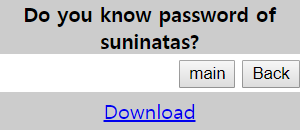
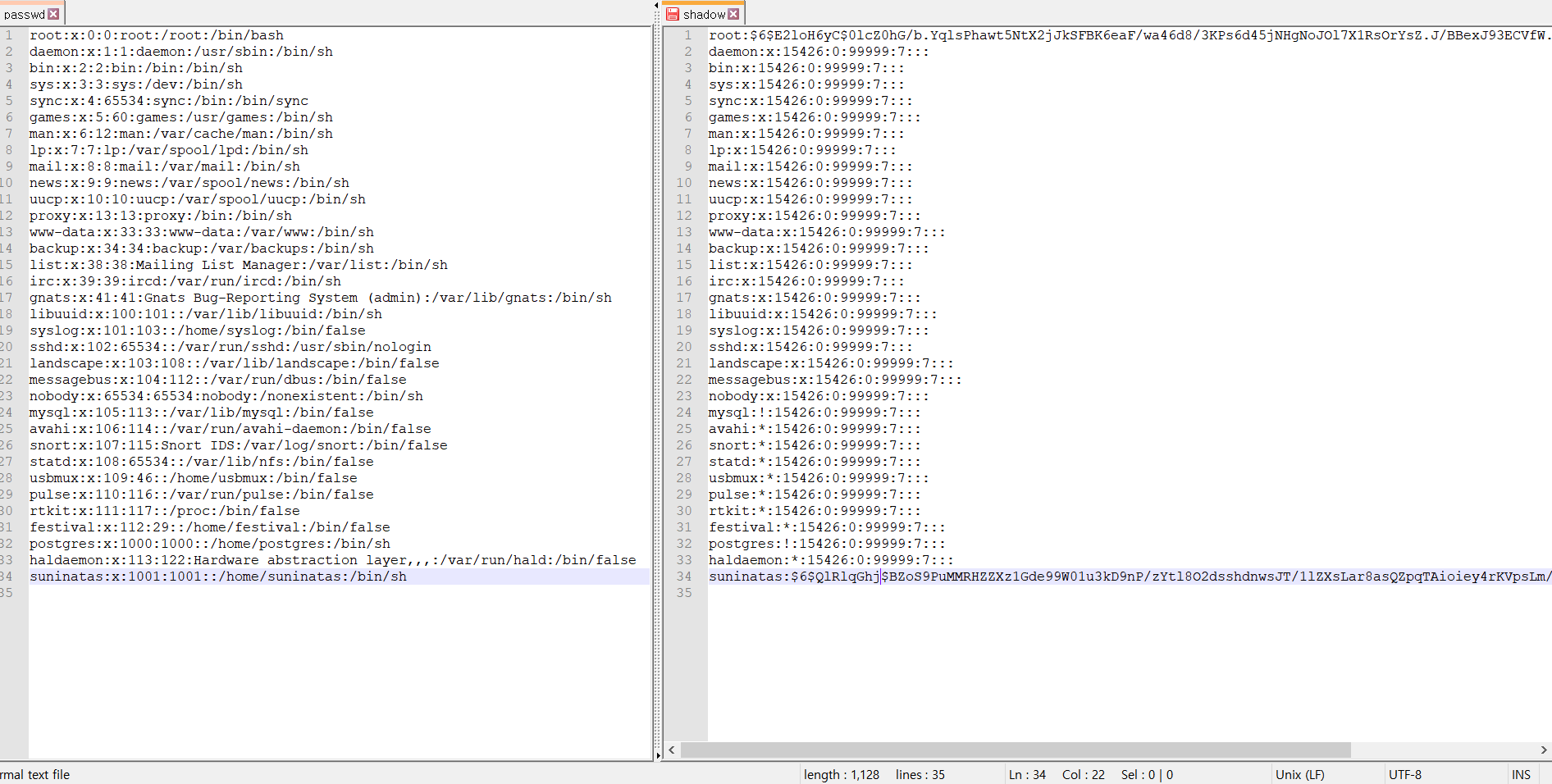
< 14번 워게임 풀이문서 >

김구민

당신은 suninatas의 비밀번호를 아십니까? 라는 문구로 문제는 시작한다. 그리고 다운로드 링크가 참조되어 있다.링크를 누르면 다음과 같은 파일들이 다운로드된다.

