FTZ_level8

```
[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.
```

리눅스 find 명령어를 이용하여 파일크기가 2700인 것을 찾아내야함

```
[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
```

해당 파일을 열어서 내용 확인

```
[level8@ftz level8]$ cd /etc/rc.d
[level8@ftz rc.d]$ ls -l found.txt
-r--r-----    1 root     level8       2700 Sep 10  2011 found.txt
[level8@ftz rc.d]$ cat found.txt
level9:$1$vkY6sSlG$6RyUXtNMEVGsfY7Xf0wps.:11040:0:99999:7:-1:-1:134549524
```

순정 shadow파일의 내용이 들어가 있는 것을 확인

level9: 사용자명

1vkY6sSlG$6RyUXtNMEVGsfY7Xf0wps.: 패스워드

(비어있는 경우 로그인 시 패스워드 필요 없음, *이 있는 경우 계정을 사용하지 않음)

11040: 최근 패스워드를 바꾼 날

0: 패스워드 최소 사용기간 (0일 경우 언제든 바꿀 수 있음)

99999: 패스워드 최대 사용기간(99999일 경우 무기한 사용)

7: 패스워드 사용 만기일 전에 경고 메시지를 제공하는 일 수

-1: 로그인 접속 차단 일 수

-1: 로그인 사용을 금지하는 일 수 (월/일/년)

134549524 : 예약필드

주로 봐야 할 부분은 패스워드 부분

$로 구분하고 있으며 $hashid $salt $hash value 를 나타냄

HashID : 어떤 Scheme를 이용해서 Hash 했는지 보여줌. 주로 사용하는 HashID는 $1, $5, $6

Salt : 패스워드를 암호화하는데 있어서 OS내에서 생성하는 임의의 값임. salt 값과 설정한 암호를 cript() 함수를 이용하여 암호화함. 형식 cript(Salt, 설정한 암호)

Hash Value : HashID에 따른 해시 방법과 Salt 값을 가지고 암호화된 결과

관련 명령어

pwconv : 일반 패스워드에서 shadow 패스워드로 변경하는 명령어. 이 명령어가 수행되고 나면 /etc/passwd의 두 번째 필드에 이는 암호화된 패스워드 부분만이 /etc/shadow 파일에 따로 저장되게 됨.

pwunconv : shadow 패스워드에서 일반 패스워드로 되돌리는 명령어. 이 명령어는 /etc/shadow 파일에 보관되었던 패스워드를 다시 /etc/passwd 파일에 저장하게 됨.

```
C:₩Users₩swye1₩john-1.9.0-jumbo-1-win64₩john-1.9.0-jumbo-1-win64₩run>john -show pass.txt
level9:apple:11040:0:99999:7:-1:-1:134549524

1 password hash cracked, 0 left
```

John the Ripper를 이용하여 level9의 암호 획득