```
login as: level8
level8@192.168.98.133's password:
[level8@ftz level8]$ ls
hint  public_html  tmp
[level8@ftz level8]$ cat hint


level9의 shadow 파일이 서버 어딘가에 숨어있다.
그 파일에 대해 알려진 것은 용량이 "2700"이라는 것 뿐이다.
```

현재 위치에서 파일을 찾아봄

```
[level8@ftz level8]$ ls -al
total 80
drwxr-xr-x    4 root     level8       4096 Jan 14  2010 .
drwxr-xr-x   34 root     root         4096 Sep 10  2011 ..
-rw-------    1 root     root            1 Jan 15  2010 .bash_history
-rw-r--r--    1 root     root           24 Feb 24  2002 .bash_logout
-rw-r--r--    1 root     root          224 Feb 24  2002 .bash_profile
-rw-r--r--    1 root     root          151 Feb 24  2002 .bashrc
-rw-r--r--    1 root     root          400 Sep 24  2000 .cshrc
-rw-r--r--    1 root     root         4742 Sep 24  2000 .emacs
-r--r--r--    1 root     root          319 Sep 24  2000 .gtkrc
-rw-r--r--    1 root     root          100 Sep 24  2000 .gvimrc
-rw-r-----    1 root     level8        109 Jan 14  2010 hint
-rw-r--r--    1 root     root          226 Sep 24  2000 .muttrc
-rw-r--r--    1 root     root          367 Sep 24  2000 .profile
drwxr-xr-x    2 root     level8       4096 Feb 24  2002 public_html
drwxrwxr-x    2 root     level8       4096 Jan 14  2009 tmp
-rw-r--r--    1 root     root            1 May  7  2002 .viminfo
-rw-r--r--    1 root     root         4145 Sep 24  2000 .vimrc
-rw-r--r--    1 root     root          245 Sep 24  2000 .Xdefaults
```

2700크기의 파일이 없어 사이즈를 이용하여 찾아봄

find / -size 사이즈+용량의 단위 2> /dev/null

512byte → b, byte → c, kbyte → k, 2byte → w

용량의 단위를 알 수 없어 다 해 보았다.

```
[level8@ftz level8]$ find / -size 2700b 2> /dev/null
[level8@ftz level8]$ find / -size 2700c 2> /dev/null
/var/www/manual/ssl/ssl_intro_fig2.gif
/etc/rc.d/found.txt
/usr/share/man/man3/IO::Pipe.3pm.gz
/usr/share/man/man3/URI::data.3pm.gz
```

```
[level8@ftz rc.d]$ cat found.txt
level9:$1$vkY6sSlG$6RyUXtNMEVGsfY7Xf0wps.:11040:0:99999:7:-1:-1:134549524

level9:$1$vkY6sSlG$6RyUXtNMEVGsfY7Xf0wps.:11040:0:99999:7:-1:-1:134549524

level9:$1$vkY6sSlG$6RyUXtNMEVGsfY7Xf0wps.:11040:0:99999:7:-1:-1:134549524

level9:$1$vkY6sSlG$6RyUXtNMEVGsfY7Xf0wps.:11040:0:99999:7:-1:-1:134549524

level9:$1$vkY6sSlG$6RyUXtNMEVGsfY7Xf0wps.:11040:0:99999:7:-1:-1:134549524

level9:$1$vkY6sSlG$6RyUXtNMEVGsfY7Xf0wps.:11040:0:99999:7:-1:-1:134549524

level9:$1$vkY6sSlG$6RyUXtNMEVGsfY7Xf0wps.:11040:0:99999:7:-1:-1:134549524

level9:$1$vkY6sSlG$6RyUXtNMEVGsfY7Xf0wps.:11040:0:99999:7:-1:-1:134549524

level9:$1$vkY6sSlG$6RyUXtNMEVGsfY7Xf0wps.:11040:0:99999:7:-1:-1:134549524

level9:$1$vkY6sSlG$6RyUXtNMEVGsfY7Xf0wps.:11040:0:99999:7:-1:-1:134549524

level9:$1$vkY6sSlG$6RyUXtNMEVGsfY7Xf0wps.:11040:0:99999:7:-1:-1:134549524

level9:$1$vkY6sSlG$6RyUXtNMEVGsfY7Xf0wps.:11040:0:99999:7:-1:-1:134549524

level9:$1$vkY6sSlG$6RyUXtNMEVGsfY7Xf0wps.:11040:0:99999:7:-1:-1:134549524
```

