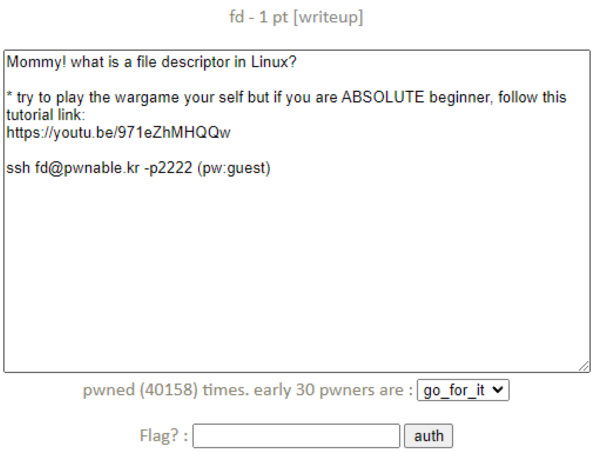
Pwnable.kr
- fd -

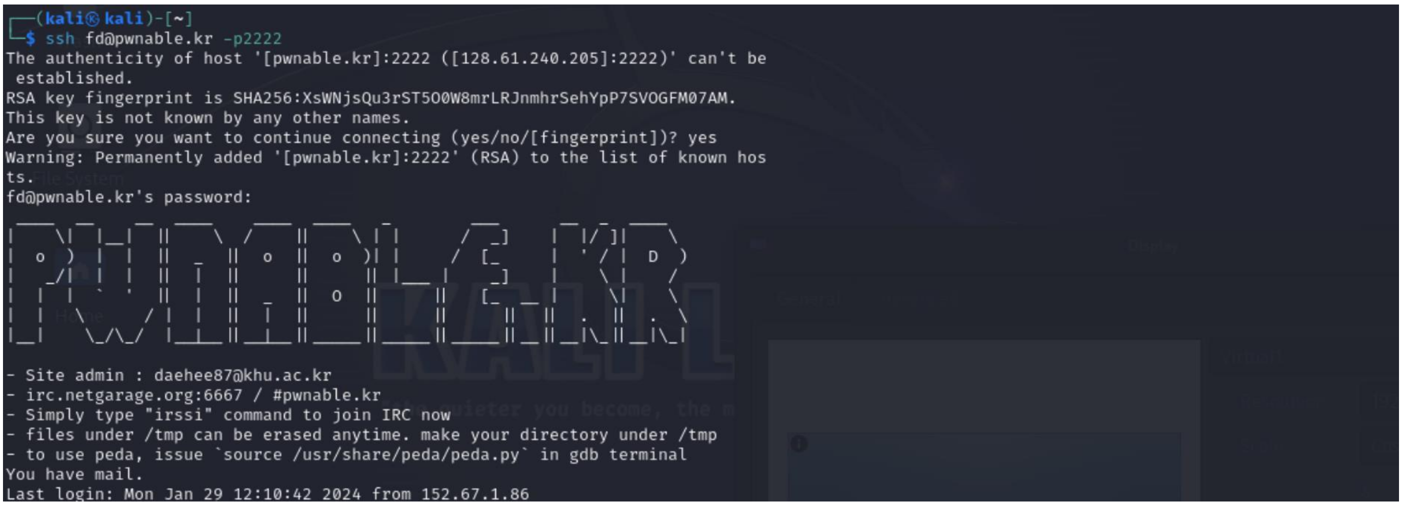
ssh fd@pwnable.kr –p 2222
pw : guest

0. 문제 살펴보기



문제에서 파일 디스크립터에 대한 이야기를 하고 있다.

