

2025.09.26

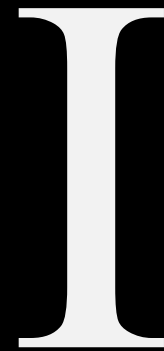
Hook & Command

가디언 시스템 보안 & 취약점 분석 세미나 3.2

Guardian 2025

Hook Overwrite

Free/Malloc Hook



Hook

Introduction

금융앱 "키보드 보안 프로그램"

키보드 입력 → (훅) → 암호화 → 은행 앱

Hook

Introduction

SetWindowsHookEx

요런 WinAPI 사용

Event 발생 → 목록에 있는 함수 호출

Llibc의 hook

glibc < 2.35 , ubuntu < 22.04

Free / Malloc hook 존재

exploit에서 자주 쓰여 glibc 2.35 부터는 지원 x



```
1 0x7ffff7fa61e0 <__malloc_hook>: 0x0000000000000000
2 0x7ffff7fa61e8 <__free_hook>: 0x0000000000000000
```

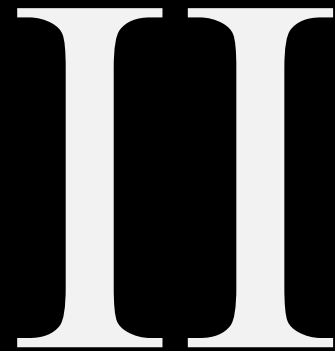
정확히는 glibc <2.34. 그러나 주로 stable 버전에 쓰이는 2.27, 2.35, 2.4x 만 고려

Homework [fho]

dreamhack.io/wargame/challenges/355

Misc Techniques

Command



Linux Commands

command separators

`command1 ; command2`

`command1, command2` 모두 실행

`command1 && command2`

`command1`이 성공(`exit status=0`)일 때만 실행

`command1 || command2`

`command1`이 실패(`exit status!=0`)일 때만 실행

`.....;/bin/sh`

Linux Commands

Command substitution

`command $(other command)`

`command `other command``

Linux Commands

Shell

`(command1 ; command2)`

Subshell

`{command1 ; command2}`

Current shell

`(cd /tmp; pwd) vs { cd /tmp; pwd; }`

Linux Commands

Pipelining

`command1 | command2`

`command1`의 `stdout` 을 `command2`의 `stdin`으로

`command1 |& command2`

+ `stderr` 추가

Linux Commands

Redirecting fd

```
command1 > filepath
```

open(filepath)를 stdout으로 사용

```
command1 n> filepath
```

open(filepath)를 n(fd)로 사용

Linux Commands

Redirecting fd

```
command1 < filepath
```

open(filepath)를 stdin으로 사용

```
command1 n< filepath
```

open(filepath)를 n(fd)로 사용

Linux Commands

Env variables

\$HOME = 기본 홈 디렉토리

~의 의미

```
export HOME=/tmp/fakehome
```

Linux Commands

Expansion

```
touch file{1,2,3}.txt
```

Homework [sane-env]

dreamhack.io/wargame/challenges/1274

2025.09.26

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

1cm-1cm 떨어진 주석 12px

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

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

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

