**Homework #1 & #2**

201511054 컴퓨터과학과 임현

**HW#1** : 슬라이더 4-11 페이지의 코드를 4-12의 whitelisting 방법을 이용하여 안전하게 변경하세요.

1. 리눅스 2.6 커널을 이용하여 코드를 작성하여 실행파일을 만든다.

2. 실행 파일을 이용하여 수업시간에 실험한 공격을 가한다.

**코드**

#include <stdio.h>

#include <stdlib.h>

int main(void)

{

char buffer[100];

char addr[100];

static char ok\_chars[] = "abcdefghijklmnopqrstuvwxyz"

"ABCDEFGHIJKLMNOPQSTUVWXYZ"

"123456788\_-.@";

gets(addr);

char \*cp = addr;

const char \*end = addr + strlen(addr);

for (cp += strspn(cp, ok\_chars); cp != end; cp += strspn(cp, ok\_chars))

{

\*cp = '\_';

}

sprintf(buffer, "mail -s \"First Letter\" %s < .bashrc", addr);

system(buffer);

return 0;

}

**공격 실행한 화면 캡처**



**공격이 실패한 이유**

기존의 코드는 모든 char를 다 허용했지만, whitelisting 방법을 이용한 코드는 액세스가 가능한 char들을 먼저 선언해줌으로써 ok\_char[]에 없다면, 허용하지 않습니다.

그래서 이 코드는 whitelist에 없다면, 그 문자를 ‘\_’로 바꾸기 때문에 프로그램이 정상 실행되지 않습니다.

**기타**

whitelisting 방법과 다른 방법으로는 blacklisting이 있으며, 이는 허용하지 않는 char들을 선언해줌으로써 이 char에 포함된다면, 허용하지 않습니다.

strspn함수 : 문자열에서 특정 문자로 구성된 문자열의 길이 구하기

**HW#2** : 슬라이더 4-15 페이지의 코드를 argc argv를 이용하여 login을 편하게 할 수 있는 easylogin 프로그램을 만들고 이를 공격에 이용하세요.

1. 리눅스 2.6 커널을 이용하여 코드를 작성하여 실행파일 easylogin을 만든다. 이 때 login의 옵션과 username을 자유롭게 입력 받을 수 있도록 한다.

2. 일반계정으로 root 계정에 패스워드를 입력하여 일반적인 방법으로 login을 먼저한 후에 logout 한다.

3. 일반계정에서 easylogin -f root 를 실행하여 패스워드 입력없이 바로 root계정에 login하도록 한다.

**코드**

#include <unistd.h>

int main(int argc, char \*argv[])

{

execl("/bin/login", "login",

"-p",

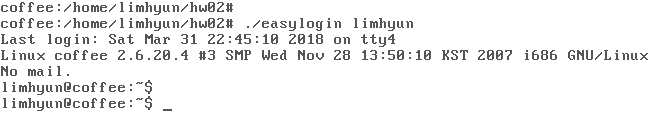
"-f", argv[1],

NULL);

return 0;

}

**공격 실행한 화면 캡처**



**공격이 성공한 이유**

login 명령어 옵션 중 -f 옵션은 login을 한 번 인증했으면 다시 인증할 필요가 없는 옵션이기 때문 입니다.

**기타**

login 옵션들

-f user : 이미 인증 절차를 거친 사용자라면, 지정한 user의 인증 절차를 무시

-h hostname : 로그인을 원격 로그인으로 인식하고 hostname으로 로그인을 시도

-p : logdin 실행할 때 이전 환경들을 그대로 사용하도록 getty 명령에 의해 사용

일반 계정에서 login 명령이 permission denied가 뜹니다.