-/etc/shadow 파일

root : 6E2loH6Yc$0lcZ0hG……. : 15426 : 0 : 99999 : 7 :   :   :

1   2   3   4   5   6   7   8   9

1 → 사용자 계정

2 → 패스워드를 암호화한 값

비어있는 경우(::)는 로그인하는데 패스워드가 필요 없다는 것을 나타낸다.

*라고 되어 있으면 그 계정은 막아 두었다는 것을 나타낸다.

3 → 1970년부터 1월 1일부터 패스워드가 수정된 날짜의 일수를 계산한 값

4 → 패스워드가 변경되기 전 최소사용기간(일수)

0이면 언제든지 바꿀 수 있다는 뜻

5 → 패스워드 변경 전 최대사용기간(일수)

99999는 오랫동안 패스워드를 바꾸지 않았다는 뜻

6 → 패스워드 사용 만기일 전에 경고 메시지를 제공하는 일수

7 → 로그인 접속차단 일 수

8 → 로그인 사용을 금지하는 일 수 (월/일/연도)

9 → 예약 필드로 사용되지 않음

-2 부분의 패스워드 해석

```
level9:$1$vkY6sSlG$6RyUXtNMEVGsfY7Xf0wps.
```

Identifier	Scheme	Hash function	Salt length (in # of characters)	Salt length (in bits)
1	MD5-crypt	MD5	8	64
2a	B-crypt	Blowfish	8	64
md5	Sun MD5	MD5	8	64
5	SHA-crypt	SHA-256	16	128
6	SHA-crypt	SHA-512	16	128

< /etc/shadow 파일의 hashid 에 따른 해시 방법 >

$로 구분되어 있으며 $hash id $salt $hash value 의 형식이다.

$hash id는 어떤 해시를 하용해서 암호화를 할 것인지에 대한 정보를 가지고 있다

주로 많이 사용하는 hash id는 2,5,6이다. (id값이 1이면 MD5를 의미한다)

$salt는 패스워드를 암호화하는데 있어서 os내에서 생성하는 임의의 값이다.

$hash value는 salt + 비밀번호를 조합하여 MD5 해시화한 결과 값이다.

암호를 찾기 위해 john the ripper라는 프로그램을 이용하는데 (https://www.openwall.com/john/)

Download the latest John the Ripper core release (release notes):

- 1.9.0 core sources in tar.xz, 8.6 MB (signature) or tar.gz, 13 MB (signature)
- Development source code in CVS repository

밑의 것을 다운받아 압축파일을 풀고 그 안의 run 폴더에 암호를 써 txt파일로 넣는다.

```
level9:$1$vkY6sSlG$6RyUXtNMEVGsfY7Xf0wps.:11040:0:99999:7:-1:-1:134549524
```

cmd를 켜 run 폴더까지 이동한 다음 john.exe paw.txt를 실행하여 패스워드를 획득

```
C:₩>cd john-1.8.0-Win-32

C:₩john-1.8.0-Win-32>cd run

C:₩john-1.8.0-Win-32₩run>john.exe paw.txt
      1 [main] john 13952 find_fast_cwd: WARNING: Couldn't compute FAST_CWD pointer.  Please report this probl
the public mailing list cygwin@cygwin.com
Loaded 1 password hash (md5crypt [MD5 32/32])
Press 'q' or Ctrl-C to abort, almost any other key for status
apple            (level9)
1g 0:00:00:00 100% 2/3 2.881g/s 8489p/s 8489c/s 8489C/s apple
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```