

2025.09.17

Buffer OverFlow

가디언 시스템 보안 & 취약점 분석 세미나 2.1

임준서

Shell Code
as ASM

I

목표

프로그램의 흐름을 탈취하자

원하는 코드를 실행하고 싶다

가장 좋은 도구는?

원도우는 PowerShell, 리눅스는 Shell(/bin/shell)

Shell

/bin/sh

```
zirajs@ubuntu:~$ sh  
$  
zirajs@ubuntu:~$ /bin/sh  
$ /bin/sh  
$  
$
```

쉘도 프로그램이므로 nano {file} 같은 식으로 실행 가능하다

쉘 안에서 쉘 실행도 가능

Syscall

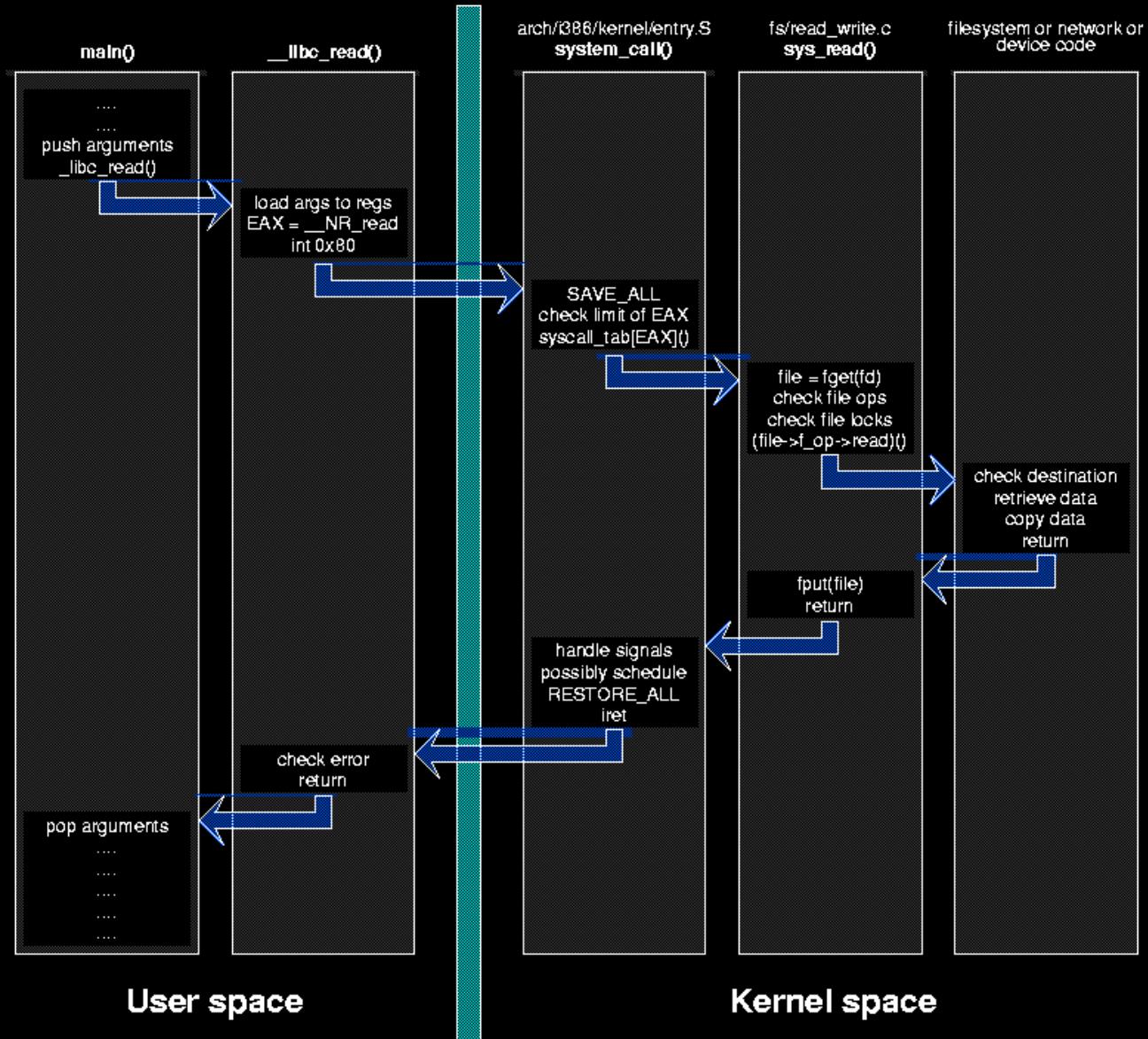
커널에 필요한 기능 요청

프로그램이 read, write 하고 싶음

근데 그건 권한 없는데?

Syscall로 직접 호출하자

Syscall



시스템한테 “해줘” 하는 거임
도라에몽 나 이거 출력해줘

Syscall

커널에 필요한 기능 요청

겁나 많다.

필요할때 찾아보자

reference

chromium.googlesource.com/chromiumos/docs/+/master/constants/syscalls.md

실습 [shell_basic]

dreamhack.io/wargame/challenges/410

CTF에서 적어도 한 문제는 나오는 클래식

System()

System("/bin/sh")

Shell로 child process를 생성

```
execl("/bin/sh", "sh", "-c", command, (char *) NULL);
```

Buffer OverFlow

Hello, world!



Ret / Leave

function call

[ret]
pop rip;

[leave]
mov rsp, rbp;
pop rbp;

Ret2Func

gets(), strcpy() = Shell

RBP

RBP - 0x20 =

Prog. Stack

Return Addr
SPO

Buffer [0x20]

Ret2Func

gets(), strcpy() = Shell

Win Addr = 0x403400

RBP

RBP - 0x20 = RSP

Prog. Stack

	AAAAAAA
	AAAAAAA
Return Addr	AAAAAAA
SPO	AAAAAAA
	AAAAAAA
Buffer [0x20]	AAAAAAA

Ret2Func

gets(), strcpy() = Shell

Win Addr = 0x403400

코드 흐름을 탈취

RBP

RBP - 0x20 = RSP

Prog. Stack

	AAAAAAA
	AAAAAAA
Return Addr	00403400
SPO	AAAAAAA
	AAAAAAA
Buffer [0x20]	AAAAAAA

Ret2ShellCode

+ use Shellcode

If Win 함수가 없다

RBP

스택에 명령어(쉘)를 올리자

이후 그 스택 위치로 return

RBP - 0x20 = RSP

Prog. Stack

	AAAAAAA
	AAAAAAA
Return Addr	00403400
SPO	AAAAAAA
	AAAAAAA
Buffer [0x20]	AAAAAAA

Ret2ShellCode

+ use Shellcode

shell code 위치로 ret

RBP

RBP - 0x20 = RSP

Prog. Stack

AAAAAAA	Stk Addr
AAAAAAA	AAAAAAA
Return Addr	Stk Addr
SPO	AAAAAAA
AAAAAAA	SomeCode
SomeCode	SomeCode
Buffer [0x20]	SomeCode

실습 [Ret2Shellcode]

notion에 업로드 된 Ret2Shellcode.zip

2025.09.17

Q&A

질문이 있다면 하십시오

임준서

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

1cm-1cm 떨어진 주석 12px