[ 다운로드된 파일 내용 ]



passwd 파일을 보면 다양한 요소들의 암호 형식이 나열되어 있음을 볼 수 있다.

마지막 줄을 참조해 보자면 다음과 같다.

suninatas:x:1001:1001::/home/suninatas:/bin/sh

1 2 3 4 5 6 7

1 : 계정명

2 : 패스워드

3 : 사용자 ID

4 : 그룹 ID

5 : comment

6 : 홈 디렉토리

7 : 기본 쉘 종류

두번째 패스워드의 경우는 암호화하여 저장할 경우 x로 표기되며 암호화된 패스워드는 shadow 파일에서 볼 수 있다.

shadow 파일에 suninatas 암호화된 비밀번호에 대한 정보가 있었는데 다음과 같았다.

suninatas:$6$QlRlqGhj$BZoS9PuMMRHZZXz1Gde99W01u3kD9nP/zYtl8O2dsshdnwsJT/1lZXsLar8asQZpqTAioiey4rKVpsLm/bqrX/:15427:0:99999:7:::

suninatas : 계정명

$6$QlRlqGhj$BZoS9PuMMRHZZXz1Gde99W01u3kD9nP/zYtl8O2dsshdnwsJT/1lZXsLar8asQZpqTAioiey4rKVpsLm/bqrX/ : 암호화된 패스워드

15427 : 패스워드가 수정된 일 수

0 : 패스워드 변경 전 최소 사용기간

99999 : 패스워드 변경 전 최대 사용기간

7 : 패스워드 만기 전 알림을 제공하는 횟수

그리고 그 뒤의 내용은 내용없음으로 처리되어 있는데 각각 로그인 접속 차단 일 수 / 로그인 금지 일 수(월/일/년도) / 예약필드(사용하지 않음) 의 의미를 가지고 있다.

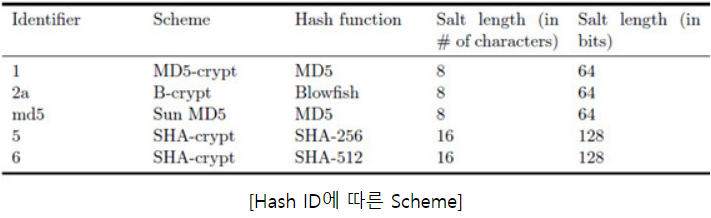
암호화된 패스워드는 ‘$’ 라는 구분자를 사용한다.

$6

$QlRlqGhj

$BZoS9PuMMRHZZXz1Gde99W01u3kD9nP/zYtl8O2dsshdnwsJT/1lZXsLar8asQZpqTAioiey4rKVpsLm/bqrX/

이들은 각각 Hash ID, Salt, Hash Value 라고 한다.



첫번째로 확인할 수 있는 Hash ID는 1, 5, 6이 가장 흔하게 사용된다고 한다.