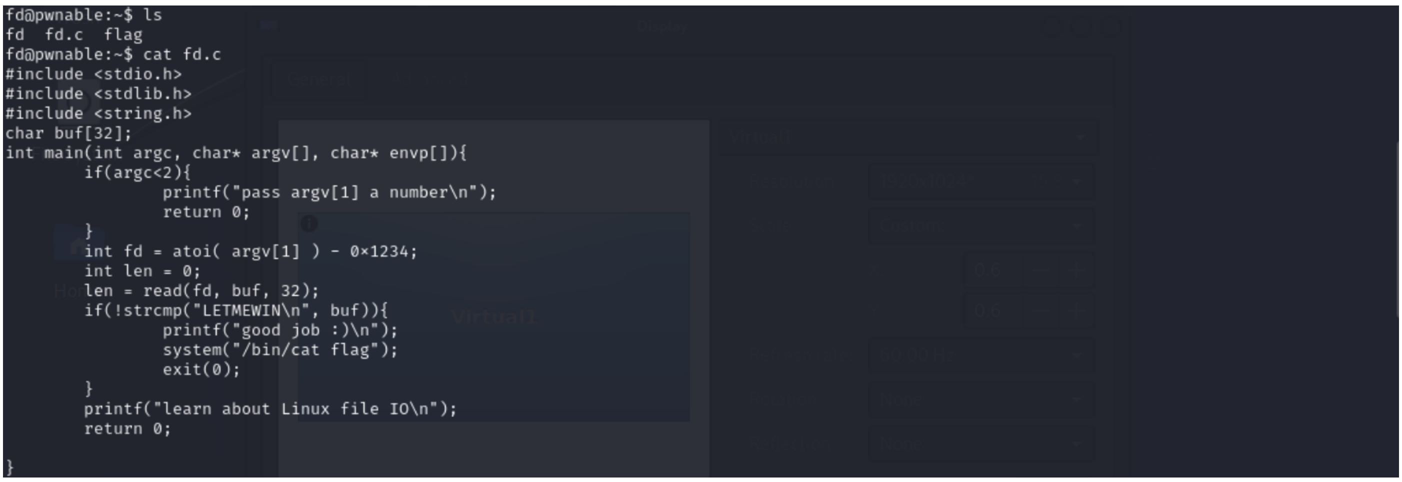
1. SSH 접속 및 살펴보기



```
┌──(kali㉿kali)-[~]
└─$ ssh fd@pwnable.kr -p2222
The authenticity of host '[pwnable.kr]:2222 ([128.61.240.205]:2222)' can't be
 established.
RSA key fingerprint is SHA256:XsWNjsQu3rST5O0W8mrLRJnmhrSehYpP7SVOGFM07AM.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[pwnable.kr]:2222' (RSA) to the list of known hos
ts.
fd@pwnable.kr's password:

- Site admin : daehee87@khu.ac.kr
- irc.netgarage.org:6667 / #pwnable.kr
- Simply type "irssi" command to join IRC now
- files under /tmp can be erased anytime. make your directory under /tmp
- to use peda, issue `source /usr/share/peda/peda.py` in gdb terminal
You have mail.
Last login: Mon Jan 29 12:10:42 2024 from 152.67.1.86
```

SSH를 이용해 상단에 표기해놓은 주소와 포트 번호로 접속한다.



```
fd@pwnable:~$ ls
fd  fd.c  flag
fd@pwnable:~$ cat fd.c
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
char buf[32];
int main(int argc, char* argv[], char* envp[]){
        if(argc<2){
                printf("pass argv[1] a number\n");
                return 0;
        }
        int fd = atoi( argv[1] ) - 0x1234;
        int len = 0;
        len = read(fd, buf, 32);
        if(!strcmp("LETMEWIN\n", buf)){
                printf("good job :)\n");
                system("/bin/cat flag");
                exit(0);
        }
        printf("learn about Linux file IO\n");
        return 0;

}
```

디렉토리의 파일들을 살펴보자 C 코드 파일이 존재하여 확인해보니 위와 같은 코드를 알 수 있었다.

프로그램 실행 시, 인자를 하나 넘겨 fd 의 값을 0 으로 만든 뒤, LETMEWIN 을 입력하면 같은 디렉토리에 있는 flag 라는 파일을 읽을 수 있게 되는 것 같다.

※ read 함수
ssize_t read(int fd, void *buf, size_t bytes)
fd : File Descriptor, 0 - 표준 력, 1 - 표준 력, 3 - 표준 오류
buf : 파일을 읽어 저장할 배열
bytes : 읽을 byte 수
반환 값은 읽어들인 byte 수이며, 실패했을 시 -1을 반환한다.

2. 공격

fd의 값을 0으로 만들기 위해서는 0x1234의 10진수 값을 알아야 한다.
0x1234를 10진수로 나타내면 4660이다.
따라서, 우리는 fd를 실행할 때, 그 인자로 4660을 넘겨주면 int fd = atoi(argv[1]) - 0x1234 부분에서 0이 저장되고 read(0, buf, 32)가 되어 표준 입력으로 buf 배열에 문장을 입력 받게 된다.
따라서, 우리는 주어진 입력에 대해서 LETMEWIN을 입력하면 if 문으로 인해 system 함수가 동작한다.
그렇다면, 우리는 flag를 얻을 수 있을 것이다.