Hacker School FTZ
- level 8 -

1. hint 파일 살펴보기

```
[level8@ftz level8]$ ls
hint  public_html  tmp
```

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

```
[level8@ftz level8]$ cat hint


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

cat 명령을 이용해 hint 파일의 내용을 살펴보았다.

2. shadow 파일 찾기

현재 용량이 2700인 파일을 찾아야 한다. 여기서 우리는 find 명령에서 -size 옵션을 이용해야 한다는 것을 알 수 있다. 하지만, 그 용량의 단위를 알지 못하므로 우리는 하나씩 대입해보아야 한다.

2-1) 블록

```
[level8@ftz level8]$ find / -size 2700b 2>/dev/null
[level8@ftz level8]$
```

블록 단위로 용량이 2700인 파일은 존재하지 않는 것을 확인할 수 있다.

2-2) byte

```
[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
```

검색 결과가 4개가 등장하였다. 여기서 수상해 보이는 found.txt 파일을 찾을 수 있다. 다음 스텝에서 확인해보자.

2-3) kbyte

```
[level8@ftz level8]$ find / -size 2700k 2>/dev/null
[level8@ftz level8]$
```

파일 용량이 2700kbytes인 파일은 존재하지 않는 것을 확인할 수 있다.

2-4) 2byte 워드

```
[level8@ftz level8]$ find / -size 2700w 2>/dev/null
/usr/lib/perl5/5.8.0/I18N/Collate.pm
/usr/share/locale/es/LC_MESSAGES/memprof.mo
/usr/share/locale/uk/LC_MESSAGES/gtk+.mo
```

검색 결과 3개가 등장하였다. 하지만, 수상해 보이는 파일은 존재하지 않는 것 같다.

※ -size 옵션
b : 블록 단위
c : byte
k : kbyte
w : 2byte 워드

-size +[용량][단위] : [용량] 이상 크기의 파일
-size -[용량][단위] : [용량] 이하 크기의 파일
-size [용량][단위] : [용량] 크기의 파일

3. found.txt 파일 확인

