]

dreamhack.io/wargame/challenges/2103

Out of Bound and ROP

2025.09.24

Q&A

질문이 있다면 하십시오

Guardian 2025

2.5cm-2.5cm 떨어진 제목 36px

제목 하단의 부제목 18px

3.5cm 떨어진 내용 1 32px

좌측으로 0.5cm 떨어진 내용 하단의 설명 18px

3.5cm 떨어진 내용 2 32px

좌측으로 0.5cm 떨어진 내용 하단의 설명 18px

3.5cm 떨어진 내용 3 32px

좌측으로 0.5cm 떨어진 내용 하단의 설명 18px

1cm-1cm 떨어진 주석 12px ㅇ

1cm-1cm 떨어진 주석 12px

2.5cm-3.5cm 떨어진 제목 36px

제목 하단의 부제목 18px

3.5cm 떨어진 내용 1 32px

```
Git init
Git status
Git add text.txt
Git add .
Git commit
Ctrl+C
Git commit -m “genesis”
Git log
Git log --oneline
```

```
Git add .
Git reset .
Git commit -m “add README”
Git log --oneline -n 3
Git commit –a –m “hello”
```

1cm-1cm 떨어진 주석 12px

1cm-1cm 떨어진 주석 12px

중심에서 0.3cm 떨어진 소속 18px