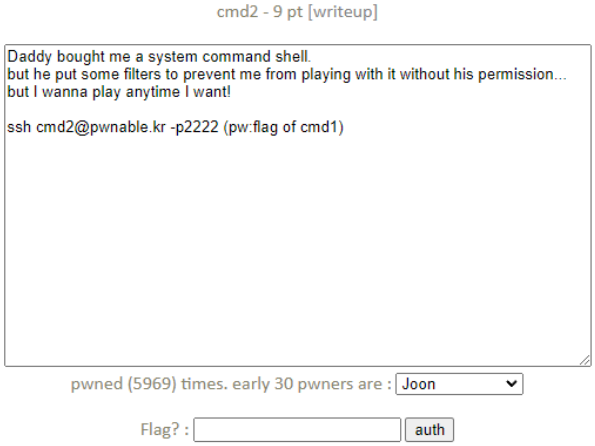
Pwnable.kr
- cmd2 -

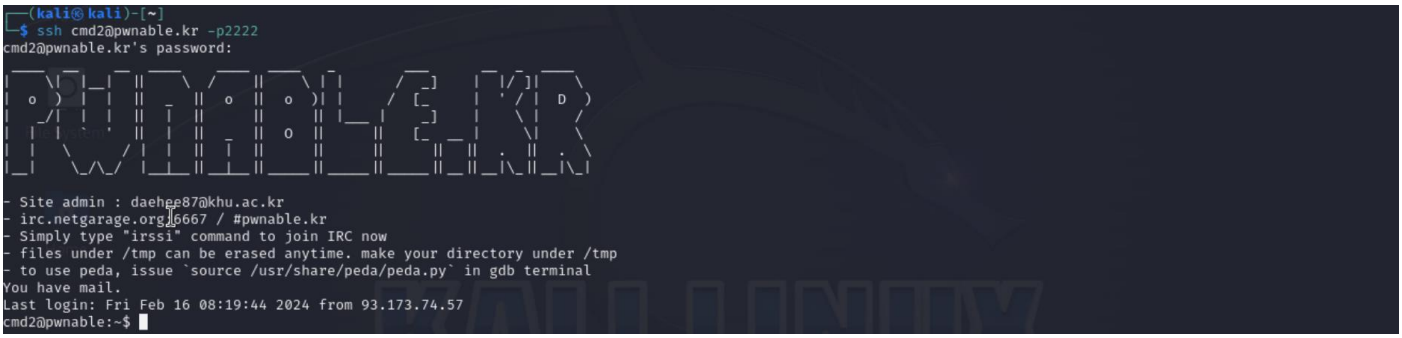
ssh cmd2@pwnable.kr -p2222
pw : mommy now I get what PATH environment is for :)

0. 문제 살펴보기



시스템 커맨드 쉘에 대한 얘기를 하며, 몇몇 필터가 있다고 한다.

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.
main() 함수가 실행되자마자 delete_env() 함수에 의해 환경변수들이 삭제되고, 새로운 PATH 환경변수를 삽입한다. argv[1]를 filter() 함수로 검사하여 =, PATH, export, /, `, flag 문자들이 없을 때, system() 함수를 통해 argv[1]의 문장을 실행하는 것 같다.

2. 취약점 파악

filter() 함수로 인해 새로운 환경변수를 삽입하지 못하고, '/' 문자로 인해 경로가 있는 상당수의 명령어들을 사용하지 못할 것이다.
하지만, 문제에서 현재 system command shell에 대해 얘기하였다. '/' 문자로 경로를 입력해야 하는 명령어들을 사용하지 못한다면, shell command를 사용하면 될 것이다. echo, mkdir, rm 등과 같은 명령어들은 쉘 명령어로, 따로 경로가 존재하지 않는다. 그렇다면 우리는 이 점을 이용하면 될 것이다.

3. 공격

많은 쉘 명령어들을 찾아보았다. 우리는 command라는 명령어를 사용할 것이다.
우리는 flag 파일을 보고 싶으므로 cmd1에서 사용했던 방식인 와일드 카드를 이용하여 cmd1을 볼 것이다.
여기서 우리는 cat을 이용할 것이지만, 그대로 이용하려면 /bin/cat과 같이 입력해야 하므로 filter() 함수에 의해 프로그램이 바로 종료된다.
따라서, command 명령어의 -p 옵션을 이용하여 cat을 경로 없이 실행할 것이다.

```
cmd2@pwnable:~$ ./cmd2 'command -p cat fl*'
command -p cat fl*
```

※ command
명령어 실행, 경로 확인, 쉘 내장 명령어 무시 등 다른 명령어와 함께 사용되어 다양한 목적으로 활용되는 유틸리티이다.
<옵션>
-p : 지정된 명령어의 실행 파일 경로를 찾아 사용한다.
-v : 지정된 명령어의 버전을 출력한다.
-V : 명령어를 실행할 때 추가 정보를 출력한다.
-h : 명령어에 대한 도움말을 출력한다.
-a : 명령어를 찾을 경로를 출력한다.
-e : 지정된 명령어가 발견되면 종료 코드 0을 반환한다. 발견되지 않으면 종료 코드 1을 반환한다.
-s : 쉘에서 명령어를 실행할 때, 사용할 기본 쉘을 설정한다.

```
command: command [-pVv] command [arg ...]
    Execute a simple command or display information about commands.

    Runs COMMAND with ARGS suppressing  shell function lookup, or display
    information about the specified COMMANDs.  Can be used to invoke commands
    on disk when a function with the same name exists.

    Options:
      -p        use a default value for PATH that is guaranteed to find all of
        the standard utilities
      -v        print a description of COMMAND similar to the `type' builtin
      -V        print a more verbose description of each COMMAND

    Exit Status:
    Returns exit status of COMMAND, or failure if COMMAND is not found.
```