```
[level1@ftz level1]$ cat hint

level2 권한에 setuid가 걸린 파일을 찾는다.
```

root로 setuid가 걸린 파일을 찾는다면

find /-user root -perm -4000이고 에러가 출력되어 에러가 나오지 않게 하려면

끝에 2>/dev/null을 추가한다.

find /-user root -perm -4000 2> /dev/null

(설명)

*파일을 찾을 때 – find

특수권한인 setuid가 걸려있는 파일을 찾으므로 → -perm 사용

파일 소유주가 level2인 파일을 찾으므로 -user 사용

*2는 표준 에러 출력을 의미, /dev/null은 버린다는 의미

(0이라면 표준입력 1이라면 표준 출력이다

표준 출력과 표준 오류 출력 둘 다 무시하는 경우는 뒤에 > /dev/null 2>&1

표준 출력과 표준 오류 출력방향을 지정하여 다른 파일로 저장하는 경우는 뒤에 예를 들어

1> ok.txt 또는 1> /dev/null 2> fail.txt)

level2 권한에 걸린 setuid를 찾는 것이니 find /-user level2 -perm -4000 2> /dev/null

```
[level1@ftz level1]$ find /-user level2 -perm -4000
find: /-user: No such file or directory
find: level2: No such file or directory
[level1@ftz level1]$ find / -user level2 -perm -4000 2> /dev/null
/bin/ExecuteMe
```

bin 폴더로 이동

```
[level1@ftz level1]$ cd /
[level1@ftz /]$ cd bin
[level1@ftz bin]$ ls
arch         cut            fgrep     login          ps          sync
ash          date           gawk      ls             pwd         tar
ash.static   dd             gettext   mail           red         tcsh
autodig      df             grep      mkdir          rm          touch
awk          dmesg          gtar      mknod          rmdir       true
basename     dnsdomainname  gunzip    mktemp         rpm         umount
bash         doexec         gzip      more           rvi         uname
bash2        domainname     hostname  mount          rview       unicode_start
bsh          dumpkeys       igawk     mt             sed         unicode_stop
cat          echo           ipcalc    mv             setfont     unlink
chgrp        ed             kbd_mode  my-pass        setserial   usleep
chmod        egrep          kill      netstat        sh          vi
chown        env            level7    nice           sleep       view
cp           ex             link      nisdomainname  sort        ypdomainname
cpio         ExecuteMe      ln        pgawk          stty        zcat
csh          false          loadkeys  ping           su
[level1@ftz bin]$
```

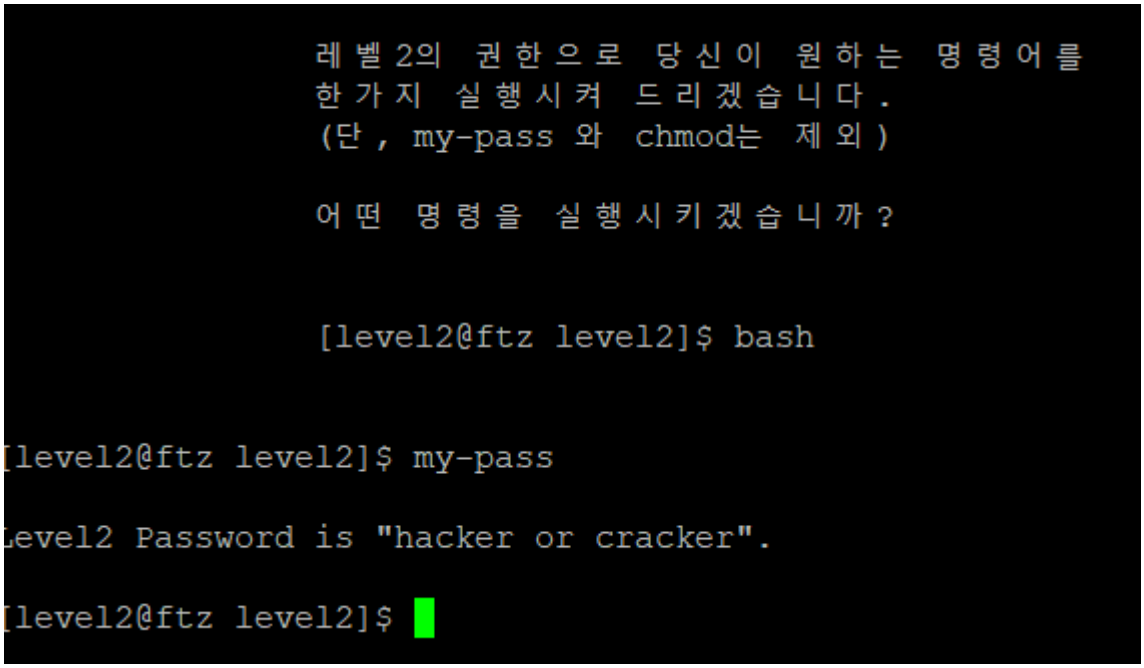
```
[level1@ftz /]$ /bin/ExecuteMe


        레벨2의 권한으로 당신이 원하는 명령어를
        한가지 실행시켜 드리겠습니다.
        (단, my-pass와 chmod는 제외)

        어떤 명령을 실행시키겠습니까?


        [level2@ftz level2]$
```

★ bash를 입력하여 level2 권한의 bash 쉘 획득


레벨2의 권한으로 당신이 원하는 명령어를
한가지 실행시켜 드리겠습니다.
(단, my-pass 와 chmod는 제외)
어떤 명령을 실행시키겠습니까?
[level2@ftz level2]$ bash
[level2@ftz level2]$ my-pass
Level2 Password is "hacker or cracker".
[level2@ftz level2]$

※ 사용법

항목	설명
cd [디렉토리 경로]	이동하려는 디렉토리로 이동
cd .	현재 디렉토리
cd ..	한 단계 상위 디렉토리로 이동
cd /	최상위 디렉토리로 이동
cd $변수명	변수에 저장된 경로로 이동
cd ~ cd $HOME cd	사용자 홈 디렉토리로 이동
cd ~계정명	입력한 사용자의 홈 디렉토리로 이동
cd -	이전 경로로 이동