```
[level8@ftz level8]$ cat /etc/rc.d/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
```

cat 명령을 이용해 이전 스텝에서 수상해 보였던 파일을 확인하였더니, 위와 같은 shadow 파일을 확인해 볼 수 있었다. level9 계정의 정보가 담긴 shadow 파일이다. 우리는 두 번째 항목이 비밀번호임을 알고 있으므로 이를 해석해야 한다. 비밀번호의 가장 앞 필드의 값이 $1이므로 MD5로 Hash 값이 설정되었다는 것을 알 수 있다.

※ shadow 파일

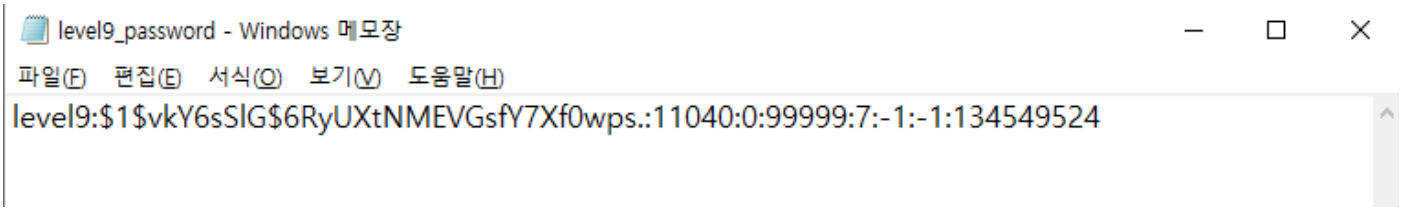
shadow 파일은 암호화된 패스워드와 패스워드 설정 정책이 기재되어 있으며 root 계정만이 읽을 수 있다.
각 필드마다 콜론(:)을 통해 구분된다.
사용자 계정명 : 첫 번째에 있는 필드로 사용자의 계정 이름을 나타낸다.
비밀번호 : 두 번째에 있는 필드로 암호화된 비밀번호를 나타낸다.
idsalt$encrypted_password 의 구조를 나타내고 있으며 각 필드는 $로 구분된다.
id : 암호화 알고리즘의 id 로 번호에 따라 (1) MD5, (2) BlowFish, (5) SHA-256, (6) SHA-512 로 나뉜다.
salt : 암호화를 더 어렵게 하기 위한 값으로 각 Hash 에 첨가하는 랜덤값이다.
비밀번호를 설정한 시간, 알고리즘 반복횟수 등을 이용하여 랜덤한 값을 삽입한다.
encrypted_password : 알고리즘과 salt 를 이용해 암호환한 비밀번호이다.
마지막 변경 : 1970 년 1 월 1 일을 기준으로 비밀번호를 변경한 날짜를 표시한다.
비밀번호 최소 사용 기간 : 비밀번호 변경 이후 최소한의 사용 기간을 표시한다.
비밀번호 최대 사용 기간 : 비밀번호 변경 이후 현재 비밀번호를 최대로 사용할 수 있는 기간으로 이 기간이 지나면 비밀번호를 재설정해야 한다.
경고 : 비밀번호 만료 이전 경고할 경고 일수이다.
비활성화 : 비밀번호 만료 이후 계정이 비활성화되기 전까지의 일수이다. 해당 기간 안에 변경해야 한다.
만료일 : 계정 만료일로 1970 년 1 월 1 일 기준으로의 일수이다.

4. 비밀번호 복호화

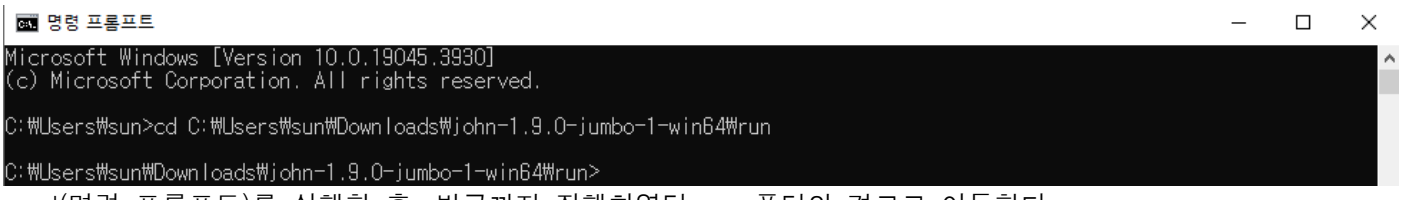
이 shadow 파일의 비밀번호를 해석하는 방법에는 여러 개가 있겠지만, 우리는 “John the ripper”라는 툴을 이용할 것이다.

https://www.openwall.com/john/

위 링크로 접속해 자신의 OS에 맞는 버전을 설치한다. 나는 windows를 사용하므로 이를 기준으로 풀이하였다.
압축된 폴더를 해체 후, john the ripper 폴더의 run 폴더를 들어간다.



이후, 이름을 임의로 정한 txt 파일을 하나 만들고 우리가 확인하였던 shadow 파일의 내용을 복사하여 txt 파일에 붙여넣기 한 후 저장한다.



cmd(명령 프롬프트)를 실행한 후, 방금까지 진행하였던 run 폴더의 경로로 이동한다.

```
C:₩Users₩sun₩Downloads₩john-1.9.0-jumbo-1-win64₩run>john.exe level9_password.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-opencl"
Use the "--format=md5crypt-opencl" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x3])
Will run 12 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 4 candidates buffered for the current salt, minimum 288 needed for performance.
Proceeding with wordlist:password.lst, rules:Wordlist
[redacted]           (level9)
1g 0:00:00:00 DONE 2/3 (2024-01-24 21:51) 15.38g/s 62153p/s 62153c/s 62153C/s 123456..88888888
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

john.exe 명령을 통해 해당 john the ripper 프로그램을 실행시킬 것이다. 여기에 우리가 작성하였던 txt 파일을 매개로 삽입하여 같이 실행한다. 그러면 프로그램일 실행되고 중간에 복호화된 비밀번호가 등장한 것을 확인할 수 있다. 이는 다음 단계인 level9의 비밀번호로 level9 로그인 시, 이용하자.