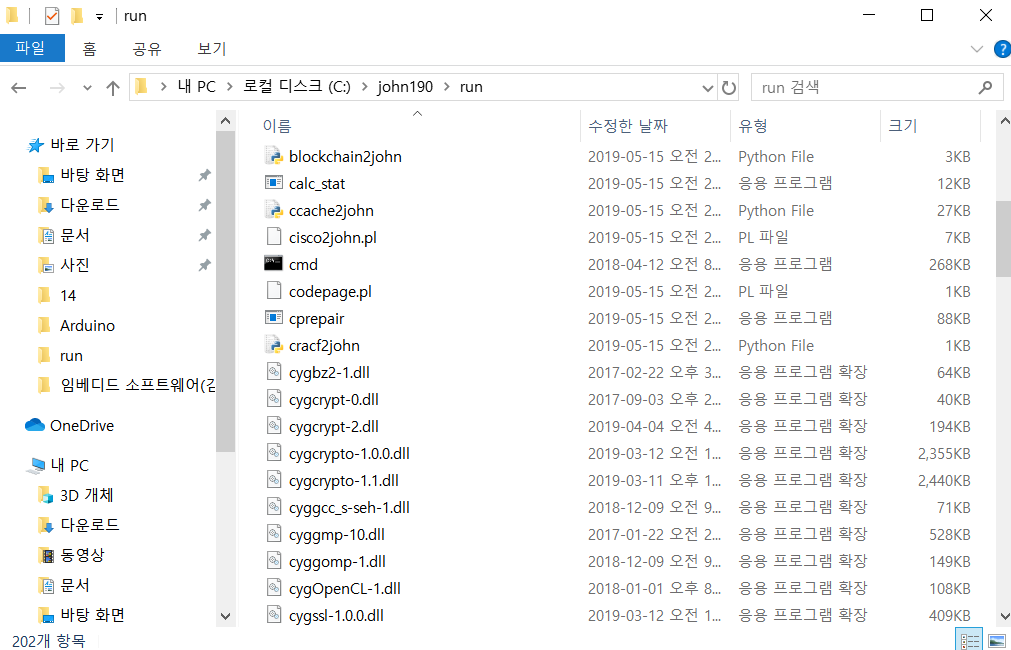
두번째는 Salt로 OS에서 임의로 생성되는 값이다. 이 값은 패스워드와 함께 Hash 함수로 들어가 패스워드를 암호화하는데 사용한다고 한다. 그렇기 때문에 이 값을 모르면 크래킹이 불가하다.

세번째는 Hash Value로 Hash ID에 따른 Hash 방법과 Salt 값을 가지고 암호화된 결과이다.

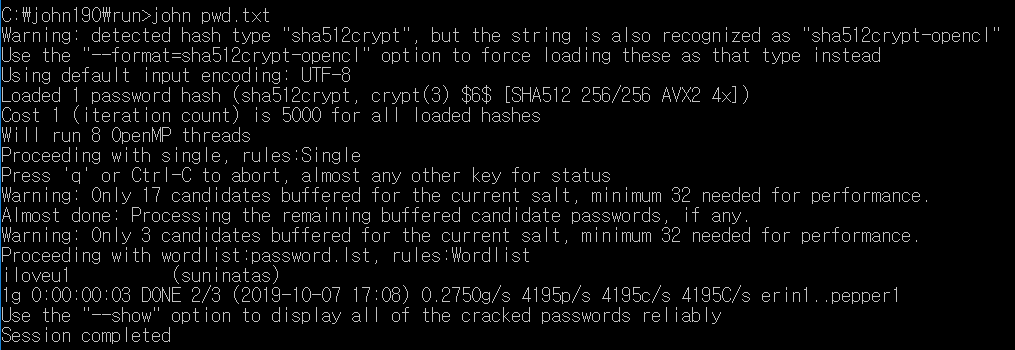
본인은 이 암호화된 패스워드를 복호화하기 위해서 ‘John the Ripper’ 라는 프로그램을 사용했다.

다음과 같이 john the ripper 폴더에 cmd.exe 를 복사해서 위치시킨다.

또 shadow 파일의 암호화된 패스워드의 내용을 텍스트 파일로 만들어서 저장한다.



그 다음 cmd.exe 를 실행시키고 john the ripper 프로그램으로 텍스트 파일의 내용을 복호화한다.



내용을 확인해 보면 최종 복호화된 비밀번호가 ‘iloveu1’ 임을 알 수 있다.