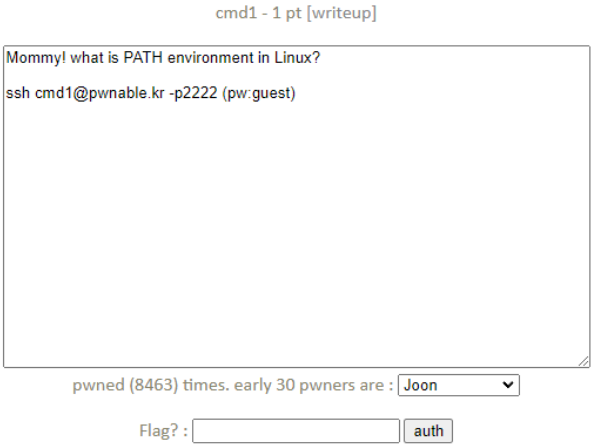
Pwnable.kr
- cmd1 -

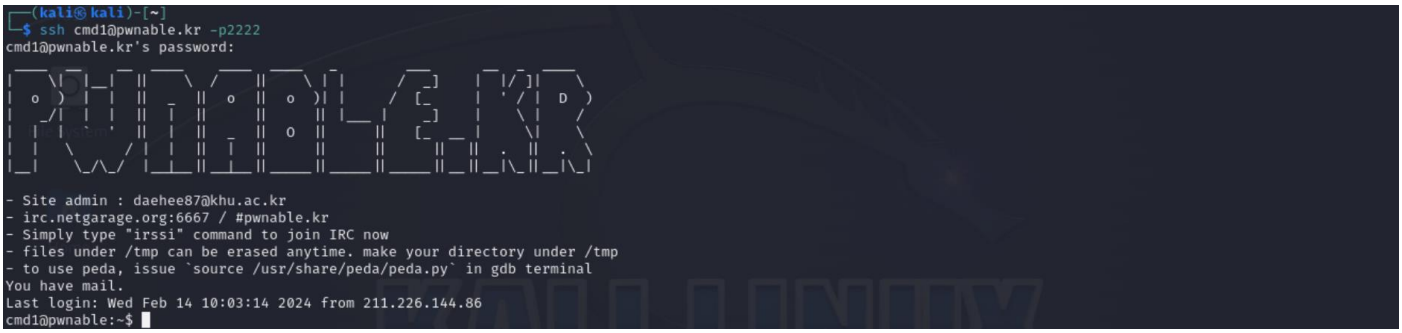
ssh cmd1@pwnable.kr -p2222
pw : guest

0. 문제 살펴보기



환경 변수에 대하여 얘기하고 있다.

1. SSH 접속 및 살펴보기



SSH를 이용해 상단에 표기해놓은 주소와 포트 번호로 접속한다.

디렉토리의 파일들을 살펴보자 C 코드 파일이 존재하여 확인해보니 위와 같은 코드를 알 수 있었다.
PATH 환경변수를 다른 값으로 뒤덮고, argv[1]의 문장에서 flag, sh, tmp 단어들이 없을 때, system 함수를 실행하는 것 같다.

※ strstr()
#include <string.h>
char *strstr(const char *string1, const char *string2);
string1 에서 string2 의 첫 번째 표시를 찾는다.
string1 에서 string2 의 첫 번째 표시 시작 위치에 대한 포인터를 반환한다.
string2 가 string1 에서 발견되지 않으면 NULL 을 반환한다.
string2 가 길이가 0 인 스트링을 가리키면 string1 을 반환한다.

※ PATH 환경변수
실행 파일이나 명령어를 찾는 경로를 설정하는 환경변수이다.
우리가 사용하는 명령어들은 모두 리눅스 내 어디인가에 위치해 있다. (ex. /bin/sh)
PATH 환경변수는 이러한 명령어들을 찾는 위치와 순서를 정의한다.

```
cmd1@pwnable:~$ env | grep PATH
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
```

콜론(:)을 기준으로 나뉘며, 실행 파일이나 명령어를 실행하면 가장 왼쪽에서부터 차례대로 탐색한다.
첫 번째 위치에서 탐색을 시작하고 없으면 다음 콜론 뒤, 없으면 다음 콜론 뒤로 이동하며 찾는다.

2. 공격

우리는 현재 PATH 경로가 바뀌어 다른 곳에서 명령어를 입력하지 못한다.
또한, flag, sh, tmp 단어들이 모두 금지되어 flag 파일을 직접 입력하지 못하고, 쉘도 실행하지 못하며, tmp 파일에 우회 경로를 만들어 놓지 못한다.
하지만, 간단한 방법이 있다. 바로, 와일드카드(*)를 사용하면 된다는 것이다.
문장에서의 와일드카드는 어떠한 문장이든 올 수 있다는 것을 뜻한다.
만약, 'cm*'이라고 한다면, 현재 디렉토리에서는 cmd1과 cmd1.c가 될 수 있다.
우리는 이를 이용할 것이다.

```
cmd1@pwnable:~$ ./cmd1 '/bin/cat fl*'
```

위와 같이 argv에 문장을 넣어주면 flag 파일이 정상적으로 읽혀 우리가 찾고자 했던 flag를 얻을 수 있다.